RAPPORT D'ACTIVITÉ

AGENCE
NATIONALE
DE LA SÉCURITÉ
DES SYSTÈMES
D'INFORMATION

***Édité par** l'Agence nationale de la sécurité des systèmes d'information (ANSSI)*
***Directeur de la publication :** Guillaume Poupard*
***Coordination :** Séverine Oger et Anne-Catherine Belliot*
***Conception et réalisation :** Prop'OSE et Chien Jaune studio*
prop-ose.fr | chienjaunestudio.com
***Coordination éditoriale :** Stéphane Malagnac*
***Crédits photos :** S.de la Moissonnière / P. Gaillardin / E. Flogny / N. Krtolica /P. Vermes / ANSSI / Shutterstock : Ikars / Fotolia : IR Stone, Vasyl, phonlamaiphoto, shock*
***Illustrations :** Chien Jaune studio*

SOMMAIRE

Louis Gautier, secrétaire général de la défense et de la sécurité nationale

Louis Gautier, secrétaire général de la défense et de la sécurité nationale

LOUIS GAUTIER

Quel bilan peut-on tirer de l'activité de l'ANSSI en 2017 ?

2017 aura été une année marquée par plusieurs échéances électorales et le renouvellement des autorités que nous servons. À l'automne 2016, j'ai attiré l'attention sur les risques qui pouvaient affecter les processus électoraux, dès les primaires organisées par certains partis politiques. Devant l'acuité de la menace, les équipes des candidats à ces scrutins ont été sensibilisées à différents risques, notamment cybernétiques. Le rôle qu'a joué l'ANSSI dans ce processus a été exemplaire. La disponibilité, l'investissement et l'analyse fine dont a fait preuve l'ANSSI ont permis de caractériser un risque encore nouveau et aux contours mal définis.

En quoi 2017 a-t-elle marqué un tournant dans la manière dont l'ANSSI assume son rôle d'autorité ?

2017 a installé l'ANSSI comme dépositaire de compétences rares, précieuses et indispensables au bon fonctionnement de la République, au-delà des compétences décrites par le décret fondateur du 7 juillet 2009. Nous devons nous en féliciter collectivement. Si les obligations qui résultent de ces attentes sont grandes, l'ANSSI a su être fidèle à ce qui fait notre patrimoine génétique commun : l'alliance de la compétence technique et de la faculté d'anticipation, dans un mouvement permanent d'adaptation aux besoins de l'État.

Si vous deviez revenir sur un projet majeur de l'ANSSI, quel serait-il ?

L'ANSSI avait prévu, avec le CTG, le passage à une nouvelle génération de téléphones fixes sécurisés à l'usage, dans un premier temps, des cabinets ministériels. Nous avons fait le choix d'installer ces nouveaux terminaux baptisés Osiris dès l'arrivée des nouvelles équipes gouvernementales pour les sensibiliser et les familiariser le plus tôt possible à leur utilisation. Ce projet, par les multiples compétences et l'investissement humain qu'il requiert, a été mené de façon exemplaire à plus d'un titre. Loin de s'arrêter à la mise en service des téléphones, ce projet impose un suivi et un accompagnement de « clients » exigeants. C'est une satisfaction collective de pouvoir proposer aux plus hautes autorités les outils adaptés au bon exercice de leur mandat.

Guillaume Poupard, directeur général de l'ANSSI

Guillaume Poupard, directeur général de l'ANSSI

GUILLAUME POUPARD

LA SÉCURITÉ NUMÉRIQUE N'EST PAS UNE OPTION ; ELLE EST DÉFINITIVEMENT L'AFFAIRE DE TOUS

Quelles sont les grandes leçons que l'ANSSI a retenues de l'année 2017 ?

Je dirais en premier lieu que 2017 est une année singulière à plus d'un titre. D'abord et avant tout car c'est une année électorale d'importance, avec plusieurs scrutins nationaux aux enjeux de cybersécurité majeurs. Ensuite, parce qu'elle a permis à l'ANSSI de mieux faire comprendre que le risque cyber n'est pas – n'est plus pour certains attentistes – l'affaire des autres, un dossier à traiter « plus tard » mais bel et bien un enjeu actuel, prégnant. Enfin, car les attaques qui ont émaillé le calendrier ont montré une dimension nouvelle : plus sophistiquées, mieux élaborées, plus destructrices et touchant désormais toute la société, du citoyen à la grande entreprise… et même à notre démocratie.

Plus largement, le développement du numérique s'accompagne désormais du développement concomitant de la menace numérique. Dans un tel contexte, il est plus que jamais utile de rappeler le rôle essentiel que les responsables politiques et économiques ont à jouer pour penser la sécurité à la lumière des enjeux économiques, stratégiques ou encore d'image qui sont les leurs.

Comment l'action de l'ANSSI a-t-elle répondu à ces cyberattaques en 2017 ?

Répondre n'est qu'une partie de notre action. Nous sommes là pour anticiper, veiller, sensibiliser, former et développer un écosystème vertueux à même de prévenir et détecter les attaques.

Justement, 2017 a peut-être permis de mettre en lumière tout le faisceau d'actions que nous menons au quotidien au-delà de celui, parfois plus visible, de « pompier informatique. » Un pompier intervient quand l'incendie s'est déclaré ; c'est indispensable, mais insuffisant dans notre domaine car notre objectif est bien d'éviter le plus possible les sinistres et surtout de se faire déborder par un nombre exponentiellement croissant de catastrophes.

L'ANSSI développe et entretient une culture de l'innovation en se plaçant non pas comme suiveur mais comme prescripteur. Prescripteur de bonnes pratiques, de bons réflexes, de bonne information. Pour les partager, nos partenaires et nous créons des outils, menons des actions de sensibilisation et soutenons le développement de solutions à la pointe de la technologie pour que chacun puisse s'en emparer et, ainsi, contribuer à cet effort de sécurité numérique qui ne peut être que collectif.

Cet effort ne se conjugue pas qu'au national. Le travail de l'ANSSI s'inscrit également dans une logique européenne et internationale. Comment ?

Par étape ai-je envie de répondre. Parce que, même s'il y a urgence, avancer à marche forcée est contre-productif.

Depuis des années, nous avons engagé un patient travail de coopération avec les États membres de l'Union européenne afin de constituer un ensemble cohérent face à la menace. Cette collaboration s'illustre également par des échanges constants avec la commission européenne. L'élaboration puis la transposition de la directive Network and Information Security (NIS) dans le droit national en est un exemple particulièrement vertueux et efficace.

L'ANSSI tisse également des liens avec des États désireux d'élever leur niveau de sécurité et nous répondons présent pour échanger bonnes pratiques, conseils et informations. Enfin, l'idée selon laquelle l'entretien de liens resserrés avec nos partenaires favorise nos capacités respectives à faire face aux attaques nous amène à engager de nombreuses discussions avec des pays dont le modèle d'organisation et la maturité vis-à-vis de ces enjeux sont parfois différents des nôtres. Si le modèle français peut sembler original en comparaison avec d'autres approches, chaque jour nous apporte la preuve d'un écho bel et bien effectif. Une réalité qui place l'ANSSI au centre du jeu stratégique et non plus seulement opérationnel et technique.

La sécurité numérique n'est pas une option ; elle est définitivement l'affaire de tous.

8 & 14 avril 2017

SHADOW BROKERS

MENACE

Le groupe Shadow Brokers publie gratuitement plusieurs outils informatiques offensifs et très sophistiqués porteurs de vulnérabilités de type O Day. On compte parmi elles Eternal Blue sur lequel se sont appuyées les deux campagnes d'attaques WannaCry et NotPetya.

à partir de mars 2017

VAULT 7 ET 8

MENACE

À l'occasion de deux campagnes de publication massives – Vault 7 et 8 – Wikileaks divulgue des documents décrivant un arsenal d'outils d'attaque informatique datés de 2013 à 2016 en affirmant que ces programmes auraient été développés par la CIA.

octobre 2017

IOTROOP

MENACE

Un an après Mirai, émergence d'un nouveau réseau massif d'objets connectés zombies, dénommé IoT_Reaper/IoTroop. Ce réseau pourrait permettre la revente des capacités de calcul et la conduite de différents types d'attaques, notamment par déni de service.

fin 2017

UBER ET DELOITTE

ATTAQUE

L'entreprise de VTC Uber et le cabinet de conseil Deloitte ont annoncé avoir été victimes de cyberattaques faisant état de l'exfiltration de données personnelles sur leurs clients.

PARTI DÉMOCRATE USA

ATTAQUE

Perturbation des élections présidentielles américaines *via* la publication de milliers d'e-mails des responsables démocrates.

CYBER PANORAMA 2017

L'année 2017 a vu se matérialiser de nouvelles tendances à travers l'identification de cybermenaces et la conduite de cyberattaques qui ont marqué par leur intensité, leur caractère inédit et les nouvelles craintes qu'elles font peser.

Si certains des événements observés s'illustrent par le recours à des modes opératoires nouveaux ou connaissant un pic de croissance sans précédent, d'autres interpellent par leur résonance parfois mondiale dans les sphères politiques, économiques et stratégiques.

Les tentatives de déstabilisation des processus démocratiques et de l'ordre économique s'inscrivent dans cette dernière catégorie et nécessitent parfois peu de moyens, suscitant une émotion d'autant plus vive.

16 octobre 2017

VULNÉRABILITÉ WPA2

MENACE

Plusieurs failles de sécurité importantes ont été révélées dans le protocole Wi-Fi WPA2 qui sécurise l'immense majorité des réseaux Wi-Fi domestiques.

décembre 2017

4IQ LEAKS

MENACE

L'entreprise 4IQ, spécialisée dans la recherche de données personnelles publiées sur Internet, diffuse un article relatif à la découverte, sur le *dark net*, d'une base de données libre d'accès recensant près d'1.4 milliard d'identifiants et mots de passe.

du 13 mai au 30 juillet 2017

EQUIFAX

ATTAQUE

Série d'attaques exploitant une faille d'un serveur Web de l'agence d'évaluation de crédit Equifax, conduisant au vol de bases de données contenant les informations à caractère personnel de plus de 145 millions d'Américains.

5 mai 2017

PRÉSIDENTIELLES FRANÇAISES

MENACE

Suite à l'observation et à l'analyse de la campagne de déstabilisation des élections américaines, la France et l'Allemagne activent un plan d'action pour leurs scrutins nationaux.

27 juin 2017

NOTPETYA

ATTAQUE

S'appuyant sur le code d'exploitation Eternal Blue publié par Shadow Brokers, le code malveillant NotPetya s'est répandu suite à la mise à jour d'un logiciel ukrainien paralysant de nombreuses entités, principalement en Europe. Une attaque à des fins de sabotage au mode opératoire et à l'ampleur inédits.

7 juin 2017

RÉFÉRENDUM BRITANNIQUE

ATTAQUE

Au Royaume-Uni, attaque en déni de service sur le site Internet d'enregistrement du vote au référendum.

12 mai 2017

WANNACRY

ATTAQUE

Grâce à l'exploitation de failles divulguées par Shadow Brokers, dont Eternal Blue, une vague d'attaques distribue le rançongiciel WannaCry dans plus de 150 pays. Près de 250 000 entités auraient été impactées.

mai 2017

QATAR

ATTAQUE

Le compte Twitter de l'agence de presse officielle du Qatar a été compromis et utilisé pour publier un communiqué de presse factice rapportant de faux propos attribués à l'émir du Qatar.

août & septembre 2017

CCLEANER

ATTAQUE

Compromission du système de mise à jour du logiciel de maintenance informatique grand public CCleaner. En exploitant ainsi la confiance des utilisateurs, cette attaque discrète et indirecte, introduisant une modification malveillante en amont de la distribution, a infecté un grand nombre d'ordinateurs.

3 avril 2017

APT10

ATTAQUE

Publication d'un rapport faisant état d'une campagne d'espionnage de grande ampleur dont le mode opératoire dénommé APT10 repose sur la compromission des fournisseurs et sous-traitants des entreprises ciblées pour les atteindre.

8 GRANDES TENDANCES

_DÉSTABILISATION DES PROCESSUS DÉMOCRATIQUES

_DÉSTABILISATION DE L'ORDRE ÉCONOMIQUE

_SOPHISTICATION DES MODES OPÉRATOIRES

_CARACTÈRE INDIRECT

_CARACTÈRE NON DISCRIMINANT

_RÉSURGENCE D'EFFETS DESTRUCTEURS

2017
UNE ANNÉE CYBER INÉDITE

L'ANNÉE 2017 AURA ÉTÉ MARQUÉE PAR DE NOMBREUSES ATTAQUES CYBERNÉTIQUES, INÉDITES PAR LEUR AMPLEUR, LEUR MODE DE DIFFUSION ET LEUR CARACTÈRE DÉSORMAIS NON-DISCRIMINANT. DES MENACES QUI ONT MOBILISÉ TOUTE L'ATTENTION DE L'ANSSI, LUI PERMETTANT AINSI D'APPORTER UNE RÉPONSE OPÉRATIONNELLE ET STRATÉGIQUE ADAPTÉE AUX ACTEURS NATIONAUX QUE CES ATTAQUES ONT TOUCHÉS OU MENACÉS.

JANVIER 23

FIC 2017 – 26 FORMATIONS REÇOIVENT LE LABEL SECNUMEDU

Lors du Forum International de la Cybersécurité, 26 formations supérieures en sécurité du numérique selon les critères de l'agence reçoivent des mains de Guillaume Poupard les premiers certificats SecNum*edu*.
L'objectif : offrir plus de lisibilité à l'offre de formation tout en rapprochant les acteurs de cette filière.

FÉVRIER 23

PUBLICATION DU GUIDE « L'ESSENTIEL DE LA SÉCURITÉ NUMÉRIQUE POUR LES DIRIGEANTS »

Un guide à l'initiative du Conseil de l'Économie et de l'Information du Digital (CEIDIG) auquel l'ANSSI et d'autres acteurs du numérique ont participé.
L'objectif : donner un coup de projecteur positif et constructif sur les enjeux de sécurité du numérique pour encourager les dirigeants à s'emparer de ces questions éminemment stratégiques.

MARS

MISE EN PLACE DU DISPOSITIF DE VIGILANCE RENFORCÉE DE L'AGENCE POUR LES ÉLECTIONS 2017

SÉMINAIRES DE SENSIBILISATION DES CANDIDATS À LA PRÉSIDENTIELLE

Plusieurs actions de sensibilisation et de prévention sur les cybermenaces sont menées auprès des partis politiques représentés au Parlement ainsi qu'auprès des équipes de campagne des candidats à l'élection présidentielle.

AVRIL 06 et 07

CONFÉRENCE INTERNATIONALE

Sous l'impulsion du secrétaire général de la défense et de la sécurité nationale, l'ANSSI organise la conférence internationale ***« Construire la paix et la sécurité internationales de la société numérique »*** à l'Unesco (Paris).

23

ÉLECTIONS PRÉSIDENTIELLES

Anticipant un risque de déstabilisation démocratique lors des élections nationales qui ont ponctué l'année, l'ANSSI a engagé un plan d'action global et original de protection du processus électoral : sensibilisation des partis, audits et sécurisation des systèmes d'information concourant au processus électoral, mise en place d'un processus de saisine par la CNCCEP, du Conseil d'État et du Conseil constitutionnel et mise en place d'un dispositif de vigilance renforcée.

JUIN

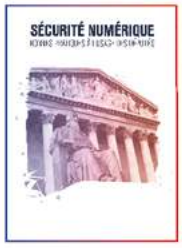
11 - 18 *ÉLECTIONS LÉGISLATIVES*

27 *ATTAQUE NOTPETYA*

29 *SENSIBILISATION DES NOUVEAUX CABINETS MINISTÉRIELS PAR LA MISE À DISPOSITION D'UN GUIDE DE BONNES PRATIQUES*

JUILLET

SENSIBILISATION DES DÉPUTÉS PAR LA MISE À DISPOSITION D'UN GUIDE DE BONNES PRATIQUES



MAI

07 ***MISE EN PRODUCTION DU SYSTÈME OSIRIS***

Le système de téléphonie fixe sécurisée Osiris est déployé auprès des équipes gouvernementales afin de sécuriser les transmissions relevant du secret de la défense nationale.

12 *ATTAQUE WANNACRY*

18 ***LANCEMENT DU MOOC SECNUMACADÉMIE***

Parce que la sécurité du numérique est l'affaire de tous, l'ANSSI la rend accessible aux étudiants, salariés, dirigeants ou particuliers en proposant la formation en ligne SecNum*académie* dont les contenus, pédagogiques et interactifs, ont été conçus par des experts de l'agence.

SecNum académie
ANSSI

AOÛT

CONTRIBUTION DE L'ANSSI À LA REVUE STRATÉGIQUE DE CYBERDÉFENSE

Emmanuel Macron a confié au SGDSN, chargé des travaux de la prochaine Loi de programmation militaire (2019-2025), la conduite d'une revue stratégique spécifique en matière de cyberdéfense : une première pour notre pays. L'ANSSI a apporté sa contribution à cette initiative portée à l'échelle interministérielle.

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

OCTOBRE

LANCEMENT NATIONAL DE LA PLATEFORME CYBERMALVEILLANCE.GOUV.FR

MOIS EUROPÉEN DE LA CYBERSÉCURITÉ

05 ***PUBLICATION D'UNE ORDONNANCE RELATIVE À L'IDENTIFICATION ÉLECTRONIQUE ET AUX SERVICES DE CONFIANCE POUR LES TRANSACTIONS ÉLECTRONIQUES***

Présentée au Conseil des ministres du 4 octobre 2017 par le Premier ministre Édouard Philippe, l'ordonnance 2017-1426 vise à renforcer la sécurité des échanges électroniques *via* une certification par l'ANSSI des services d'identification électronique mis à disposition des utilisateurs.

11 ***ASSISES DE LA SÉCURITÉ : GUILLAUME POUPARD ANNONCE LE LANCEMENT IMMINENT DES VISAS DE SÉCURITÉ***

Dans le cadre des Assises de la sécurité et des systèmes d'information organisées à Monaco, l'ANSSI annonce la mise en place en 2018 de « Visa de sécurité ANSSI ».
L'objectif : offrir davantage de lisibilité et de visibilité à l'offre de solutions qualifiées et certifiées.

VISA DE SÉCURITÉ

DÉPLOIEMENT DES TERMINAUX SECDROID POUR NÉOGEND

À l'issue d'une phase d'expérimentation dans les Hauts-de-France, 80 000 terminaux mobiles sécurisés Secdroid sont déployés sur le territoire national pour équiper les personnels de gendarmerie dans le cadre du programme NÉOgend.

SEPTEMBRE

06

20 000 FOLLOWERS SUR TWITTER

14 et 15 ***CONFÉRENCE SUR LE MARCHÉ UNIQUE DU NUMÉRIQUE (MUN) DE TALLINN (ESTONIE)***

L'ANSSI participe à la conférence organisée par la présidence estonienne du Conseil de l'Union européenne sur le Marché Unique du Numérique et la sécurité numérique commune organisée à Tallinn. À cette occasion, elle rappelle et défend les grands axes de l'autonomie stratégique de l'UE.

24

ÉLECTIONS SÉNATORIALES

NOVEMBRE

ACCORD DE COOPÉRATION ENTRE LA FRANCE ET LA TUNISIE

Signature d'un programme de coopération entre l'ANSSI et son homologue tunisienne l'Agence nationale de sécurité informatique (ANSI) pour renforcer le partage d'informations, d'expériences et de bonnes pratiques.

DÉCEMBRE

18

SENSIBILISATION DES SÉNATEURS PAR LA MISE À DISPOSITION D'UN GUIDE DE BONNES PRATIQUES

– MENACE CYBER : POUR TOUT COMPRENDRE

LE PANORAMA DE LA CYBERMENACE A MIS EN ÉVIDENCE TROIS PHÉNOMÈNES MAJEURS EN 2017.

1 PROLIFÉRATION D'OUTILS D'ATTAQUES SOPHISTIQUÉS

La publication d'outils d'attaques sophistiqués facilite leur prolifération, allant parfois jusqu'à la conduite de véritables campagnes d'attaques dont les conséquences peuvent se révéler désastreuses. En effet, ces outils peuvent par nature être copiés à l'infini et se diffuser très rapidement. Ceux divulgués sur Internet sont ainsi récupérés par d'autres groupes malintentionnés pour venir grossir les rangs de leur propre arsenal informatique. Une multiplicité d'outils, de modes opératoires et d'acteurs qui rend plus difficile voire impossible l'identification de l'origine de l'attaque.

2 RÉSURGENCE D'ATTAQUES AUX EFFETS DESTRUCTEURS

L'ANSSI a constaté une recrudescence d'attaques aux effets destructeurs réalisées à des fins lucratives ou de sabotage. Parmi elles, l'agence observe depuis 2014 une hausse constante des attaques par rançongiciel, de virulence variable. Ce type de code malveillant séquestre les données des équipements informatiques infectés jusqu'à ce que la victime paie la rançon, généralement avec une cryptomonnaie telle que le Bitcoin.

3 ESPIONNAGE PAR COMPROMISSION D'ÉDITEURS OU DE PRESTATAIRES INFORMATIQUES

À l'échelle mondiale, l'ANSSI constate une multiplication des opérations d'espionnage informatique. Ces opérations, menées par des groupes organisés, consistent à capter des informations confidentielles sur un savoir-faire, des individus, des concurrents, un secteur d'activité donné ou encore des organisations, gouvernementales ou non. L'objectif de ces actions offensives est d'obtenir à l'insu de la cible un avantage stratégique par le recours à des outils et modes opératoires adaptés au niveau de sécurité du système d'information ciblé. En 2017, ces opérations se sont particulièrement illustrées par leur caractère indirect avec des attaques visant notamment la chaîne d'approvisionnement de l'entreprise ciblée.

GRADATION DES RISQUES CYBER

2 435 *signalements*

–

dont **1 621** *traités*

–

794 *incidents (hors OIV)*

–

20 *incidents majeurs*

–

12 *opérations de cyberdéfense*

–

3 *crises*

–

UNE RÉPONSE AGILE ET ADAPTÉE À CHAQUE MENACE

2017 AURA INCONTESTABLEMENT REPRÉSENTÉ UNE ÉTAPE IMPORTANTE DANS LA PERCEPTION DU RISQUE CYBER. IMPORTANTE DE PAR L'AMPLEUR ET L'ÉVOLUTION DES ATTAQUES ; IMPORTANTE PAR L'ÉCLAIRAGE APPORTÉ AU TRAVAIL DE L'ANSSI À L'ÉGARD DES ACTEURS POLITIQUES, ÉCONOMIQUES ET DU GRAND PUBLIC ; IMPORTANTE, ENFIN, DANS LA PRISE DE CONSCIENCE DE LA NÉCESSITÉ DE DÉVELOPPER DES OUTILS ET DES MÉTHODES AGILES À MÊME DE S'ADAPTER EN PERMANENCE AU CARACTÈRE DÉSORMAIS MOUVANT DE CES ATTAQUES.

L'AGENCE S'APPUIE SUR UNE APPROCHE TRANSVERSE POUR ANTICIPER, PRÉVENIR ET RÉAGIR AUX CYBERATTAQUES AVEC POUR SOCLE UNE FORTE COORDINATION INTERMINISTÉRIELLE.

« Des attaques comme WannaCry sont la concrétisation de craintes que nous avions et de scénarios que nous avions imaginés.

En 2017, nous avons découvert une nouvelle victime de cyberattaques : la démocratie ! Désormais, à l'aune de ce qu'il s'est passé lors des élections présidentielles, aux États-Unis et en France, nos démocraties – et pas uniquement nos économies, nos sociétés, nos administrations – doivent poursuivre leur développement numérique en prenant en compte un risque numérique encore insuffisamment considéré. »

Guillaume Poupard

– DÉSTABILISATION DÉMOCRATIQUE : UNE ANNÉE À HAUT RISQUE

Au sortir de l'été 2016, la fin de la campagne présidentielle américaine est émaillée par des attaques cyber et la révélation d'e-mails de personnalités du Parti Démocrate. Au regard de ces événements et dans la perspective du scrutin national français, le SGDSN fait le choix d'organiser un séminaire de sensibilisation à l'acuité de la menace pour les partis politiques. Il s'agissait de la première élection majeure française sur laquelle portait un tel niveau de cybermenaces . À ce titre, les enjeux associés étaient multiples : assurer l'intégrité et la disponibilité du processus électoral tout en restant neutre vis-à-vis de celui-ci, assurer sa transparence pour maintenir la confiance dans l'élection tout en garantissant la confidentialité des votes, assurer une sécurité tout en maintenant l'accessibilité des systèmes.

COOPÉRATION INTERMINISTÉRIELLE

En s'appuyant sur toutes les compétences, où qu'elles soient, la stratégie, telle qu'élaborée par l'ANSSI, mise sur une coopération interministérielle forte ; un représentant du ministère de l'Intérieur était ainsi présent dans les locaux de l'agence tout au long des deux tours de scrutin.

« Ces élections ont vu la mise en place de dispositifs de synchronisation totalement inédits », résume Bruno Marescaux, sous-directeur du Centre opérationnel de la sécurité des systèmes d'information (COSSI). « Une variété exceptionnelle de métiers et de compétences ont été mobilisés au sein de l'agence, du SGDSN et des autorités impliquées dans le processus électoral pour assurer sa bonne tenue malgré le niveau élevé de cybermenaces. » Des actions ont dû être conduites auprès de publics jusqu'alors peu impliqués face aux cybermenaces (Conseil d'État, Conseil constitutionnel) ou ne faisant pas partie des bénéficiaires de l'agence (partis politiques). Parmi les nouveaux acteurs du processus électoral, citons la Commission Nationale de Contrôle de la Campagne électorale (CNCCEP) et la Haute Autorité pour la transparence de la vie publique (HATVP). Afin de créer un cadre normatif approprié, l'ANSSI et la CNCCEP ont mis en place un accord relatif aux modalités de saisine de l'agence en cas d'incident.

APPRÉHENDER LA SÉCURITÉ À LA LUMIÈRE DE L'ACTUALITÉ

Le 26 octobre 2016, le SGDSN convie à un séminaire l'ensemble des partis représentés aux parlements français et européen. L'objectif est clairement de mettre en perspective les événements survenus outre-Atlantique avec les risques que peuvent courir les organisations politiques dans le cadre des présidentielles françaises. Une actualité passée au crible et complétée par le partage de bonnes pratiques parmi lesquelles un volet juridique sur la répression des actes de cybermalveillance.

Outre le séminaire proposé aux partis politiques en octobre, l'ANSSI a poursuivi son travail de sensibilisation auprès des représentants des équipes de campagne des candidats ayant obtenu les 500 parrainages.

En marge de ce dialogue entretenu avec les partis, l'ANSSI a édité en avril le guide « Sécurité numérique – Bonnes pratiques et outils à l'usage des hautes autorités » qui invite les membres du Gouvernement à appliquer dés leur entrée en fonctions les bonnes pratiques élémentaires en matière de sécurité numérique et en vertu des obligations inhérentes à leurs fonctions. Une opération de sensibilisation renouvelée à l'approche des élections législatives puis sénatoriales avec l'édition de deux nouveaux guides s'adressant spécifiquement aux députés et sénateurs.

« AU-DELÀ DE L'ATTAQUE PROPREMENT DITE, NOUS DEVONS COMBATTRE L'INSTILLATION DU DOUTE QUI A DES EFFETS INSIDIEUX SUR LA STABILITÉ DE LA NATION. »

MOBILISATION DES FORCES OPÉRATIONNELLES

Alors qu'en externe, l'ANSSI déploie plusieurs actions de sensibilisation, en interne, la mobilisation s'organise. Dès le mois de mars, l'agence met en place une organisation de gestion de crise visant à prévenir ou gérer une crise de nature cyber : astreintes renforcées pendant trois mois, réunions hebdomadaires avec les équipes concernées, veille quotidienne au sein de l'équipe communication.

Outre la mise en place d'une procédure d'intervention en assistance d'un parti politique, l'ANSSI a aussi adressé un aspect moins prégnant mais primordial de la gestion de crise : veiller à ne communiquer qu'à l'issue d'une analyse technique approfondie assurée par les équipes compétentes de l'ANSSI pour communiquer l'information juste.

« EN MARS, L'ANSSI ORGANISE UN SÉMINAIRE DE SENSIBILISATION POUR LES CANDIDATS À LA PRÉSIDENTIELLE ET LEURS ÉQUIPES DE CAMPAGNE. ».

ANSSI, FORCE DE RECOMMANDATION : L'EXEMPLE DU VOTE ÉLECTRONIQUE

Le 6 mars, le gouvernement annonce l'abandon du vote électronique pour les Français de l'étranger à l'occasion des élections législatives de juin. Une décision prise en tenant compte des remarques formulées par l'ANSSI en date de février et tenant compte du niveau de menace extrêmement élevé susceptible d'affecter le bon déroulement du vote électronique.

Vincent Strubel, sous-directeur Expertise (SDE), résume : « Nous ne disposions pas d'une solution satisfaisante d'authentification sur la plateforme en cours de développement et surtout nous avions identifié un contexte particulier d'augmentation forte de la menace sur le processus électoral comme cela venait d'être vécu durant les élections américaines. Nous voulions à tout prix éviter de générer une défiance sur le vote électronique. » Cet avis technique réservé émis par l'ANSSI a été suivi par le gouvernement qui a pris la décision d'annuler le vote électronique.

SÉCURISER LES HAUTES AUTORITÉS : OSIRIS

Au cœur des réponses apportées par l'ANSSI pour garantir la continuité de l'État et prévenir le risque cyber figurent la création et le déploiement d'une solution de téléphonie sécurisée. Il s'agissait de fournir à la nouvelle équipe gouvernementale une solution de télécommunications adaptée à ses besoins et ergonomique.

À ce titre, le déploiement d'Osiris auprès des cabinets ministériels, de ceux du Premier ministre et de la Présidence a été un réel succès et un gage supplémentaire d'élévation du niveau de sécurité des systèmes d'information. (*Voir aussi p. 31*)

NOTPETYA

ATTAQUE À FINALITÉ DE SABOTAGE INÉDITE PAR SON MODE DE PROPAGATION ET L'AMPLEUR DU PÉRIMÈTRE TOUCHÉ.

IDENTIFICATION DE L'ATTAQUE

PARTENAIRES / RÉSEAU DES CSIRT
COLLABORATION INTERMINISTÉRIELLE
PRESTATAIRES QUALIFIÉS

+ CAPACITÉS DE DÉTECTION DES CYBERATTAQUES

+ VEILLE
- SUPERVISION
- PRESSE ET WEB

ANALYSE DES CONTENANTS

OBJECTIFS :

CONNAISSANCE ET ANTICIPATION DE LA MENACE

5 HEURES + TARD
ANALYSE DE LA MENACE

RÉACTION

Bulletins d'information du CERT-FR

COORDINATION
des services de l'État

INFORMATION
des entités concernées ou susceptibles de l'être

ASSISTANCE
Technique
Logistique
Juridique

COMMUNICATION
Opérationnelle
Interministérielle
Institutionnelle

Communiqués de presse et réseaux sociaux

REMÉDIATION

ACCOMPAGNER les victimes

CONSTRUIRE un plan de reprise d'activité

S'appuyant sur le code d'exploitation Eternal Blue publié par le groupe Shadow Brokers, le code malveillant NotPetya, en prenant l'apparence d'un rançongiciel, s'est répandu suite à la mise à jour d'un logiciel de comptabilité ukrainien, paralysant de nombreuses entités, principalement en Europe.

– WANNACRY ET NOTPETYA : UNE GESTION DE CRISE OPÉRATIONNELLE ET INSTITUTIONNELLE

WannaCry et NotPetya auront permis de mettre en lumière la menace cyber et d'illustrer le travail de l'ANSSI qui a développé des solutions agiles pour y répondre. L'agence s'impose *in fine* comme dépositaire d'un savoir-faire en termes de réaction opérationnelle et technique face à la crise mais aussi d'information vis-à-vis des différentes parties prenantes.

La gestion de la crise par l'ANSSI se conçoit en amont et en aval de celle-ci, intégrant dès le départ une dimension de communication, tant interne qu'externe. « Pour chaque situation, une cellule *ad hoc* est mise en place et implique une variété de profils complémentaires.», explique Benoît Nicolas, responsable d'opérations de cyberdéfense au sein du COSSI. Au cœur de métier d'expertise technique s'ajoutent des compétences transverses sur des aspects juridique, réglementaire, d'anticipation, de coordination et de communication.

« L'ANSSI fait intervenir des agents dont les compétences sont fonction des besoins nécessaires à la gestion de crise et la communication en fait partie », complète Anne-Charlotte Brou, responsable de bureau des relations presse et communication de crise. « Le traitement de l'information est primordial à plus d'un titre mais ne se conçoit pas dans la réaction. En règle générale, l'ANSSI observe une grande maîtrise dans la prise de parole. » Il est essentiel de distinguer les cibles, méthodes et objectifs de la communication opérationnelle de ceux de la communication plus institutionnelle. Si la première s'adresse à des acteurs de la sécurité des systèmes d'information par le biais des bulletins opérationnels que publie le CERT-FR et à des fins elles aussi opérationnelles, la seconde répond à d'autres exigences. Lors de la campagne d'attaques WannaCry par exemple, l'ANSSI, le plus souvent à travers la voix de son directeur général, a rappelé avec insistance sur le web et dans les médias les recommandations et bonnes pratiques à observer dans ce contexte. « L'attaque ayant été engagée le vendredi, il s'agissait dans ce cas d'alerter les victimes potentielles avant le lundi, jour où les messageries infectées, à leur ouverture, auraient pu propager le virus », explique Anne-Charlotte Brou.

S'adresser à des experts et responsables informatiques ou s'adresser à des autorités et citoyens sont deux exercices bien différents mais tout aussi essentiels. « C'est là tout le challenge de la communication de crise : adapter - sans la dénaturer - une communication opérationnelle nécessairement réactive à un public moins expert dont les attentes et les besoins diffèrent », appuie Benoît Nicolas. En résulte selon les cas, lorsque surviennent des attaques ou en temps de vigilance renforcée comme lors des processus électoraux, une communication à plusieurs vitesses et trajectoires dont la bonne conduite repose sur un échange permanent entre tous les acteurs de cette communication et plus largement de ces dispositifs au sein de l'ANSSI.

DIFFUSER PAR CAPILLARITÉ

L'ANSSI produit de nombreux documents (guides, fiches, communiqués) tout au long de l'année en s'appuyant sur les relais que sont les médias. L'objectif est de produire des messages justes, clairs et précis que l'utilisateur final va pouvoir appréhender. Ces échanges permanents entre l'opérationnel et l'institutionnel permettent d'obtenir cette clarté et lisibilité du message, jusques et y compris au niveau international. « Avec nos partenaires, homologues européens et internationaux, les échanges permanents et retours d'expérience donnent à nos communications une cohérence qui aide à parler d'une même voix pour avoir une force de frappe plus importante dans la diffusion de nos messages, par capillarité en quelque sorte. », explique Yves Verhoeven, sous directeur aux relations extérieures et à la coordination (RELEC)

UNE AGENCE D'EXCELLENCE ET DE RÉFÉRENCE

FACE À UNE MENACE DE PLUS EN PLUS SOPHISTIQUÉE, SOUVENT INDIRECTE ET RAREMENT CONÇUE SELON LE MÊME SCHÉMA, IL CONVIENT D'APPORTER DES RÉPONSES CONSTAMMENT ADAPTÉES, ÉLABORÉES PAR ET POUR L'ENSEMBLE DES ACTEURS CONCERNÉS DANS UN SOUCI D'EFFICIENCE.

C'EST TOUTE L'APPROCHE DE L'ANSSI QUI VISE À CONSTRUIRE UN VÉRITABLE ÉCOSYSTÈME AUTOUR DE LA FORMULATION DE DOCTRINES, D'AUDITS ET D'INSPECTIONS EN VUE D'AUGMENTER LE NIVEAU DE SÉCURITÉ GLOBAL DES ACTEURS LES PLUS SENSIBLES. PAR UN INVESTISSEMENT CONSTANT DANS LA R&D, L'ANSSI ASSURE LE MAINTIEN DE SES ÉQUIPES AU PLUS HAUT NIVEAU DE COMPÉTENCES, S'ÉRIGEANT AINSI EN VÉRITABLE PÔLE D'EXCELLENCE ET DE RÉFÉRENCE.

« L'ANSSI continue d'intégrer des profils techniques et opérationnels parmi les meilleurs au monde dans le domaine de la cybersécurité, capables de se confronter aux experts les plus pointus. Nous sommes amenés à travailler avec des secteurs d'activité divers et complexes comme le secteur bancaire, la santé ou le transport aérien qui nous obligent à disposer de compétences très variées, capables d'appréhender les codes et langages d'un secteur et ses cybermenaces spécifiques. Notre ambition est de parvenir à fondre dans un ensemble cohérent tous ces profils de compétences. »

Guillaume Poupard

– RESSOURCES HUMAINES : ANIMER LES COMPÉTENCES

Comment répondre efficacement et rapidement à une menace constante et mouvante ? En faisant de la formation et du recrutement une composante clé de la stratégie de l'ANSSI plaçant l'expertise – diverse et souvent atypique – au centre du jeu.

DES RECRUTEMENTS EN HAUSSE

2017 se caractérise par une hausse constante des effectifs avec 140 agents engagés, majoritairement dans le cœur de métier de sécurité des systèmes d'information.

Indéniablement, l'ANSSI attire : en 11 mois, pas moins de 8 000 *curriculum vitae* ont été traités par la sous-direction Affaires générales (SDAG) avant, pour les plus prometteurs d'entre eux, d'être adressés aux sous-directions employeuses.

D'où vient un tel engouement ? « L'ANSSI jouit d'une bonne image employeur. Pour tous ces candidats, un passage par l'agence représente la promesse d'exercer des missions passionnantes au service de la Nation et aux prises avec l'actualité. Á l'issue de cette expérience, c'est également la garantie de trouver un emploi de haut niveau au sein de structures où les compétences développées ici sont de plus en plus prisées », explique Michel Babeau, sous-directeur Affaires générales.

DES PROFILS INFORMATIQUES MAIS PAS SEULEMENT

L'ANSSI s'est construite sur la base d'un ADN technique reconnu, au niveau d'excellence et d'exigence jamais démenti. Un code génétique qui trouve désormais un terrain d'expression dans le domaine stratégique. Ces caractéristiques font de l'agence une institution à l'identité complexe capable de s'épanouir, de contribuer et de peser sur de nombreuses discussions. Cela amène naturellement l'ANSSI à s'entourer d'agents dotés d'une expertise de pointe dans leur domaine parfois très rare.

550
AGENTS

FIN 2017

8 000
CV
reçus

Âge moyen :
35 ans

140
recrutements

77% agents contractuels

14 500 heures de formation cumulées

29 heures de formation **par agent**
(moyenne)

Le point commun à toutes ces expertises demeure en tout état de cause « la créativité », souligne Vincent Strubel, sous-directeur Expertise. « À l'ANSSI, on gère des outils mais on en crée également de nouveaux, pour prévenir et réagir de façon agile aux menaces existantes et à venir. »

VIVIER DE TALENTS

L'ANSSI recrute de jeunes diplômés dès leur sortie d'école. « Nous sommes également présents sur plusieurs salons et colloques afin de présenter l'activité de l'ANSSI. » En 2017, le bureau des Ressources humaines a ainsi participé à 15 événements et forums afin de présenter l'agence et nouer des liens avec de potentiels candidats.

L'ANSSI s'appuie sur des plateformes numériques pour dénicher et se faire connaître des profils les plus pertinents comme LinkedIn dont le compte est suivi par plus de 20 000 personnes.

FORMATION ET MOBILITÉ INTERNE POUR RESTER À L'ÉTAT DE L'ART

Rester à l'état de l'art passe donc par des recrutements permanents mais également par la formation interne, qu'elle se réalise par le suivi de programmes ou par l'expérience acquise dans de nouvelles fonctions.

En 2017, l'ANSSI a, en moyenne, proposé 29 heures de formation par agent. Les formations que suivent les agents portent essentiellement sur des spécialités liées à la sécurité des systèmes d'information et qui, de fait, participent à la mobilité interne.

Au fil des ans, l'ANSSI a ainsi placé la gestion de la compétence au cœur même de son processus de fonctionnement. Cela lui permet de traiter de manière transverse des sujets aussi diversifiés que la recherche fondamentale, le pilotage de projets informatiques, la conception et la gestion d'architectures réseaux, la négociation juridique sur des aspects réglementaires, la communication, la coopération internationale, etc.

L'ANSSI bénéficie également de cette incitation à la formation et à la mobilité. Après leur passage à l'ANSSI, les informaticiens de haut niveau formés à la cybersécurité sont en mesure d'inciter les entreprises qu'ils intègrent à se prémunir des cybermenaces en participant au renforcement de la sécurité de leurs systèmes, élevant *de facto* le niveau général de la cybersécurité sur le territoire.

UNE DÉMARCHE QUALITÉ POUR ACCOMPAGNER LA PERFORMANCE

La nécessité de déployer une démarche qualité s'est fait jour en 2015. Deux ans plus tard, les travaux menés par le bureau dédié ont abouti à la cartographie de tous les processus de l'agence. Ceux-ci ont été déclinés en plans d'actions, affinés au niveau de chaque sous-direction. Ces parcours, ces actions stratégiques et leurs indicateurs associés servent de base à chacune des sous-directions pour expliquer simplement ce pour quoi et vers quoi chaque agent travaille quotidiennement.

2 questions à ...

Véronique Brunet, déléguée ANSSI à la sécurité numérique en région Bourgogne–Franche–Comté

Quand on parle de mobilité professionnelle et de diversité des profils au sein de l'ANSSI, le parcours de Véronique Brunet, chef de projet du MOOC SecNumacadémie et, depuis décembre 2017, déléguée à la sécurité numérique en région Bourgogne–Franche–Comté est un cas tout à fait intéressant.

QUEL A ÉTÉ VOTRE PARCOURS PROFESSIONNEL AVANT D'INTÉGRER L'ANSSI ?

Dans la première partie de ma carrière, j'ai dirigé durant quinze ans une imprimerie en Franche–Comté, ma région d'origine. Ayant perçu le basculement de mon industrie vers le numérique, j'ai d'abord entamé une reconversion vers le *digital learning* et son ingénierie pédagogique via un diplôme de Master. J'ai pris en charge un premier projet de *e-learning* auprès des pilotes de chasse taïwanais qui venaient s'entraîner en France avec le désir d'apprendre à parler le français. Par la suite, j'ai piloté le projet du MOOC de l'ANSSI, SecNum*academie*.
Et, fin 2017, le MOOC étant maintenant sur les rails, je me suis vue proposer un poste de déléguée ANSSI à la sécurité numérique pour ma région, la Bourgogne-Franche-Comté.

COMMENT S'INSTALLE-T-ON DANS UN RÔLE DE DÉLÉGUÉE DE L'ANSSI EN RÉGION ?

Du fait de mon parcours professionnel précédent, je connais déjà en partie les acteurs du milieu économique en Bourgogne–Franche–Comté. À mon arrivée, j'ai commencé par nouer des contacts avec les délégués à l'information stratégique et à la sécurité économiques (DISSE), la Gendarmerie, la DGSI, les universités, etc., afin d'envisager des actions communes de sensibilisation à la sécurité des systèmes d'information que nous pourrons réaliser en 2018 auprès des collectivités territoriales, des entreprises ou encore des étudiants.

Je trouve très intéressant de retourner dans ma région d'origine avec une nouvelle perspective : celle de représenter l'ANSSI. D'ailleurs, à l'issue de mes premiers contacts, j'ai déjà constaté que l'agence était très attendue par les décideurs locaux. Je suis à peine en poste et déjà sollicitée pour participer à des rencontres professionnelles. L'une de mes missions est également de nouer et d'entretenir des liens avec l'ensemble des acteurs régionaux, afin de pouvoir, le moment venu, accompagner les coordinateurs sectoriels de l'ANSSI sur le terrain et expliquer de quelle manière intervient l'agence auprès de ses bénéficiaires et partenaires tels que l'État, les opérateurs d'importance vitale (OIV), bientôt les opérateurs de services essentiels (OSE) et de nouveaux dispositifs élargis comme la plateforme Cybermalveillance.gouv.fr.

UN SUPPORT JURIDIQUE NÉCESSAIREMENT SPÉCIALISÉ

Depuis sa création, le bureau des Affaires juridiques a vu son implication croître au rythme des mutations de la menace et du périmètre d'intervention de l'agence. Chaque événement, prise de position ou encore intervention opérationnelle auxquels l'ANSSI prend part doit en effet se réaliser conformément à un cadre législatif et réglementaire appelant, sans cesse, des adaptations. Le support juridique requiert agilité et sagacité tant la matière est spécifique et nécessite une compétence de pointe.

En 2017, près de 150 sollicitations requérant une expertise juridique ont été formulées. Parmi elles, 80 relèvent de conventions, 63 de conseils et 5 de réglementations. L'ANSSI apporte à ses bénéficiaires une expertise dans la mise en place d'accords de confidentialité, conventions d'audit et inspection, de détection, d'accords internationaux ou encore d'accords de consortium. Elle sécurise également les opérations de l'agence par son activité de conseil. Enfin, le bureau a participé aux travaux de l'agence dans le domaine réglementaire, notamment sur des dossiers relatifs à la transposition de la directive NIS ou encore les textes d'application de la loi pour une République numérique.

– UN ÉCOSYSTÈME À ANIMER

FAIRE DE LA SÉCURITÉ NUMÉRIQUE UN ENJEU COMPRIS ET PARTAGÉ

Avec l'extension du périmètre de son action et l'arrivée prochaine de nouveaux bénéficiaires, l'agence doit faire preuve d'ouverture et considérer l'émergence voire la création de nouvelles compétences et expertises comme intrinsèques à son positionnement.

« Il nous faut nous ouvrir à de nouveaux métiers qui sont la conséquence directe de nouveaux usages », explique Guillaume Poupard. « Pour apporter une réponse adaptée à chaque besoin, il nous faut parler le même langage que nos interlocuteurs. Cela vaut pour les relations internationales mais aussi – et pas seulement – pour les multiples secteurs d'activités que nous adressons. »

C'est notamment sur ce terrain que s'illustre l'activité des coordinateurs sectoriels dont la mission est d'améliorer la prise en compte des enjeux de sécurité du numérique selon une logique sectorielle. « La notion de cybersécurité dans le secteur bancaire est bien différente de celle du transport aérien ; ce sont d'autres langages, d'autres problématique, d'autres menaces. » Un dialogue permis par une connaissance pointue, pour chaque secteur, de ses métiers, de ses principaux acteurs et de son niveau de maturité en matière de sécurité des systèmes d'information.

LA PRÉVENTION ET L'ANTICIPATION COMME PRÉREQUIS OPÉRATIONNELS

Face aux cyberattaques, l'ANSSI a développé une méthode sûre en matière d'audit, d'inspection, de sécurisation et d'assistance sur le long terme que le COSSI met en œuvre avec le soutien des autres sous-directions afin de pouvoir, en cas d'attaque, réagir rapidement tout en proposant des audits préventifs.

En 2017, l'ANSSI a réalisé 63 prestations d'audit de sécurité de systèmes d'information, à travers l'inspection de ministères, l'audit d'opérateurs d'importance vitale et des audits sur demande. Il est intéressant de noter que le nombre d'audits à la demande est en augmentation, passant de 60 à 65 % de la charge totale des prestations du COSSI.

Sur l'année, les prestations d'audit ont bénéficié en premier lieu aux institutions, ministères et autorités indépendantes (58 % de l'ensemble des audits), principalement pour la Présidence de la République, les services du Premier ministre et les ministères des Armées, des Finances, de l'Intérieur, de l'Environnement et de l'Éducation.

Les opérateurs d'importance vitale, répartis en douze secteurs, représentent près de la moitié des activités d'audit de l'agence.

LES 12 SECTEURS D'ACTIVITÉ D'IMPORTANCE VITALE

SECTEURS DE LA VIE ÉCONOMIQUE ET SOCIALE DE LA NATION

Énergie, communications électroniques, audiovisuel et information, transports, finances, industrie

SECTEURS ÉTATIQUES

Activités civiles de l'État, activités militaires de l'État, activités judiciaires, espace et recherche

SECTEURS DE LA PROTECTION DES CITOYENS

Santé, gestion de l'eau, alimentation

« LA CYBERSÉCURITÉ NE DOIT NI NE PEUT FREINER LA NUMÉRISATION CROISSANTE DES ACTIVITÉS HUMAINES. IL FAUT ACCOMPAGNER CES INNOVATIONS PAR LE RESPECT DE PRÉCEPTES QUI ONT FAIT LEURS PREUVES. »

DES VISAS DE SÉCURITÉ POUR INSTAURER LA CONFIANCE

Annoncés lors des Assises de la sécurité et des systèmes d'information organisées à Monaco en octobre et officiellement lancés au Forum International de la Cybersécurité (FIC) en janvier 2018, les « Visas de sécurité » délivrés par l'ANSSI sont un maillon structurant dans le développement d'un écosystème de confiance.

Ces visas permettent d'identifier facilement une solution dont le niveau de sécurité est attesté robuste par l'agence à l'issue d'un processus de qualification ou de certification clair et précis. Ils sont aussi un atout de compétitivité pour les fournisseurs de produits ou de services de sécurité qui disposent ainsi d'un levier concurrentiel fort.

Suivant les tendances d'évolution du secteur informatique vers une économie du service, l'ANSSI qualifie des prestataires de services en matière de cybersécurité. Plus de six typologies de services différents font l'objet d'un Visa de sécurité. Parmi les services qualifiés les plus récents, on peut citer : les prestataires de détection des incidents de sécurité (PDIS), les prestataires de réponse aux incidents de sécurité (PRIS), les prestataires d'audit de la SSI et les prestataires de service informatique dans le nuage ou *cloud computing* (SecNumCloud). Dans ce dernier cas, l'obtention d'un tel visa représente un gage de sécurité fort pour les organisations qui feront le choix d'externaliser leurs données auprès d'un prestataire qualifié. À l'heure où les attaques se font de plus en plus indirectes (*Voir : grandes tendances du cyberpanorama p.8*) et loin de vouloir freiner le développement de telles solutions, la qualification de prestataires de services informatiques en nuage par l'ANSSI illustre une nouvelle fois la volonté de l'agence d'accompagner le développement de solutions innovantes mettant en œuvre une sécurité native.

En 2017, les experts de l'ANSSI ont poursuivi leur travail de qualification de produits et de services de sécurité. Parmi cet arsenal, on peut citer la publication le 11 octobre 2017 du référentiel d'exigences pour les prestataires de réponse aux incidents de sécurité. En trois mois, six prestataires ont déposé une demande de qualification actuellement en cours.

« FAIRE TRAVAILLER ENSEMBLE CEUX QUI FONT LE NUMÉRIQUE ET CEUX QUI FONT LA SÉCURITÉ NUMÉRIQUE. »

En 2017, sept prestataires de détection d'incidents de sécurité sont entrés en qualification. « Les sondes de détection qualifiées par l'ANSSI d'une part, la qualification des PDIS d'autre part, sont très attendues de la part des OIV » confie Vincent Strubel. « C'est un enjeu de défense et la détection devient un sujet à part entière pour tous ces opérateurs. »

L'agence délivre également une qualification relative aux prestataires d'audit de la sécurité des systèmes d'information. « L'offre PASSI, déjà large, semble bien acceptée et appréhendée par les OIV, même si la demande, de plus en plus grande, met au défi ce processus au long cours pour disposer de suffisamment de prestataires pour y répondre.»

CONSEILLER ET ACCOMPAGNER

L'ANSSI renforce l'accompagnement technique assuré auprès des administrations et opérateurs critiques. Au sein de la sous-direction Expertise, cette mission est plus particulièrement portée par la division Assistance technique. Cet accompagnement des bénéficiaires de l'agence se traduit par des actions de conseil, de suivi et de soutien techniques dans la conception et la mise en œuvre de leurs systèmes d'information les plus critiques.

Les agents de la division apportent également leur support dans la mise en œuvre des plans d'action issus des audits ou inspections effectués par un autre service. Ceci afin de garantir la continuité de l'accompagnement et émettre avis et recommandations associés.

« Au fil du temps, souligne Shah Mohsin Wahed, expert en sécurisation des infrastructures, les OIV et les administrations avec lesquels nous avons l'habitude de travailler ont compris l'intérêt qu'il y avait à nous consulter très tôt dans un projet de système d'information. Cela leur évite d'être contraints de repenser l'architecture d'un système de fond en comble en cas de vulnérabilité découverte sur le tard. »

Une expertise technique et un rapport privilégié avec le terrain qui font de ces experts des contributeurs actifs dans l'élaboration des guides techniques édités par l'agence *(Voir : bibliographie p. 48)*.

3 questions à ...

Shah Mohsin Wahed, expert en sécurisation des infrastructures au sein de la division Assistance technique

COMMENT AVEZ-VOUS INTÉGRÉ L'ANSSI ?

Lorsqu'en 2013 j'ai envoyé ma candidature à un poste qui s'ouvrait à l'ANSSI, je disposais alors d'une expérience de plus de dix ans en tant qu'ingénieur systèmes et réseaux au sein d'une start-up puis d'un important opérateur télécom français, pour lequel je m'occupais de l'architecture de stockage. Aujourd'hui, mes interventions m'amènent à accompagner les OIV et les ministères sur des aspects techniques mais pas seulement. La sensibilisation et le partage des bonnes pratiques font partie intégrante de cette démarche qui se matérialise notamment dans les publications de l'ANSSI et auxquelles je contribue également.

QUELS SONT LES AUTRES PROFILS DE COMPÉTENCE PRÉSENTS AU SEIN DE VOTRE DIVISION ?

La division Assistance technique est un service d'une trentaine de personnes aux profils très variés. C'est ce qui fait sa richesse et permet une réelle émulation. On y trouve des ingénieurs en matière de systèmes d'information, certains expérimentés, d'autres jeunes diplômés issus d'écoles d'ingénieurs, des militaires et des ingénieurs systèmes qui ont travaillé dans l'industrie…

EN QUOI CONSISTE VOTRE MISSION AU SEIN DE LA DIVISION ?

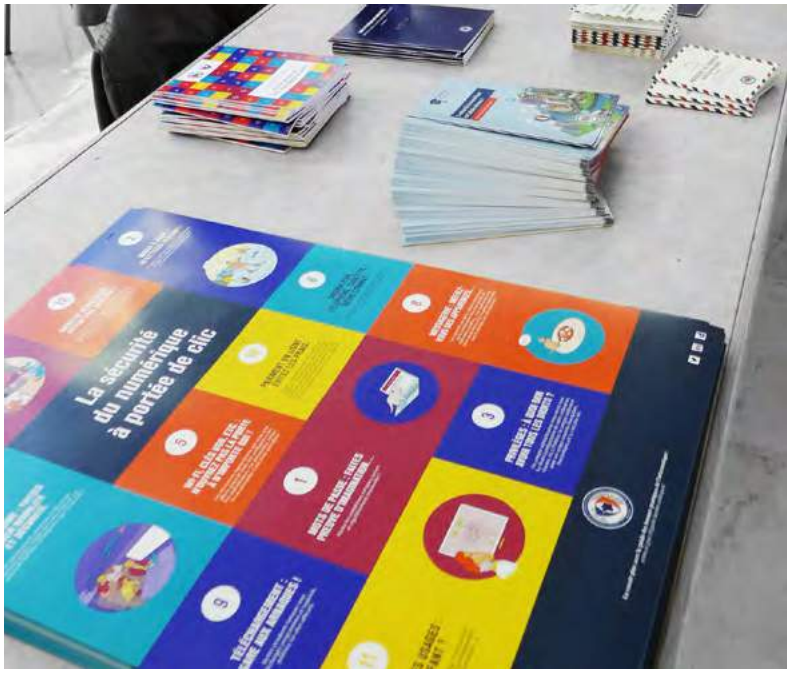
Je fais du conseil sur la sécurisation des infrastructures des centres de données, comme par exemple les infrastructures de virtualisation, de stockage ou de sauvegarde. J'accompagne les organisations qui nous consultent dans la sécurisation des centres de données et de l'hébergement dans le *cloud*. Nous alertons aussi sur la nécessité de considérer la sécurité d'un système d'information dans son ensemble et de ne pas négliger la sécurisation des parties les moins sensibles, car c'est souvent là que se trouvent les failles de sécurité par lesquelles se réalisent les cyberattaques. ⬢

UNE DOCTRINE QUI SE MATÉRIALISE

75. C'est le nombre de documents (guides techniques, articles scientifiques, documents institutionnels, supports de sensibilisation – *Voir : bibliographie p.48*) édités par l'ANSSI en 2017. Parmi eux, on dénombre plus d'une dizaine de nouveaux guides techniques dont le guide *Restreindre la collecte de données sous Windows 10* téléchargé à plus de 68 000 exemplaires. Des guides techniques régulièrement mis à jour et dont l'édition est fonction d'une priorisation des besoins permise par un dialogue permanent avec les destinataires de cette documentation à savoir les développeurs, administrateurs, RSSI, DSI et utilisateurs. Les documents plus généralistes de partage de bonnes pratiques auprès de publics ciblés répondent eux aussi à cette exigence d'ancrage dans l'actualité. À titre d'exemple, la version mise à jour du *Guide d'hygiène informatique* en français enregistre en 2017 plus de 340 000 téléchargements, devenant ainsi la publication la plus téléchargée de l'année.

« LES SYSTÈMES ONT ÉVOLUÉ, LES PRATIQUES ONT CHANGÉ, LES ATTAQUES SE SONT MULTIPLIÉES ET COMPLEXIFIÉES. »

Depuis la première version du guide parue en 2012, les systèmes ont évolué, les pratiques ont changé (la mobilité par exemple), les attaques se sont multipliées et complexifiées. Il était donc essentiel de publier une version actualisée de ce guide, une posture adaptée aux nouveaux usages mais aussi aux nouvelles menaces.



La gestion de ce patrimoine éditorial est animée et coordonnée par un comité éditorial composé de représentants de chaque sous-direction. Ainsi, tout nouveau document bénéficie de retours issus de différentes expertises, assurément complémentaires et garantes de la cohérence et de la conformité des contenus avec la doctrine et la stratégie de l'agence.

Si cette littérature technique fait référence au niveau national, elle s'exporte également à l'international. Une tendance que l'ANSSI encourage en traduisant de plus en plus systématiquement ces documents, à l'image par exemple du rapport annuel de l'Observatoire de la résilience de l'Internet français que l'ANSSI co-édite depuis sept ans avec l'AFNIC (gestionnaire des noms de domaine en France). À la lumière des résultats de l'année écoulée, ce rapport dresse un panorama complet des points de vulnérabilité de l'Internet français. Les ingénieurs de l'ANSSI y ont entre autres la mission d'analyser avec l'aide des opérateurs de télécommunications la vulnérabilité des nœuds d'interconnexion IP présents dans l'hexagone.

7 LABORATOIRES AUX DOMAINES D'EXPERTISE VARIÉS ET AUX COMPÉTENCES RECONNUES

- *Architectures matérielles et logicielles*
- *Cryptographie*
- *Exploration et recherche en détection*
- *Sécurité des réseaux et protocoles*
- *Sécurité des composants*
- *Sécurité des technologies sans fil*
- *Sécurité du logiciel*

Contributions open-source **34** *projets référencés sur le Github de l'ANSSI*

Contributions au noyau et aux distributions Linux

46 *articles scientifiques présentés dans* **+ de 20** *conférences nationales et internationales ou publiés dans des journaux à comité de lecture*

Dispense de cours dans le cadre de formations diplômantes

POUR ACCOMPLIR LEURS MISSIONS D'EXPERTISE ET DE R&D

EXEMPLES DE TRAVAUX MENÉS

- *Élaboration de solutions sécurisées et partage du code source (CLIP OS)*
- *Contribution à l'élaboration de guides et référentiels techniques*
- *Évaluation de produits (apport d'expertise dans le cadre des procédures de qualification, certification et agrément)*
- *Audit*
- *Observatoire de la résilience de l'Internet français*
- *Suivi des standards internationaux pour les communications sécurisées*
- *Développement de preuves de concept*
- *Prototypage*
- *Transfert de compétences*

SUJETS ÉMERGENTS

- *Détection*
- *Sécurité des systèmes industriels*
- *Objets connectés et systèmes embarqués*
- *Sécurité électromagnétique*
- *Vulnérabilités des processeurs*

2E CONTRIBUTEUR *à la communauté open source après ETALAB*

EN ÉCHANGE PERMANENT AVEC

5 SOUS-DIRECTIONS DE L'ANSSI

SUPPORT OPÉRATIONNEL
DOSSIERS STRATÉGIQUES ET INTERNATIONAUX
VISAS DE SÉCURITÉ
FORMATION
ETC.

BÉNÉFICIAIRES DE L'AGENCE

ÉTAT
ENTREPRISES CRITIQUES

INDUSTRIE / SECTEURS

SEMI-CONDUCTEUR
TÉLÉCOMMUNICATIONS
SANTÉ
DÉFENSE
ETC.

MONDE ACADÉMIQUE

GRANDES ÉCOLES
CONFÉRENCES SCIENTIFIQUES NATIONALES ET INTERNATIONALES
INSTITUTS DE RECHERCHE
UNIVERSITÉS

PARTAGER LA CONNAISSANCE POUR RENFORCER LA CAPACITÉ DE DÉTECTION DES ATTAQUES

Pour faire face à la propagation de virus non-discriminants à l'échelle planétaire comme WannaCry ou NotPetya ou la mise à jour de logiciels compromis notamment, l'ANSSI agit sur plusieurs leviers au premier rang desquels figure la détection des attaques. Un enjeu prioritaire pour l'agence qui souhaite effectuer un saut capacitaire en la matière pour élever le niveau de cybersécurité en France.

Si l'agence développe sans cesse ses connaissances techniques sur les modes opératoires et les attaquants eux-mêmes afin d'adapter ses capacités de détection, le partage de ces connaissances avec d'autres acteurs apparait comme un élément clé de ce renforcement. Dans cette perspective, les prestataires de détection d'incidents de sécurité qualifiés par l'ANSSI, les bénéficiaires de ces services et les interlocuteurs de l'agence au niveau interministériel ont, par leurs connaissances et retours d'expérience, un rôle majeur à jouer dans cet effort.

L'ANSSI OUVRE LE CODE-SOURCE DE CLIP OS

Dans le cadre de travaux de recherche et le développement de plateformes de communication sécurisées pour l'État et les OIV, l'ANSSI a conçu son propre système d'exploitation, Clip OS. Avec une conception entamée il y a près de 10 ans et depuis continuellement amélioré, Clip OS est passé du stade de prototype à celui d'outil effectivement déployé au sein de l'administration et plus récemment chez certains OIV. Dans la continuité de sa mission de promotion et de partage des bonnes pratiques en matière de sécurité numérique, l'ANSSI met maintenant progressivement à disposition de la communauté des développeurs le code-source de Clip OS. Cette action s'inscrit dans la logique de transparence et de modernisation numérique souhaitée par l'État. Une initiative qui n'est pas isolée dans la démarche de l'ANSSI : « En matière de SSI, l'agence est ainsi le 2e service public contributeur à la communauté open source après ETALAB », souligne Vincent Strubel, sous-directeur Expertise.

– SECDROID, OSIRIS : AU CŒUR DES COMMUNICATIONS SÉCURISÉES DE L'ÉTAT

En 2017, l'activité de la sous-direction Systèmes d'information sécurisés (SIS) s'est illustrée par la conduite de deux projets d'envergure nécessitant une coopération interministérielle forte et en prise directe avec l'actualité.

Citons d'abord le déploiement d'un nouveau système de téléphonie fixe sécurisée de niveau « Confidentiel Défense » baptisé Osiris mais aussi la poursuite du déploiement de terminaux Secdroid auprès des forces de l'ordre au terme d'une phase d'expérimentation dans les Hauts-de-France initiée en 2016 aux côtés de la Gendarmerie nationale.

NÉO : LA TRANSFORMATION NUMÉRIQUE DE L'ÉTAT VUE DU TERRAIN

Ce sont ainsi pas moins de 80 000 terminaux Secdroid qui ont été déployés sur le territoire national dans le cadre du dispositif NÉO qui regroupe les programmes NÉOgend et NÉOpol visant respectivement à équiper gendarmes et policiers. Dans un discours du Président de la République aux forces de sécurité intérieure du 19 octobre 2017, Emmanuel Macron citait NÉO en rappelant son souhait que « la police et la gendarmerie prennent résolument le virage de la transformation numérique. […] Il faudra faciliter davantage l'accès au service public de la sécurité en tirant pleinement parti des possibilités et des opportunités ouvertes par le numérique. »

En permettant une nouvelle forme de proximité avec la population pour les forces de l'ordre, NÉO répond à leurs besoins de mobilité et de large accès aux applications métier spécifiques à l'exercice de leurs missions, le tout dans un environnement entièrement sécurisé.

384 POSTES
OSIRIS
10
MINISTÈRES

1 650 POSTES
ISIS
374
SITES

2017 **80 000**
POSTES
SECDROID
DÉPLOYÉS

3 382
LIGNES
RIMBAUD
4 803
ABONNÉS

2 125
SITES
RIMBAUD

3 325
TEOREM

OSIRIS : UNE ORCHESTRATION RÉUSSIE

Autre projet majeur, Osiris. Un chantier imposant, tant par l'exigence du cahier des charges que par son calendrier serré et la multiplicité des acteurs à coordonner. Mis en service en mai 2017 pour l'arrivée des nouvelles équipes gouvernementales, le dispositif a relevé plusieurs défis, « à commencer par celui de l'ergonomie, car l'expérience montre que lorsqu'un terminal sécurisé est peu intuitif et difficile à prendre en main, la tentation est grande de lui préférer d'autres circuits moins protégés, au détriment de la sécurité globale », souligne Stéphane Gobert, chef adjoint de la division Pilotage des systèmes d'information.

Pour garantir à la fois l'ergonomie, la protection des communications de niveau « Confidentiel Défense » et l'interopérabilité avec des solutions offrant un autre niveau de service comme Teorem afin d'assurer la continuité des communications de l'État, une dizaine d'agents aux profils complémentaires se sont investis dans ce projet. « Il fallait non seulement sécuriser au maximum le téléphone mais également l'architecture du système dont le chiffreur gouvernemental qui représente le cœur de la sécurité des communications », explique Christophe Benoît, ingénieur Réseaux à l'ANSSI sollicité durant l'été 2016 pour copiloter le projet. Un volet technique auquel s'ajoutent de multiples paramètres nécessitant l'intervention de nombreux autres acteurs à l'échelle interministérielle avant d'aboutir à l'installation effective des systèmes.

Les premiers déploiements ont été opérés à partir de mai 2017 et, au 31 décembre, ce sont quelque 384 postes qui ont été installés dans une dizaine de cabinets ministériels, auxquels il convient d'ajouter les cabinets du Premier ministre et de la Présidence de la République. « Le nombre de téléphones installés est un élément important mais cela ne représente pas toute la complexité de la mise en œuvre de ce chantier », précise Christophe Benoît.

« Un élément plus factuel, complète Stéphane Gobert, est qu'avec dix fois moins d'abonnés par rapport à l'ancien système, nous avons constaté qu'il y avait dix fois plus de minutes de communication. Il s'agit donc d'un taux d'adoption du système bien meilleur que le précédent. »

2018 verra l'intensification de ce déploiement dans les cabinets des autres ministères mais également dans ceux de certains services déconcentrés de l'État (préfectures, etc.).

NÉOGEND : UN DÉPLOIEMENT D'ENVERGURE

Le Lieutenant-colonel Olivier Langou a supervisé l'opération de déploiement de terminaux mobiles Secdroid au sein des équipes de gendarmerie et de police dans le cadre du dispositif NÉO.

3 questions à ...

Le Lieutenant-colonel Olivier Langou

Á QUELS BESOINS MÉTIERS LE DISPOSITIF NÉOGEND RÉPOND-IL ?

NÉOgend permet de gagner en efficacité et performance en donnant accès aux applications et données du système d'information sur le terrain et ainsi de gagner en proximité avec le citoyen.

QUELLES ONT ÉTÉ LES GRANDES ÉTAPES DE MISE EN PLACE D'UNE TELLE SOLUTION ?

Trois gendarmes étaient détachés à temps partiel à l'ANSSI avec des points réguliers organisés. Nous avons ainsi établi un dialogue constant avec un partage des informations en temps réel. Nous avons tout d'abord réalisé en 2015 une expérimentation de la solution avec 1 200 terminaux déployés dans le Nord de la France pour la Gendarmerie nationale et 500 terminaux en région parisienne pour la Police nationale.

En 2016, nous avons changé d'échelle avec une préfiguration du déploiement complet et l'installation de 12 000 terminaux en Bourgogne pour la gendarmerie et dans le département du Lot pour la police. En 2017 enfin, ce sont 80 000 terminaux supplémentaires qui ont été déployés sur l'ensemble de la métropole et les outre-mer.

QUEL EST LE PREMIER BILAN DE CE DÉPLOIEMENT ?

À ce jour, 77 847 terminaux ont été déployés. Restent les 3 370 terminaux des outre-mer à couvrir. Ces terminaux mobiles s'ajoutent aux 12 000 déjà en place. Les retours des gendarmes comme des policiers sont très positifs.

La principale réussite est d'avoir maintenu en 2017 des projections calendaires difficiles. Et, d'ailleurs, ce n'est pas fini, car un nouveau déploiement de 22 000 terminaux est prévu pour la Police nationale.

La réussite de NÉOgend est directement liée à la capacité de l'ANSSI à livrer un système d'exploitation et des applications opérationnelles ainsi qu'à la capacité des techniciens locaux à s'approprier l'outil. Le seul point d'amélioration est sans doute notre capacité à prévoir une équipe technique capable d'être projetée rapidement sur le terrain pour lever des difficultés locales.

En 2018, de nombreuses applications sont en cours de développement pour optimiser l'usage des smartphones. ⬢

« AVEC OSIRIS, L'ANSSI CONFIRME SON RÔLE D'INTÉGRATEUR DE SOLUTIONS SÉCURISÉES. »

UNE APPROCHE OUVERTE ET CONCERTÉE

FACE À UNE MENACE QUI SE JOUE DES FRONTIÈRES ET À DES ATTAQUES QUI NE SE CANTONNENT PLUS À UN SEUL SECTEUR ÉCONOMIQUE NI UNIQUEMENT AUX GRANDES ENTREPRISES, LE RISQUE CYBER N'A JAMAIS ÉTÉ AUSSI PROTÉIFORME. ON DOIT CETTE PRISE DE CONSCIENCE QUI GRANDIT AU TRAVAIL DE L'ANSSI QUI A NOTAMMENT MIS EN PLACE CETTE ANNÉE UN FAISCEAU D'OUTILS DE SENSIBILISATION, D'INFORMATION ET DE PRÉVENTION VISANT À DÉVELOPPER LA CONNAISSANCE DU RISQUE CYBER. DANS LE MÊME TEMPS, L'AGENCE ENTRETIENT DES RELATIONS PRIVILÉGIÉES AVEC CERTAINS ÉTATS TOUT EN POURSUIVANT SON TRAVAIL D'ÉCHANGES ET DE COOPÉRATION AVEC D'AUTRES.

UNE STRATÉGIE TENDUE VERS UN SEUL ET UNIQUE BUT : CONSTRUIRE ENSEMBLE LA SÉCURITÉ NUMÉRIQUE DE DEMAIN.

« Il y a donc une véritable nécessité à développer une approche concertée de la cybersécurité en Europe d'abord, mais également au-delà. La sécurité est un continuum.

En matière de sécurité numérique, la responsabilité est nécessairement partagée : responsabilité de l'État dans la protection des citoyens et des infrastructures critiques, dans l'organisation de la défense et de la sécurité des systèmes d'information ; responsabilité des acteurs économiques dans la sécurité des produits et services qu'ils proposent ; responsabilité des citoyens dans l'exercice de leur vie numérique. »

Guillaume Poupard

– VERS UNE PRISE DE CONSCIENCE ACCRUE DU RISQUE CYBER

L'année 2017 aura une nouvelle fois prouvé l'urgente nécessité de s'emparer des questions de sécurité numérique. Cette année a en effet été marquée par de nombreuses attaques dont les modes opératoires soulignent un niveau de préparation conséquent et une certaine forme de créativité. C'est le cas avec NotPetya : l'attaquant n'a pas frappé directement les victimes, mais le fournisseur d'un logiciel de comptabilité très utilisé en Ukraine. En forçant celui-ci à pousser une mise à jour, piégée, mais légitime, l'attaquant est parvenu à toucher l'ensemble des entreprises implantées en Ukraine utilisatrices de ce logiciel et, par effet boule de neige, de nombreuses autres organisations liées à ces premières victimes.

Pour s'en prémunir ou limiter les effets d'une telle attaque, l'ANSSI est intervenue pour responsabiliser les organisations comme les citoyens par le partage de mesures préventives et réactives. Un effort de sensibilisation dont s'empare chaque agent et qui irrigue chaque mission.

COUP DE PROJECTEUR SUR LA CYBERSÉCURITÉ

L'ANSSI a coordonné plusieurs événements internationaux et multiplié en 2017 sa présence sur des rencontres professionnelles afin de promouvoir la cybersécurité. En quelques chiffres, cela représente plus de 1 000 interventions en régions et la participation à près d'une centaine d'événements nationaux (conférences, colloques, évènements territoriaux, séminaires, forums) et 30 à l'échelle internationale.

Parmi ces événements particulièrement mobilisateurs et novateurs, citons la tenue les 6 et 7 avril de la Conférence internationale « Construire la paix et la sécurité internationales de la société numérique » à l'Unesco. Organisé sous l'impulsion du secrétaire général de la défense et de la sécurité nationale et en partenariat avec le ministère de l'Europe et des Affaires étrangères, l'événement a rassemblé pendant deux jours des représentants de l'économie numérique, d'organisations internationales, d'ONG, des chercheurs et des diplomates venus des cinq continents pour échanger sur les moyens de faire d'Internet un espace de paix et de sécurité où le droit international s'appliquerait.

À l'initiative de l'ENISA (*European Union Agency for Network and Information Security)*, l'agence européenne chargée de la sécurité des réseaux et de l'information, l'ANSSI a coordonné sur le plan national l'édition 2017 du Mois européen de la cybersécurité, un événement européen de sensibilisation organisé chaque année en octobre. « Sensibilisation pour tous, car la cybersécurité n'est pas uniquement une affaire d'experts , rappelle Guillaume Poupard. Les dirigeants, les salariés et les citoyens faisant usage de systèmes d'information sont également concernés. Sans avoir vocation à devenir experte en matière de cybersécurité, chaque organisation doit pouvoir se protéger à son niveau et de manière autonome. » En parlant d'une seule voix un mois durant, les acteurs publics et associatifs français ont ainsi saisi l'opportunité de multiplier les initiatives à destination des professionnels, des particuliers et des étudiants.

L'agence a participé à la 9e édition du Forum International de la Cybersécurité les 24 et 25 janvier 2017 à Lille ; un moment de réflexion autant que de prospective. L'ANSSI, par la voix de son directeur général, y est intervenue lors de la conférence « THE DAY AFTER : quelle cybersécurité à l'horizon 2020 ? » Elle a également collaboré à de nombreux ateliers sur des thèmes tels que la sécurisation du *cloud*, le véhicule connecté, la gestion de crise cyber à l'échelle européenne et les questions de formation à la cybersécurité.

En disant « Oui à la transformation numérique sécurisée », l'ANSSI a ouvert les Assises de la sécurité et des systèmes d'information en octobre à Monaco. L'occasion d'échanger sur des études de cas concrètes et les bonnes pratiques à mettre en place dans une optique de responsabilité partagée entre l'État, les acteurs économiques et les citoyens. Tous ces éléments concourent à l'émergence d'une industrie de cybersécurité de haut niveau. ⬢

– L'ÉTAT SE DONNE LES MOYENS D'UNE TRANSFORMATION NUMÉRIQUE SÉCURISÉE

La collaboration interministérielle est un prérequis pour offrir aux plus hautes autorités de l'État un niveau de sécurité efficient. Sont également concernés les OIV et bientôt les opérateurs de services essentiels (OSE).

LES OPÉRATEURS D'IMPORTANCE VITALE (OIV)

Comme le souligne Yves Verhoeven, sous-directeur RELEC : « Malgré l'existence de recommandations, de guides et de campagnes de sensibilisation, le niveau de cybersécurité progresse trop lentement au regard du risque.» L'absence de bonnes pratiques élémentaires de sécurité numérique, souvent liée à un manque de moyens humains et financiers accordés à la cybersécurité, expose les entreprises à des attaques numériques, dont les plus élémentaires sont susceptibles de perturber gravement leur activité. C'est le constat effectué par le Gouvernement lorsqu'il a considéré qu'il était urgent de fixer par voie législative des exigences minimales de cybersécurité pour les acteurs critiques.

C'est ainsi que la loi de programmation militaire 2014-2019, dans son article 22, a défini un nouveau cadre réglementaire imposant des mesures de renforcement de la sécurité des systèmes d'information des opérateurs d'importance vitale.

Il existe aujourd'hui plus de 200 OIV en France, répartis en 12 secteurs d'activités d'importance vitale. La mise en œuvre de ces dispositions s'est poursuivie depuis 2014, et l'ANSSI a publié en 2017 les derniers arrêtés sectoriels s'appliquant aux OIV du secteur privé.

« Les arrêtés sectoriels ont été définis grâce à un important travail de coordination entre l'ANSSI, les ministères coordonnateurs et les OIV », explique François Charbonnier, chef adjoint de la division coordination sectorielle de l'ANSSI. « En 2017, pas moins de 1 000 systèmes d'information d'importance vitale ont été déclarés à l'ANSSI. »

« EN 2018, L'AP-HP RENFORCERA SA CAPACITÉ À DÉTECTER LES MENACES ET LES VULNÉRABILITÉS SUR L'ENSEMBLE DE SON SI. »

UN NOUVEL ENJEU RÉGLEMENTAIRE : LA DIRECTIVE NIS ET LES FUTURS OPÉRATEURS DE SERVICES ESSENTIELS

Au-delà de ce cadre réglementaire national pour les OIV, qui constituent le cœur de la résilience de la Nation, d'autres acteurs fournissent des services essentiels au bon fonctionnement de notre économie et à la vie quotidienne de nos concitoyens. Beaucoup de ces acteurs, publics comme privés, demeurent en effet très vulnérables aux attaques informatiques, comme l'ont montré les récentes campagnes d'attaques informatiques mondiales WannaCry et NotPetya. Pour pallier cette situation, des mesures concrètes sont nécessaires.

C'est tout l'enjeu de la directive européenne du 6 juillet 2016 sur la sécurité des réseaux et de l'information (dite directive SRI, ou NIS en anglais).

Cheffe de file des négociations de la directive, l'ANSSI mène depuis plus d'un an les travaux de transposition, en concertation avec les ministères et les différentes parties prenantes nationales en vue d'apporter expertise et compétence dans la mise en place de ce futur cadre réglementaire. ⬢

ASSISTANCE PUBLIQUE HÔPITAUX DE PARIS

AU-DELÀ DE LA RÉGLEMENTATION : L'ACCOMPAGNEMENT DE GRANDS ACTEURS DE L'ÉTAT

C'est le cas avec l'Assistance Publique – Hôpitaux de Paris (AP-HP) : « En 2017, l'ANSSI et le ministère de la Santé ont accompagné l'AP-HP dans l'amélioration du pilotage du plan d'action de sécurisation de ses systèmes numériques, explique Catherine Sueur, secrétaire générale de l'AP-HP. L'ANSSI a apporté une contribution significativement dans l'identification et la réduction du niveau d'exposition aux menaces Internet des applications et téléservices. »

Au-delà, « l'application des bonnes pratiques du guide d'hygiène informatique de l'ANSSI améliorera sensiblement la résilience du système d'information face à une attaque ciblée garantissant la continuité des soins. »

Pour Catherine Sueur, le risque d'une attaque contre l'AP-HP similaire à celle subie par les hôpitaux britanniques en 2017 « est envisageable même si le contexte français est différent. Avant tout, il s'agit d'inciter les industriels (éditeurs, fabricants de dispositifs médicaux, etc.) à intégrer la sécurité dans les systèmes qu'ils conçoivent et mettent à disposition des établissements de soins. Le maintien en condition de sécurité des systèmes techniques et biomédicaux reste complexe et difficile à intégrer par les équipes qui en ont la charge. Les impacts de l'arrivée des objets connectés dans le SI restent encore largement à appréhender aussi bien dans les usages que dans leur intégration sécurisée au système d'information. En 2018, l'AP-HP renforcera sa capacité à détecter les menaces et les vulnérabilités sur l'ensemble de son SI (environ 100 000 adresses IP) y compris pour les systèmes biomédicaux ou techniques, et améliorera ses pratiques de segmentation au niveau des hôpitaux. » ⬢

– MISER SUR LA PROXIMITÉ
EN LIGNE ET SUR LE TERRITOIRE

L'ANSSI encourage le développement d'initiatives ciblées en son sein ou aux côtés de ses partenaires pour répondre le plus efficacement possible aux besoins en misant sur une approche coordonnée et sur-mesure. Elle a ainsi déployé des agents en régions pour créer les conditions d'une action de proximité. Elle a, en outre, incubé un dispositif destiné à aider les collectivités, TPE/PME ainsi que les citoyens victimes d'actes de cybermalveillance en les mettant en relation avec des prestataires de proximité.

DÉLÉGUÉ À LA SÉCURITÉ NUMÉRIQUE : UN RAPPORT PRIVILÉGIÉ AVEC LES ACTEURS LOCAUX

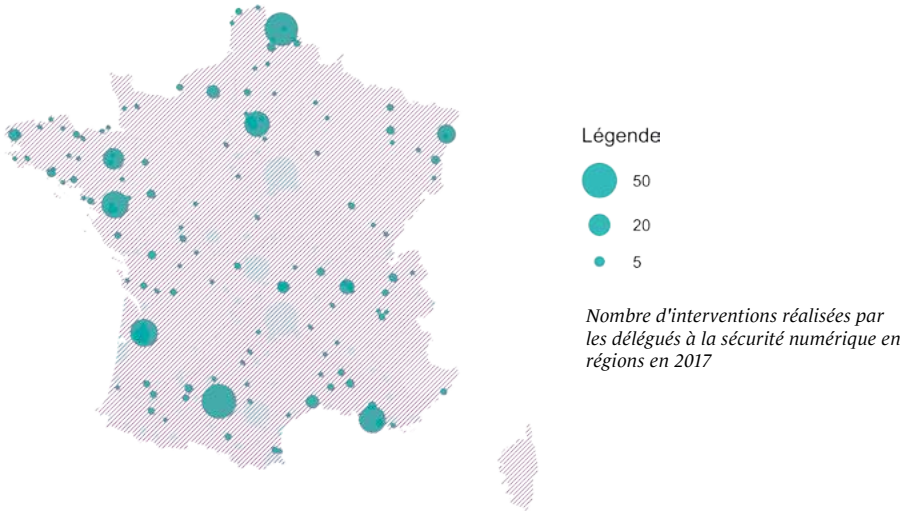
Dans le prolongement d'une réflexion interministérielle sur l'avenir de l'action territoriale en matière de sécurité numérique, l'ANSSI s'est dotée d'un dispositif d'action visant à soutenir le tissu économique et les institutions à l'échelle régionale. Recrutés en interne, les délégués à la sécurité numérique en régions disposent d'une solide expérience de la sécurité des systèmes d'information et sont d'excellents pédagogues et communicants capables d'évoluer auprès d'acteurs publics ou privés issus de secteurs diversifiés.

En outre, chaque délégué a lui-même organisé, souvent en partenariat avec d'autres institutions, au moins un colloque ou séminaire au profit des entreprises ou collectivités territoriales. En particulier, les journées #SecNumEco, en collaboration avec les service du ministère de l'Économie et des Finances permettent de souligner la communauté de démarches entre sécurité économique et sécurité numérique.

Les délégués passent près de 70% de leur temps en régions. En 2017, ils ont en moyenne participé chaque semaine à 25 entretiens, rencontres, colloques ou tables rondes diverses.

Les délégués collaborent tout particulièrement avec les acteurs consulaires (CCI, chambres d'artisanat et d'agriculture, etc.), interlocuteurs privilégiés du tissu entrepreneurial en région. Cette coopération s'illustre également au sein de la plateforme Cybermalveillance.gouv.fr dont la CCI France est membre du collège « Utilisateurs. »

À titre d'exemple, pour répondre aux besoins identifiés dans les territoires, l'ANSSI a publié le 20 juin une « Charte d'utilisation des moyens informatiques et des outils numériques – le guide indispensable pour les PME et ETI », toujours dans un souci d'apporter une information claire et précise aux entreprises.



Nombre d'interventions réalisées par les délégués à la sécurité numérique en régions en 2017

Cybermalveillance.gouv.fr : UN MODÈLE DE DÉVELOPPEMENT UNIQUE POUR RÉPONDRE À UN BESOIN D'UTILITÉ PUBLIQUE

L'agence a à cœur de déployer des outils permettant au plus grand nombre - et *a fortiori* aux TPE et PME - de pouvoir se prémunir en cas d'attaque. Comme le souligne Guillaume Poupard, « S'il n'y a de petites ou de grandes détresses face à un acte de cybermalveillance, on constate un effet systémique très fort qui fait que si demain, 10 % des PME françaises sont bloquées, cela devient un problème de sécurité nationale. »

Annoncé en 2016, ce projet interministériel a été incubé au sein de l'ANSSI et copiloté avec le ministère de l'Intérieur. Un modèle de développement original qui a bénéficié du soutien des ministères de l'Économie et des Finances, de la Justice et du secrétariat d'État chargé du Numérique. La plateforme a fait l'objet à partir du 30 mai 2017 d'une phase expérimentale en Hauts-de-France avant d'être déployée au niveau national à partir du 17 octobre.

Cybermalveillance.gouv.fr poursuit trois objectifs principaux :

- accompagner les victimes par une mise en relation avec des prestataires de proximité capables d'apporter l'assistance technique nécessaire ;
- prévenir et sensibiliser à la sécurité du numérique par la mise à disposition de contenus dédiés (recommandations, campagnes de sensibilisation, aide à la formation) ;
- anticiper par la création d'un observatoire de la menace numérique.

Les prestataires de services informatiques de proximité ont la possibilité de créer un compte en ligne afin de demander le référencement de leur société sur le site.

À ce jour, la plateforme a déjà enregistré 4 030 actes de cybermalveillance (sollicitations incluses) et référencés 1 350 prestataires pour 1 700 demandes formulées. En moyenne, une victime d'acte de cybermalveillance, où qu'elle se trouve en France, peut se voir proposer jusqu'à 24 prestataires proches de chez elle.

1 000
SIIV DÉCLARÉS

675
MISSIONS
À
L'INTERNATIONAL

1 000
INTERVENTIONS
EN RÉGION

40
PAYS

49 000
INSCRITS
MOOC
!

7
FORMATIONS
LABEL
CyberEdu

SecNum*académie* : FORMER ET SENSIBILISER EN LIGNE

Lancée en mai 2017, la formation en ligne (MOOC) SecNum*académie* a pour objectif de permettre aux étudiants, salariés, dirigeants d'entreprise ou particuliers d'être initiés à la cybersécurité ou d'approfondir leurs connaissances afin de pouvoir agir efficacement sur la sécurité de leurs systèmes d'information.

Gratuit et accessible à tous, SecNum*académie* donne accès à un large contenu pédagogique proposé et conçu par les experts de l'ANSSI.

Le premier module a été mis en ligne le 18 mai. Le programme est constitué de quatre modules de formation de cinq unités qui ont été diffusés en septembre et décembre 2017 - le 4e et dernier chapitre le sera en février 2018.

Ce premier MOOC créé par l'ANSSI est un succès puisque mi-décembre, la plateforme comptait prés de 50 000 inscrits !

La formation, disponible pendant trois ans à compter de la date d'inscription, est sanctionnée par une attestation de réussite obtenue par la validation progressive des crédits attribués à chaque unité.

Cyber*Edu* : FORMATIONS LABELLISÉES ET CONVENTION AVEC L'AFPA

Portée par l'ANSSI, l'association Cyber*Edu* a vocation à proposer une labellisation des formations d'enseignement supérieur mettant en œuvre les principes de sa démarche pédagogique en matière de sécurité du numérique, à la différence de SecNum*Edu* qui labellise des formations de spécialistes en sécurité du numérique.

En juin 2017, Cyber*Edu* a lancé son processus de labellisation. À ce jour, 7 formations ont reçu le label.

Le 27 octobre, l'association a signé un accord avec l'Agence nationale pour la formation professionnelle des adultes (AFPA) visant à rapprocher la formation professionnelle des enjeux de cybersécurité.

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

SecNum*edu* : 40 FORMATIONS LABELLISÉES EN 2017

Pilotée par l'ANSSI en partenariat avec le ministère de l'Éducation nationale, de l'Enseignement supérieur et de la Recherche, le Pôle d'Excellence Cyber, des écoles et des industriels, la certification SecNum*edu* apporte aux étudiants et employeurs la garantie que la formation répond à une charte et des critères définis par l'ANSSI en collaboration avec les acteurs et professionnels du domaine (établissements d'enseignement supérieur, employeurs, etc.). SecNum*edu* vise non seulement à apporter de la lisibilité à l'offre de formation et aux métiers du secteur mais également à leur offrir davantage de visibilité. À ce jour, plus de 40 établissements de formation initiale et continue ont reçu ce certificat.

« LA MEILLEURE DÉFENSE, C'EST ENCORE… LA DÉFENSE. »

SENSIBILISER DIRIGEANTS ET DSI

« Si la prise en compte de la sécurité numérique au sein des comités exécutifs progresse de manière significative, elle reste insuffisante et intervient trop souvent à l'issue d'un incident informatique grave », soulignait Guillaume Poupard en introduction du guide « L'essentiel de la sécurité numérique pour les dirigeants », publié en février, par le Conseil de l'Économie et de l'Information du Digital (CEIDIG), avec le magazine Challenges.

Ce guide, résolument pratique, a été présenté à l'occasion du Cercle européen de la sécurité, avec un objectif précis : donner un « coup de projecteur » à la fois positif et constructif sur la sécurité numérique tout en étant résolument utile et pratique pour faire écho chez un public prioritaire dont le sens de l'action peut être déterminant sur les questions de sécurité et de santé numérique de l'entreprise.

Diffusé dans sa version papier en supplément du magazine Challenges, ce guide a été adressé à une liste de dirigeants français. Son édition numérique est disponible sur le site des éditions Eyrolles.

FRANCE

SÉCURISER L'ÉTAT ET LA NATION

ÉTAT / OIV

1er pays à adopter une approche régulatrice

COMMENT ?

PRIS, PDIS,
PASSI, SecNumCloud

TPE-PME, grand public et collectivités territoriales + PARTENAIRES

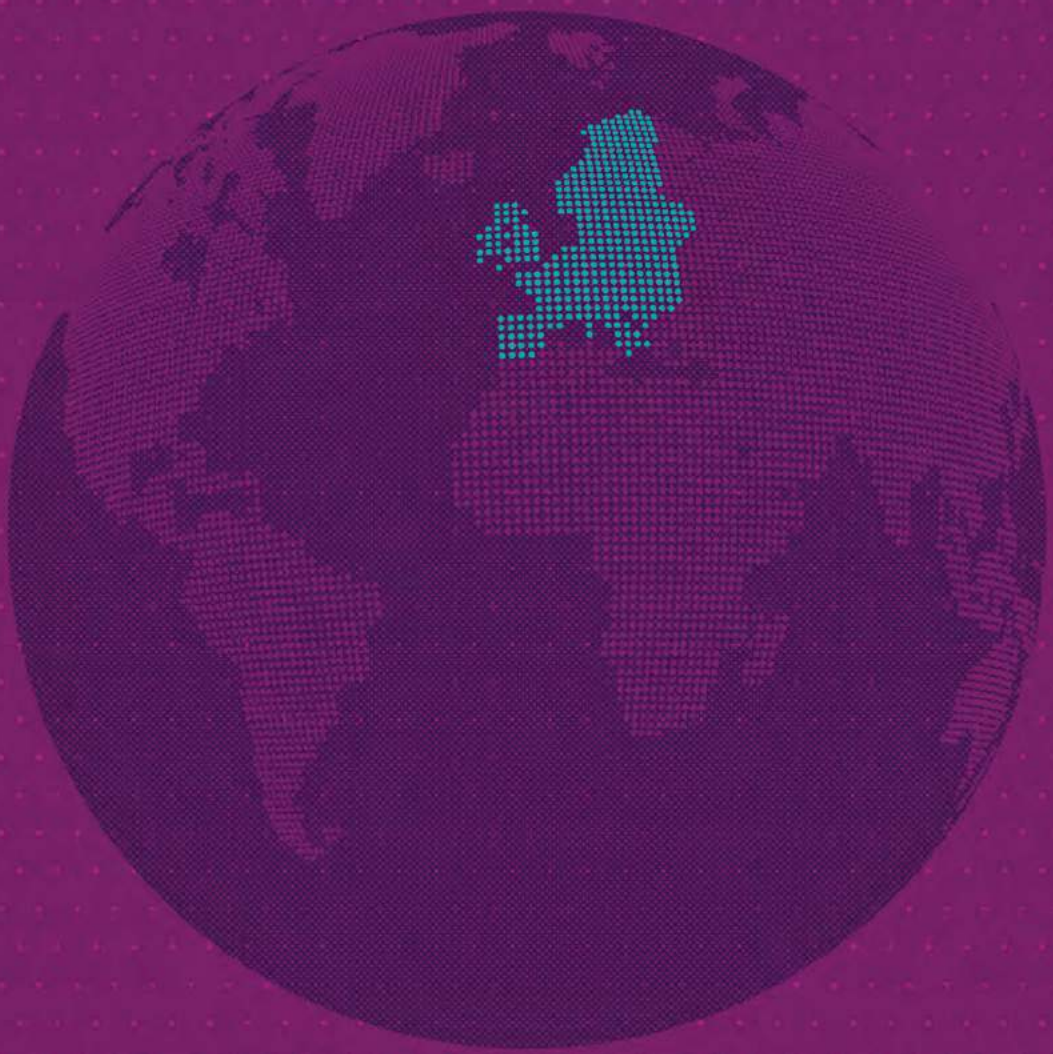
COMMENT ?

Cybermalveillance.gouv.fr
Délégués à la sécrutité numérique

EUROPE

RENFORCER LA RÉSILIENCE *du Marché Unique du Numérique*

Augmenter les capacités nationales des États membres en matière de cybersécurité.
Accroître la coordination en cas d'incidents transnationaux.
Instaurer des exigences de sécurité et de notification d'incidents.



CONSTRUIRE LA PAIX ET LA STABILITÉ DU CYBERESPACE INTERNATIONAL

États | Entreprises | Organisations | Citoyens

En promouvant l'applicabilité du droit international au cyberespace.
En établissant des mesures de renforcement de la confiance entre États.
En participant aux efforts de renforcement capacitaire *via* l'échange de bonnes pratiques.

– RISQUE CYBER : UN ENJEU EUROPÉEN ET INTERNATIONAL

Le modèle français de cyberdéfense sépare la protection et la défense du renseignement et de l'attaque. Cette singularité s'illustre dans le climat de concertation qu'instaure l'agence avec les opérateurs privés et publics tout autant qu'avec leurs homologues européens et internationaux, dans un souci permanent d'échange d'informations et de retours d'expérience.

« Tous ces partenariats nous permettent, sur des questions relatives à l'écosystème industriel ou la réglementation, de confronter nos idées et de promouvoir notre modèle. Il est dans notre intérêt d'entretenir ce cercle vertueux afin de ne pas laisser se développer des foyers d'infection », explique Yves Verhoeven sous-directeur RELEC.

« LA FRANCE SERA, AVEC LES ÉTATS MEMBRES VOLONTAIRES, LE MOTEUR D'UNE AUTONOMIE STRATÉGIQUE DE L'UNION EUROPÉENNE. ELLE JOUERA UN RÔLE ACTIF DANS LA PROMOTION D'UN CYBERESPACE SÛR, STABLE ET OUVERT. »

POURSUIVRE LES ÉCHANGES AVEC LES PAYS PROCHES

La collaboration de l'ANSSI avec ses homologues britanniques et allemands s'est illustrée à de nombreuses reprises au cours des dernières années.

La coopération franco-britannique de cybersécurité s'inscrit dans un partenariat plus large entre les deux pays sur les questions de sécurité. Cette coopération est mise en œuvre par les autorités nationales respectives de cybersécurité, l'ANSSI pour la France et le *National Cyber Security Centre* (NCSC) pour le Royaume-Uni. Créé en 2016, le NCSC a pour mission principale de protéger le Royaume-Uni des menaces issues du cyberespace. Son activité repose sur une stratégie nationale à cinq ans publiée en 2016 et sur l'établissement de relations étroites avec l'ensemble des parties prenantes nationales (secteurs public et privé, opérateurs d'importance vitale, grand public) et aussi internationales comme l'ANSSI.

Leur coopération s'étend sur des domaines comme le traitement et la réponse à incident, les relations avec le secteur privé, et la sécurité du cyberespace mondial.

L'ANSSI et son homologue allemand, le *Bundesamt für Sicherheit in der Informationstechnik* (BSI) coopèrent depuis de nombreuses années au renforcement de la sécurité du numérique en France, en Allemagne et dans tout l'espace européen.

Après avoir annoncé fin décembre 2016 le lancement du label *European Secure Cloud (ESCloud)*, pour les prestataires de services d'informatique en nuage *cloud computing* de confiance, l'ANSSI et le BSI ont été particulièrement attentifs à la sécurité des processus démocratiques lors des élections françaises et allemandes de 2017. Cette coopération s'appuie sur de nombreux échanges d'informations.

ÉLEVER LE NIVEAU DE SÉCURITÉ À L'ÉCHELON EUROPÉEN : LA SLOVAQUIE

Pour la directrice de l'agence slovaque, « la collaboration entre États est un principe fondateur et immarcescible conduisant à l'émergence d'une communauté et d'un écosystème de confiance. La communication est essentielle pour apporter efficacité et rapidité. »

3 questions à ...

Colonel Martina Lisická, Director of International Cooperation and Organisation Division of NSA Office of Slovakia

QUELLES RELATIONS LE NBU ENTRETIENT-ELLE AVEC L'ANSSI ?

L'Autorité nationale de sécurité de Slovaquie NBU (NSA) a entamé une coopération stratégique avec l'ANSSI en 2017 au travers d'échanges nombreux et réguliers.

L'officier de liaison du NBU slovaque pour l'Otan à Bruxelles est devenu l'interlocuteur privilégié de l'ANSSI. Nous avons eu l'honneur d'accueillir des représentants de l'ANSSI lors d'événements nationaux et régionaux que nous avons organisés. Cette coopération s'illustre également à l'échelle européenne. Nous sommes persuadés que ces échanges et ce partage d'expérience de la part de nos deux États ne peuvent qu'être bénéfiques pour élever le niveau de sécurité.

QUELLE EST, SELON VOUS, LA MEILLEURE FAÇON DE RÉPONDRE ET DE CONTRER DES CYBERATTAQUES DE PLUS EN PLUS SOPHISTIQUÉES?

La meilleure réponse est une coopération de tous les acteurs – publics et privés – à tous les niveaux : régional, national et international. L'aspect humain de la cybercriminalité est un point qu'il faut également souligner. Pour cela, les interconnexions entre les organes techniques, d'analyse et d'enquête doivent être des plus efficaces. L'investigation ne doit pas se cantonner à la dimension cyber mais aussi avoir un équivalent dans la réalité, avec la recherche physique des attaquants. Enfin, le rôle de la R&D dans le domaine de la cybersécurité doit demeurer crucial.

COMMENT UNE COOPÉRATION RENFORCÉE ENTRE LES ÉTATS MEMBRES DE L'UE PEUT-ELLE CONTRIBUER À AMÉLIORER LA CYBERSÉCURITÉ AU NIVEAU NATIONAL ?

Il nous semble que la principale tâche à laquelle doivent s'attacher les États membres est l'harmonisation. Un autre point majeur est de porter également notre attention à ce qui se passe en dehors des frontières de l'Europe. L'Union européenne doit développer les relations avec nos voisins et partenaires. La cybersécurité est un sujet international et, dans cette optique, nous apportons notre soutien à des initiatives telles que la coopération TAIEX (avec les pays des Balkans de l'Ouest) ou les cyberdialogues du Service européen pour l'action extérieure (SEAE-EEAS). ⬢

« NOUS SOMMES PERSUADÉS QUE CES PARTAGES D'EXPÉRIENCE DE LA PART DE NOS DEUX ÉTATS NE PEUVENT QU'ÊTRE BÉNÉFIQUES POUR ÉLEVER LE NIVEAU DE SÉCURITÉ. »

PROMOUVOIR LE MODÈLE FRANÇAIS DE CYBERSÉCURITÉ PARTOUT DANS LE MONDE

Le 15 novembre 2017, l'ANSSI a signé un accord de coopération avec son homologue tunisien, l'Agence Nationale de Sécurité Informatique (ANSI), qui vise à renforcer le partage d'informations, d'expériences et de bonnes pratiques.

Ce partenariat s'inscrit dans un cadre plus global de développement des capacités de l'espace francophone et de renforcement des liens entre les deux pays. Cette stratégie de coopération internationale volontariste a pour objectif de démultiplier les capacités de réponse à la hauteur du défi collectif de la sécurité du numérique.

La France a également un rôle à jouer au sein du réseau francophone ; cela a notamment donné à lieu à la mise en place de programmes de coopération avec la Côte d'Ivoire. Et l'ANSSI suit de près l'activité numérique dans certaines zones de l'Asie, à l'instar de Singapour qui réfléchit à la mise en place effective de villes intelligentes. « C'est un laboratoire particulièrement intéressant pour nous afin de voir comment sécuriser les villes de demain », explique Guillaume Poupard.

« LE RÔLE DE LA COMMUNAUTÉ FRANCOPHONE EST PLUS QUE DEMANDÉ DANS CE DOMAINE QU'EST LA CYBERSÉCURITÉ »

3 questions à ...

Mohamed Naoufel Frikha, directeur général de l'Agence nationale de sécurité informatique (ANSI) de Tunisie

QUELLES SONT POUR L'ANSI LES PERSPECTIVES OUVERTES PAR L'ACCORD DE COOPÉRATION SIGNÉ EN NOVEMBRE 2017 AVEC L'ANSSI ?

Nous pensons que les changements géopolitiques et les avancées technologiques que nous vivons nous obligent tous à coordonner et coopérer davantage dans l'amélioration du « process de sécurisation » de l'espace cybernétique. En plus de la richesse des expériences mutuelles dans ce domaine, cette convention ANSSI-ANSI prévoit essentiellement un partage d'information sur les volets de la prévention, de la détection et de la réaction afin de garantir la cyber résilience notamment pour les services à intérêt vital.

QUELLES SONT SELON VOUS LES MENACES CYBER LES PLUS PRÉOCCUPANTES AUJOURD'HUI ?

Comme la plupart des organismes spécialisés dans le domaine, nous enregistrons au niveau de notre espace cybernétique des phénomènes « nocifs et inquiétants » qui exigeraient plus de coordination et d'efficacité à l'échelle internationale, régionale et nationale pour minimiser l'impact des cyberattaques qui ciblent les données (comme les rançongiciels) et les services (DDoS).

QUE POURRAIT APPORTER LA FRANCOPHONIE À LA CYBERSÉCURITÉ ?

Nous sommes certains que le rôle de la francophonie est plus que demandé de nos jours dans ce domaine si important et si stratégique, que ce soit dans la mise en place des programmes de renforcement des capacités francophones (formation spécialisée, supports techniques, supports de sensibilisation, R&D, etc.) ou encore dans les mécanismes de renforcement du développements et des usages des produits et services de haut niveau dans les domaines de cybersécurité.

RGPD : UN CADRE COMMUN POUR L'EUROPE

Mai 2018 coïncidera également avec l'entrée en vigueur du Règlement général sur la protection des données à caractère personnel (RGPD), qui renforce la protection des personnes à l'égard du traitement des données à caractère personnel. La Commission Nationale de l'Informatique et des Libertés (CNIL) présente les grands axes de ce règlement ainsi que les obligations qui lui sont conséquentes.

1 LES PRINCIPALES OBLIGATIONS POUR LES ORGANISMES VISÉS, NOTAMMENT EN MATIÈRE DE NOTIFICATION, ET LES NOUVEAUTÉS APPORTÉES PAR LE RÈGLEMENT

Dans la continuité de ceux de la loi « Informatique et Libertés » (1978), le RGPD introduit toutefois plusieurs changements majeurs : moins de contrôle *a priori* par la CNIL ; une plus grande responsabilisation des entreprises ; en contrepartie, un rehaussement des sanctions.

Le RGPD prévoit également des obligations nouvelles dont, dans certains cas, une obligation de notification des violations de données à caractère personnel. Enfin, ce texte redonne de la souveraineté à l'Europe en remettant les entreprises françaises et européennes à égalité de concurrence avec les entreprises étrangères même non établies en Europe, dès lors qu'elles ciblent un européen.

2 LES ÉTAPES CLÉS DE LA MISE EN CONFORMITÉ DES ORGANISMES PUBLICS ET PRIVÉS TRAITANT DES DONNÉES À CARACTÈRE PERSONNEL

La CNIL a mis en place sur son site un parcours en six étapes, avec plusieurs outils à l'appui permettant d'aider les organismes dans leur démarche de mise en conformité.

Au sein des organismes, la gouvernance des données personnelles nécessitera un véritable chef d'orchestre qui exerce une mission d'information, de conseil et de contrôle en interne : il s'agit du délégué à la protection des données (*Data Protection Officer* – DPO), dont la désignation est obligatoire pour les organismes publics ainsi que pour les entreprises dont l'activité présente une certaine sensibilité.

3 LA POSITION DE LA CNIL AVEC L'ENTRÉE EN VIGUEUR DU RGPD

Le RGPD entraîne un changement d'échelle de la régulation *via* un mécanisme de guichet unique donnant aux entreprises un interlocuteur unique au niveau européen. Dans ce paysage, la CNIL prône une régulation basée sur deux piliers alliant l'accompagnement (information, conseil, accompagnement des DPO, autorisations, packs de conformité sectoriels, labels) et des pouvoirs répressifs renforcés à l'échelle européenne. Elle travaille à fournir aux organismes un cadre clair, qui renforce leur sécurité juridique dans un environnement concurrentiel, en leur permettant de limiter autant que possible les risques de sanctions.

> Afin d'éviter les fuites de données à caractère personnel, le RGPD prévoit plusieurs dispositions relatives à leur sécurité. Les organismes publics et privés concernés devront notamment mettre en œuvre des mesures techniques ou organisationnelles adaptées au risque. Le renforcement de leur sécurité numérique constituera, à cet égard, une dimension importante de la démarche de mise en conformité avec le règlement. Outre les recommandations émises par la CNIL, les bonnes pratiques et méthodes promues par l'ANSSI en matière de management des risques, d'hygiène informatique ou encore les labels d'offres numériques de confiance tels que SecNumCloud, constitueront autant de références pour les organismes concernés. ⬢

« UNE MEILLEURE DÉTECTION DES CYBERATTAQUES DOIT PASSER PAR UNE COLLABORATION ÉTROITE AVEC L'ÉCHELON INTERMINISTÉRIEL ET LES OPÉRATEURS. »

– 2018 : LES ENJEUX DE DEMAIN

Après une année marquée par une extension du périmètre d'intervention de l'ANSSI, l'agence, à travers la sous direction RELEC, relations extérieures et coordination, travaille depuis plusieurs mois sur les grands enjeux qui vont rythmer 2018 : réglementaire d'abord avec la transposition de la directive NIS au niveau national et l'élargissement du champ d'action de l'ANSSI aux opérateurs de services essentiels ; européen ensuite avec la construction d'une autonomie stratégique de l'Union européenne pour la sécurité du numérique qui passe par le partage d'objectifs communs et la mobilisation des moyens nécessaires à leur réalisation.

Le dernier enjeu majeur de développement pour l'ANSSI en 2018 s'attache à la question d'une meilleure détection des cyberattaques qui passe par une collaboration étroite avec l'échelon interministériel ainsi qu'avec les opérateurs de communications électroniques (OCE).

UN ENJEU RÉGLEMENTAIRE : LA DIRECTIVE NIS

La directive NIS qui doit être transposée d'ici le 9 mai 2018, permettra d'augmenter significativement le niveau de sécurité numérique des acteurs qui fournissent des services essentiels au bon fonctionnement de notre économie et à la vie quotidienne de nos concitoyens.

Ce cadre réglementaire permettra de donner à la France les moyens de protéger ces acteurs. La loi de transposition de la directive NIS n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité prévoit ainsi que les OSE, désignés par le Premier ministre, appliqueront des règles de sécurité numérique élaborées par l'Agence nationale de la sécurité des systèmes d'information. Ces opérateurs devront informer l'ANSSI des incidents de sécurité susceptibles d'avoir un impact significatif sur la continuité des services essentiels qu'ils assurent. Il introduit également un volet destiné à renforcer la cybersécurité des fournisseurs de services numériques qui seront tenus d'assurer la sécurité de leurs services et de notifier leurs incidents à l'ANSSI.

CONCERTATION, ANTICIPATION, HARMONISATION,

CONSTRUIRE L'AUTONOMIE STRATÉGIQUE DE L'UNION EUROPÉENNE

Pour l'ANSSI, la sécurité du numérique de l'Union européenne repose sur sa capacité à garantir son autonomie stratégique en la matière, autour de trois piliers :

CAPACITAIRE : renforcer la sécurité numérique des États membres et des institutions européennes par la promotion et le soutien au développement de capacités de cybersécurité au sein des membres de l'Union européenne ;

RÉGLEMENTAIRE : réguler la protection de certaines données du fait de leur sensibilité, notamment en ce qui concerne la territorialisation ou la certification des produits sur lesquels ces données transitent ou des services qui les hébergent ;

TECHNOLOGIQUE : développer l'autonomie stratégique de l'Union européenne en matière de technologies, d'industrie et de services relatifs à la sécurité du numérique, cet objectif concourant à renforcer la sécurité et la confiance dans le Marché Unique du Numérique (MUN).

L'autonomie stratégique de l'Union européenne a été identifiée par les autorités françaises parmi les cinq priorités de la Stratégie nationale pour la sécurité du numérique de 2015. Un objectif qui ne peut être atteint que collectivement, au sein de l'Union européenne.

COLLABORER AVEC LES OPÉRATEURS DE COMMUNICATIONS ÉLECTRONIQUES POUR DÉVELOPPER LA DÉTECTION D'ATTAQUES

Le dernier enjeu majeur de l'ANSSI pour 2018 vise à renforcer sa capacité de détection des attaques au moyen d'une approche coordonnée avec les acteurs concernés.

Dans une volonté permanente de concertation, l'ANSSI souhaite établir des collaborations avec les opérateurs de communications électroniques dans l'optique d'élever les capacités de cyberdéfense nationales.

L'ANSSI travaille déjà avec l'Autorité de régulation des communications électroniques et des postes (ARCEP) mais souhaite élargir le champ de coopération avec ces OCE. Tout comme les plateformes d'intermédiation privées, ces opérateurs disposent d'une capacité de détection des attaques.

Il s'agit d'identifier ce qu'il est possible de faire pour mieux utiliser les réseaux de ces opérateurs - dans le respect des libertés et de la neutralité du Net - en leur confiant par exemple un rôle dans la prévention de cyberattaques et, en cas d'attaques graves et massives, de soutien pour contrer celles-ci. ⬢

« IL S'AGIT D'IDENTIFIER CE QU'IL EST POSSIBLE DE FAIRE POUR MIEUX UTILISER LES RÉSEAUX DE CES OPÉRATEURS - DANS LE RESPECT DES LIBERTÉS ET DE LA NEUTRALITÉ DU NET. »

TELS SERONT LES MOTS-CLÉS DE 2018 POUR L'ANSSI.

DOCUMENTS DE DOCTRINE

PUBLICATIONS SCIENTIFIQUES

PUBLICATIONS INTERNES

PUBLICATIONS TOUS PUBLICS

PARTENARIATS

BI-BLIO-GRA-PHIE

DOCUMENTS DE DOCTRINE

MISES À JOUR

- *Recommandations de sécurisation d'un pare-feu Stormshield Network Security (SNS),* guide technique
- *La télé-assistance sécurisée,* guide technique
- *Bonnes pratiques pour l'acquisition et l'exploitation de noms de domaine,* guide technique
- *Mettre en œuvre une politique de restrictions logicielles sous Windows,* guide technique
- *Restreindre la collecte de données sous Windows 10,* guide technique
- *Guide d'hygiène informatique, renforcer la sécurité de son système d'information en 42 mesures,* guide
- *Guideline for a healthy information system in 42 measures,* guide

NOUVEAUX

- *Restreindre la collecte de données sous Windows 10,* guide technique
- *Mise en œuvre des fonctionnalités de sécurité de Windows 10 reposant sur la virtualisation,* guide technique
- *Recommandations pour une utilisation sécurisée de Cryhod,* guide technique
- *Recommandations de sécurité relatives à TLS,* guide technique
- *Bonnes pratiques pour l'acquisition et l'exploitation de noms de domaine,* guide technique en anglais
- *Recommandations pour la mise en place de cloisonnement système,* guide technique

- *Rapport 2016 de l'observatoire de la résilience de l'Internet français*

- *Charte d'utilisation des moyens informatiques et des outils numériques,* guide

- Collection

  - *Sécurité numérique – Bonnes pratiques à l'usage des hautes autorités*
  - *Sécurité numérique – Bonnes pratiques à l'usage des députés*
  - *Sécurité numérique – Bonnes pratiques à l'usage des sénateurs*

APPELS À COMMENTAIRES

- *Intégrer la sécurité dans une démarche agile,* guide

- Guide cartographie

RÉFÉRENTIELS

- Prestataires de détection des incidents de sécurité, référentiel d'exigences, V2

- Prestataires de réponse aux incidents de sécurité, référentiel d'exigences, V2

BULLETINS D'INFORMATION

- Bulletin hebdomadaire d'actualité du CERT-FR : https://www.cert.ssi.gouv.fr/actualite/

- Note d'information du CERT-FR relative aux rançongiciels : https://www.cert.ssi.gouv.fr/information/CERTFR-2017-INF-001/

PUBLICATIONS INTERNES

- *Piloter la performance des processus,* guide

PUBLICATIONS SCIENTIFIQUES

- Timothée Ravier : *Durcissement système à l'aide de systemd* - SSTIC 2017

- Mickaël Salaün : *Landlock : cloisonnement programmable non privilégié* - SSTIC 2017

- Marion Daubignard, Yves-Alexis Perez : *ProTIP : You should know what to expect from your peripherals* - SSTIC 2017

- Chaouki Kasmi, José Lopes Esteves, Mathieu Renard, Ryad Benadjila : *From academia to real world: a practical guide to Hitag-2 RKE System analysis* - SSTIC 2017

- Timothée Ravier : Durcissement système à l'aide de systemd – RMLL

- Ryad Benadjila, Mathieu Renard, José Lopes-Esteves, Chaouki Kasmi : *One car, two frames: Attacks on Hitag-2 Remote Keyless Entry Systems revisited* - Usenix Security

- Mickaël Salaün : *Landlock LSM: towards unprivileged sandboxing* - Linux Security Summit

- Mickaël Salaün : *Landlock LSM: Unprivileged sandboxing* - Kernel Recipes

- Anaël Beaugnon, Francis Bach, Pierre Chifflier : *ILAB: An Interactive Labelling Strategy for Intrusion Detection* - RAID

- Pierre Chifflier, Geoffroy Couprie : *Writing parsers like it is 2017* - SSTIC 2017

- Anaël Bonneton, Antoine Husson : *Le Machine Learning confronté aux contraintes opérationnelles des systèmes de détection* - SSTIC 2017

- Pierre Chifflier, Geoffroy Couprie : *Writing parsers like it is 2017* - IEEE S&P LangSec Workshop

- Pierre Chifflier : *Writing safe parsers, lecture and tutorial* – Suricon

- Johan Mazel, Romain Fontugne, Kensuke Fukuda : *Profiling Internet Scanners : Spatiotemporal Structures and Measurement Ethics* - TMA

- Tetsu Iwata, Kazuhiko Minematsu, Thomas Peyrin, Yannick Seurin : *ZMAC: A Fast Tweakable Block Cipher for Highly Secure Message Authentication* - CRYPTO 2017, LNCS, Springer 2017

- Yuanxi Dai, Yannick Seurin, John Steinberger, Aishwarya Thiruvengadam : *Indifferentiability of Iterated Even-Mansour Ciphers with Non-idealized Key-Schedules: Five Rounds Are Necessary and Sufficient* - CRYPTO 2017, LNCS, Springer 2017

- Jérémy Jean, Amir Moradi, Thomas Peyrin, Pascal Sasdrich : Bit-Sliding : *A Generic Technique for Bit-Serial Implementations of SPN-based Primitives – Applications to AES, PRESENT and SKINNY* - CHES 2017, LNCS, Springer 2017

- Jean-Pierre Flori, Gérard Cohen : *On a generalised combinatorial conjecture involving addition mod 2^k-1* - International Journal of Information and Coding Theory, IJICoT vol. 4, n°1, 2017

- Domingo Gomez-Perez, Guénaël Renault : *A Probabilistic Analysis on a Lattice Attack against DSA* - CoRR abs 2017

- Ludovic Brieulle, Luca De Feo, Javad Doliskani, Jean-Pierre Flori, Eric Schost : *Computing Isomorphisms and Embeddings in Finite Fields* - CoRR abs 2017

- Colin Chaigneau, Thomas Fuhr, Jérémy Jean, Henri Gilbert, Jean-René Reinhard : *Cryptanalysis of NORX v2.0 - FSE 2017, Transactions on Symmetric Cryptography 2017, vol. 1* - IACR 2017

- Benoît Cogliati, Jooyoung Lee, Yannick Seurin : *New Constructions of MACs from (Tweakable) Block Ciphers* - FSE 2018, Transactions on Symmetric Cryptography 2017, vol. 2 - IACR 2017

- Tetsu Iwata, Yannick Seurin : *Reconsidering the Security Bounds of AES-GCM-SIV* - FSE 2018, LNCS, Transactions on Symmetric Cryptography 2017, vol. 4 - IACR 2017

- Jérémy Jean, Thomas Peyrin, Siang Meng Sim, Jade Tourteaux : *Optimizing Implementations of Lightweight Building Blocks* - FSE 2018, Transactins on Symmetric Cryptography 2017, vol. 4 - IACR 2017

- Kaushik Chakraborty, Sumanta Sarkar, Subhamoy Maitra, Bodhisatwa Mazumdar, Debdeep Mukhopadhyay, Emmanuel Prouff : *Redefining the transparency order* - Designs, Codes and Cryptography 82(1-2), pp. 95-115

- Nicolas Bruneau, Claude Carlet, Sylvain Guilley, Annelie Heuser, Emmanuel Prouff, Olivier Rioul : *Stochastic collision attack* - IEEE Trans. Information Forensics and Security 12(9), pp. 2090-2104

- Eleonora Cagli, Cécile Dumas, Emmanuel Prouff : *Convolutional Neural Networks with Data Augmentation against Jitter-Based Countermeasures* - CHES 2017, LNCS 10529, pp. 45-68, Springer

- Sonia Bélaïd, Fabrice Benhamouda, Alain Passelègue, Emmanuel Prouff, Adrian Thillard, Damien Vergnaud : *Private Multiplication over Finite Fields* - CRYPTO 2017 Part III, LNCS 10403, pp. 397-426, Springer

- Guillaume Bouffard, Noreddine El Janati El Idrissi, Jean-Louis Lanet, Said El Hajji : *Trust can be misplaced* - Journal of Cryptographic Engineering 7(1), pp. 21-34 - Safety-critical Systems Symposium 2017

- José Lopes-Esteves, Chaouki Kasmi, Keith Armstrong, Davy Pissoort : *Analysis of effects induced by EM disturbances on devices, from a Security and functional Safety perspective* - Safety-critical Systems Symposium 2017

- Emmanuel Cottais, José Lopes-Esteves, Valentin Houchouas, Chaouki Kasmi : *Effects of Intentional Electromagnetic Interference on an Adaptive Predistortion Algorithm* - EMC Europe 2017

- Valentin Houchouas, José Lopes-Esteves, Emmanuel Cottais, Chaouki Kasmi : *Functional Safety Assessment of a Servomotor Exposed to intentional RF Pulses* - EMC Europe 2017

- Chaouki Kasmi, José Lopes-Esteves : *Emerging Threats of IEMI for Information Security: recent advance* - ASIAEM 2017 (plenary talk)

- Chaouki Kasmi, Lars-Ole Fichte, Marcus Stiemer : *Evaluation of HEMP Tests by Binary Regression Models* - ASIAEM 2017

- Chaouki Kasmi, Lars Ole Fichte, Sébastien Lallléchère, Sébastien Girard, François Paladian, Pierre Bonnet : *Probabilistic Assessment of Braid Hardening with Limited Amount of Information* - ASIAEM 2017

- Tristan Claverie, José Lopes-Esteves, Chaouki Kasmi : *Auditer des télévisions connectées* – SSTIC 2017

- Chaouki Kasmi, José Lopes-Esteves : VentriLock : *Exploring Voice-based authentication Systems* - Hack In Paris 2017

- Emmanuel Cottais, Chaouki Kasmi, José Lopes-Esteves : *A Ghost in your Transmitter: analyzing polyglot signals for physical layer covert channels detection* - Hardwear.io 2017

- Chaouki Kasmi, José Lopes-Esteves : *Agressions Électromagnétiques : quels risques pour la SSI* - MISC HS 2017

- Chaouki Kasmi, Lars Ole Fichte, Sébastien Lallléchère, Sébastien Girard, François Paladian, Pierre Bonnet : *Probabilistic Assessment of Braid Transfer Impedance with restricted Number of Measurement* - EUMW Conference 2017

- Pierre-Michel Ricordel : *Sécurité des micros sans-fil* - SSTIC 2017

- Chaouki Kasmi, José Lopes-Esteves : *Electromagnetic Threats for Information Security* - 34C3

- Maxence Tury : *Tutoriel Parser Scapy TLS* – Journée du Conseil Scientifique de l'AFNIC 2017

- Guillaume Valadon : *Tutoriel Scapy*, GreHack 2017

- Guillaume Valadon : *Présentation Scapy*, BalCCon 2017

- François Contat : *Présentation ABH*, NetSecure Day 2017

PUBLICATIONS TOUS PUBLICS

- Rapport d'activité 2016

- Modules 1, 2 et 3 du MOOC SecNum*académie*

- *La sécurité du numérique à portée de clic*, affiche

- *Élections législatives : Candidats, assurez votre sécurité numérique !*, fiche pratique

- *DDoS*, infographie

PARTENARIATS

- *L'essentiel de la sécurité numérique pour les dirigeants, CEIDIG*

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

51, BOULEVARD DE LA TOUR-MAUBOURG
75700 PARIS CEDEX 07 SP

COMMUNICATION@SSI.GOUV.FR
WWW.SSI.GOUV.FR

@ANSSI_FR
DAILYMOTION.COM/ANSSI_FR
LINKEDIN.COM/COMPANY/ANSSI-FR

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
SGDSN