

15/04/2019

DOSSIER DE PRESSE



CONSTRUIRE ENSEMBLE LA CONFIANCE NUMERIQUE DE DEMAIN

PAR L'AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION



SOMMAIRE

I- ANALYSE DE LA MENACE EN 2018

page 4

LES 5 GRANDES TENDANCES OBSERVÉES EN FRANCE ET EN EUROPE

page 4

II- RESSERRER LES LIENS AVEC NOS PARTENAIRES

page 7

RENFORCER LES PARTENARIATS AVEC LES SECTEURS PUBLIC ET PRIVÉ

page 7

LA FRANCE MOTEUR EUROPÉEN DE LA CONFIANCE NUMÉRIQUE

page 11

III- CRÉER DE NOUVEAUX CADRES D'ÉCHANGES POUR GARDER UN TEMPS D'AVANCE

page 14

ANTICIPER : UN PRÉREQUIS POUR L'AVENIR

page 14

L'OUVERTURE ET LE PARTAGE POUR MOTS D'ORDRE

page 15

RETOUR SUR LES INTERVENANTS DE LA CONFÉRENCE DE PRESSE

Introduction

Claire Landais, secrétaire générale de la défense et de la sécurité nationale
Guillaume Poupard, directeur général de l'ANSSI

Présentation de l'état de la menace

François Deruty, sous-directeur Opérations de l'ANSSI
Cyril Demonceaux, chef de la division Connaissance et anticipation de l'ANSSI

Présentation de la tendance scientifique

Vincent Strubel, sous-directeur Expertise de l'ANSSI
Timothée Ravier, chef de la cellule de développement CLIP OS de l'ANSSI

Présentation de la tendance stratégique-politique

Yves Verhoeven, sous-directeur Stratégie de l'ANSSI
Amélie Perron, chargée de mission affaires politiques européennes et internationales de l'ANSSI

L'actualité opérationnelle de l'ANSSI en 2018 a permis d'établir les grandes tendances de la menace observée en France et en Europe. Face à ces menaces, l'agence a déployé plusieurs stratégies de réponses. D'abord en resserrant les liens avec ses partenaires, au niveau national, comme européen. Ensuite en créant de nouveaux cadres d'échanges pour s'ouvrir et anticiper les problématiques du futur. Devant l'immensité des travaux à accomplir, l'objectif est de construire, dans un élan collectif, la confiance numérique de demain.

Ce dossier de presse met en lumière certains des travaux et des projets prioritaires pour l'ANSSI en 2018, qui sont présentés de manière plus exhaustive dans le rapport annuel.

I- ANALYSE DE LA MENACE EN 2018

LES 5 GRANDES TENDANCES OBSERVÉES EN FRANCE ET EN EUROPE

L'identité de l'ANSSI est fortement associée à son rôle de « cyberpompiers ». En 2018, l'activité opérationnelle de l'agence s'est caractérisée par la variété de ses interventions, des signalements aux incidents de sécurité en passant par la conduite d'opérations de cyberdéfense.

Ce travail réalisé et analysé au quotidien par la sous-direction Opérations de l'ANSSI, complété par les échanges avec les différents partenaires ont permis d'identifier **cinq grandes tendances de la menace observées en France et en Europe en 2018**.

Si les attaques les plus visibles prennent la forme de sabotage, **l'espionnage** est le risque qui pèse le plus sur les organisations. Il a été une préoccupation majeure pour l'ANSSI en 2018. Discrets, patients, et bénéficiant d'un financement important, les attaquants s'intéressent de plus en plus aux secteurs d'activité d'importance vitale et aux infrastructures critiques spécifiques, comme les secteurs de la défense, de la santé ou encore de la recherche.

« Des groupes très organisés préparent ce qui ressemble aux conflits de demain, en s'introduisant dans les infrastructures des systèmes les plus critiques. »
Guillaume Poupard, directeur général de l'ANSSI

L'agence a également observé une augmentation des **attaques indirectes** en 2018. En ciblant un ou plusieurs intermédiaires (fournisseur, prestataire, etc.), les attaquants parviennent à contourner les mesures de sécurité de très grandes organisations, pourtant de plus en plus conscientes du risque numérique. La compromission d'un seul intermédiaire suffit parfois à accéder à plusieurs organisations.

« Les attaquants exploitent de plus en plus les relations de confiance établies entre partenaires pour accéder aux informations qu'ils convoitent. »
Guillaume Poupard, directeur général de l'ANSSI

Les **opérations de déstabilisation et d'influence** ont été particulièrement nombreuses en 2018. Sans être très sophistiquées, ces attaques ont un fort impact symbolique, lié à la nature des cibles visées et aux revendications dont elles font l'objet.

Tout au long de l'année, l'ANSSI a pu observer une multiplicité d'attaques visant à **générer des cryptomonnaies**. Les attaquants, de plus en plus organisés en réseaux, profitent des failles de sécurité pour déposer discrètement des mineurs de cryptomonnaies. Contrairement aux rançongiciels, ces logiciels malveillants sont les plus discrets possibles.

Enfin, l'agence a constaté une montée en puissance de la **fraude en ligne**. Les grands opérateurs se préoccupant de plus en plus de leur sécurité numérique, les attaquants se tournent vers des cibles moins exposées mais plus vulnérables. De nombreuses campagnes d'hameçonnage ciblant des collectivités territoriales ou des acteurs du secteur de la santé ont été observées en 2018.



Pour en savoir plus sur les grandes tendances de la menace, rendez-vous à la page 6 du rapport annuel 2018 de l'ANSSI.

ACTUALITE OPÉRATIONNELLE*

2 1 869
signalements

Signalement : description détaillée des caractéristiques techniques d'évènements pouvant laisser penser qu'un incident de sécurité est survenu sur un système numérique.

391
incidents hors
opérateurs
d'importance vitale
(OIV)

Incident hors opérateurs d'importance vitale (OIV) : évènement indésirable ou inattendu qui présente une forte probabilité de menacer les systèmes numériques et de compromettre les opérations liées à l'activité d'une organisation, hors OIV.

16
incidents
majeurs

Incident majeur : évènement, indésirable ou inattendu, qui menace directement les systèmes numériques et compromet les opérations liées à l'activité d'une organisation.

14
opérations
de cyberdéfense

Opération de cyberdéfense menée par l'ANSSI : réponse à un incident de sécurité majeur menaçant directement les systèmes numériques et compromettant les opérations liées à l'activité d'une organisation d'importance vitale ou fortement sensible.

* Nombre d'interventions menées par l'ANSSI en 2018

EBIOS Risk Manager : L'IMPORTANCE DE L'ANALYSE DE RISQUE FACE AUX MENACES

L'ANSSI propose et met en œuvre plusieurs stratégies de réponse face à ces menaces. Le management et l'analyse de risque est l'une de ces réponses. Le lancement de la méthode EBIOS Risk Manager a été une étape importante pour l'agence en 2018. Pour accompagner la transformation numérique et ses acteurs vers plus de sécurité, l'ANSSI, en lien avec le Club EBIOS et le CLUSIF, a modernisé sa méthode d'analyse de risque. L'agence fournit une solution innovante et pratique, adaptée aux nouveaux enjeux de sécurité numérique.

« **Comprendre pour décider** », c'est la logique qui résume cette méthode. L'objectif est de permettre aux dirigeants d'appréhender au juste niveau les risques numériques qui pèsent sur leur organisation, au même titre que les risques stratégique, financier, juridique, d'image ou de ressources humaines.

« La gestion du risque numérique n'est pas seulement technique. Elle suppose l'implication de tous les échelons de l'organisation, de la direction aux équipes. »

Fabien Caparros, chef de division management de la sécurité numérique, sous-direction stratégie de l'ANSSI



Pour en savoir plus sur EBIOS Risk Manager, rendez-vous à la page 41 du rapport annuel 2018 de l'ANSSI.

II- RESSERRER LES LIENS AVEC NOS PARTENAIRES

La sécurité doit sortir de son domaine réservé pour associer l'ensemble des acteurs de la société numérique. L'ANSSI entraîne et anime un réseau d'acteurs extrêmement large pour avancer de manière efficace dans un élan commun.

« L'écosystème se transforme au contact de l'ANSSI et inversement. »

Emmanuel Germain, directeur général adjoint de l'ANSSI

RENFORCER LES PARTENARIATS AVEC LES SECTEURS PUBLIC ET PRIVÉ

En 2018, l'agence a développé et resserré des partenariats au niveau national, avec des acteurs de la sphère publique et de la sphère privée.

Des partenariats public-public

De nombreuses initiatives se sont concrétisées en 2018 grâce à une étroite coopération interministérielle. Si certaines visent directement le développement sécurisé de services de l'État, d'autres favorisent l'essor d'une culture de la sécurité auprès du plus grand nombre.

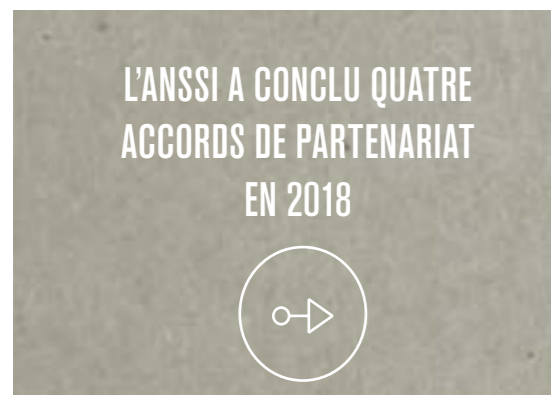
L'ANSSI travaille main dans la main avec la direction interministérielle du numérique et du système d'information et de communication de l'État (DINSIC). Une collaboration sur le long-terme qui s'est notamment illustrée en 2018 par la publication du **guide « Agilité et sécurité numériques : méthode et outils à l'usage des équipes projets »**.



Pour en savoir plus sur la coopération interministérielle, rendez-vous à la page 18 du rapport annuel 2018 de l'ANSSI.

Face à l'ampleur de ces nouvelles menaces, l'ANSSI a consolidé les liens tissés avec ses partenaires, au niveau national, comme au niveau européen.

L'ANSSI a également eu à cœur de **développer les accords sectoriels**. En 2018, l'agence et plusieurs autorités nationales sectorielles se sont engagées en faveur d'une coopération renforcée pour protéger les systèmes d'information.



17 janvier 2018
Accord avec l'Autorité de contrôle prudentiel et de résolution (ACPR)

16 février 2018
Accord avec l'Autorité des marchés financiers (AMF)


20 mars 2018
Accord avec l'Établissement public de sécurité ferroviaire (EPSF)

13 juillet 2018
Accord avec la Direction de la sécurité de l'aviation civile (DSAC)

 Pour en savoir plus sur les accords sectoriels, rendez-vous à la page 21 du rapport annuel 2018 de l'ANSSI.

Touchant de manière transversale l'ensemble des secteurs, les **actions territoriales ont été renforcées** en 2018. Les questions de sécurité économique et de sécurité numérique sont au cœur des préoccupations des entreprises et du tissu local. C'est à partir de ce constat que l'ANSSI et le Service de l'information stratégique et de la sécurité économiques (SISSE) ont créé le **dispositif SecNumEco**. Les événements SecNumEco transmettent les outils indispensables aux décideurs pour faire face aux risques, qui pèsent sur les structures publiques et privées, de toutes tailles. En 2018, dix rendez-vous SecNumEco se sont tenus à travers toute la France.



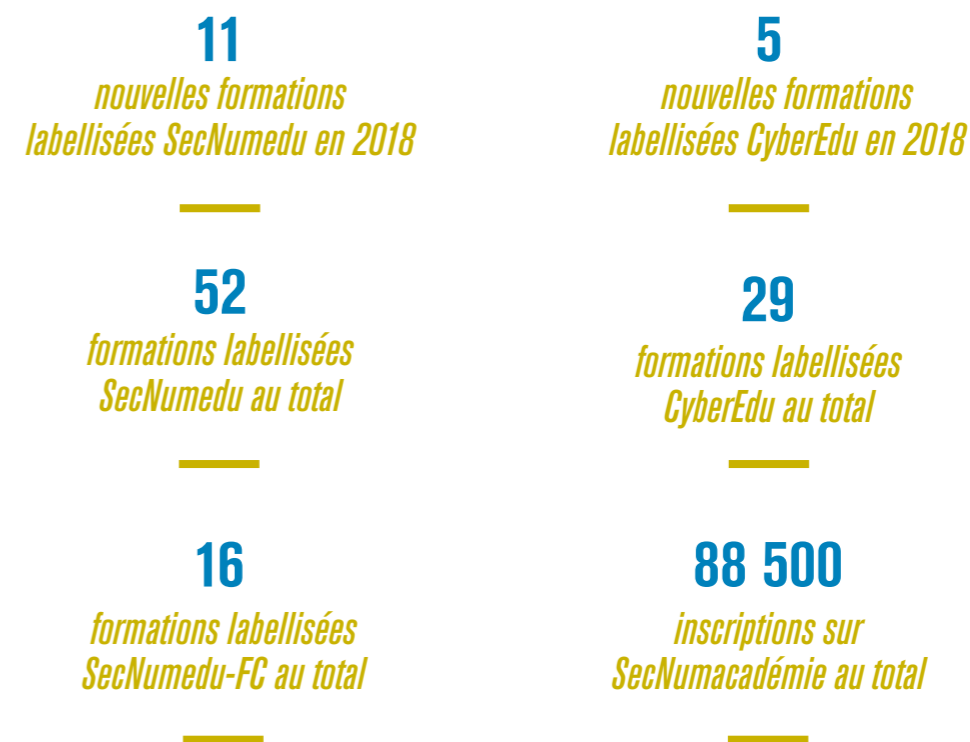
 Pour en savoir plus sur SecNumEco, rendez-vous à la page 23 du rapport annuel 2018 de l'ANSSI.

L'ensemble du territoire est confronté à une pénurie de talents dans le domaine de la cybersécurité. Les besoins d'experts en cybersécurité des entreprises et des organisations sont démesurés face au peu de candidats sur le marché. Pour répondre à ces enjeux, **la formation a été un axe de travail majeur pour l'ANSSI en 2018**, qui avance main dans la main avec les acteurs du domaine.

L'agence a renforcé et développé **des labels et des partenariats pour former et responsabiliser**. Le dispositif **SecNumedu** qui labellise des formations initiales en cybersécurité de l'enseignement supérieur a été complété en 2018 par le programme **SecNumedu-FC**. Lancé par le Centre de formation à la sécurité des systèmes d'information (CFSSI) de l'ANSSI, SecNumedu-FC référence les formations continues dédiées à la sécurité numérique et permet d'éclairer les choix des employeurs. S'ajoute à ces programmes le dispositif **CyberEdu**, qui labellise des formations supérieures en informatique intégrant un volet sécurité numérique.

Enfin, le programme de sensibilisation en ligne **SecNumacadémie** a connu un véritable succès en 2018, obtenant le prix « Coup de cœur des internautes » 2018 lors de la cérémonie *MOOC of the year*. Cette réussite confirme les attentes des citoyens dans ce domaine.

LA FORMATION EN CHIFFRES



Pour aller plus loin, il est primordial de faire entrer la sécurité numérique dans les programmes scolaires. Une véritable volonté politique incite à renforcer la sensibilisation aux enjeux de la sécurité numérique dès le plus jeune âge à l'école.

« *La sécurité numérique doit faire son entrée dans les manuels scolaires et la formation professionnelle, pour faire de chacun un acteur engagé.* »
Guillaume Poupard, directeur général de l'ANSSI



Pour en savoir plus sur SecNumedu-FC et sur les enjeux de la formation, rendez-vous à la page 25 du rapport annuel 2018 de l'ANSSI.

En complément des partenariats noués avec divers organismes publics, l'ANSSI tisse des liens forts avec les acteurs du privé, dans le but de développer un écosystème de confiance.

Des partenariats public-privé

En 2018, l'agence a renforcé ses liens avec l'industrie en remettant ses premiers **Visas de sécurité**. Ces derniers donnent une meilleure lisibilité à l'offre de solutions et de services numériques sécurisés.

CERTIFICATIONS

- 25** certifications de sécurité de premier niveau (GSPN) de produits
- 68** certificats critères communs (CC) de produits
- 12** certificats CC de sites
- 3** certificats CC de profils de protection

QUALIFICATIONS

- 15** produits
- 36** prestataires

CENTRES D'ÉVALUATION AGRÉÉS

- 15** centres d'évaluation de la sécurité des technologies de l'information (CESTI) de services



Pour en savoir plus sur les Visas de sécurité, rendez-vous à la page 25 du rapport annuel 2018 de l'ANSSI.

Dans un monde numérique sans frontières, les partenariats noués au niveau national doivent impérativement être complétés par des accords au niveau européen.

LA FRANCE MOTEUR EUROPÉEN DE LA CONFIANCE NUMÉRIQUE

La France et l'Europe ont un rôle majeur à jouer pour limiter le développement d'un far West numérique. L'ANSSI s'est fortement impliquée dans toutes les initiatives européennes de responsabilisation de l'ensemble des acteurs de l'écosystème.

Directive NIS : l'ANSSI accompagne les premiers opérateurs de services essentiels

La directive européenne *Network and Information Security (NIS)* donne l'opportunité à la France de renforcer le niveau de sécurité de nouveaux acteurs : **les opérateurs de services essentiels (OSE)**. Ces derniers fournissent un service essentiel dont l'interruption aurait un impact significatif sur le fonctionnement de l'économie ou de la société.

Pilote de la transposition de la directive en France, l'ANSSI a mis en place une démarche d'accompagnement des OSE progressive, ouverte et qualitative. La France a identifié 122 OSE au stade de l'échéance du 9 novembre 2018. Les dossiers de désignation d'une centaine d'opérateurs additionnels sont en cours d'instruction.

« *La démarche de la France, s'appuyant largement sur l'expérience positive des démarches conduites avec les opérateurs d'importance vitale depuis 2013, a pour ambition d'élever au juste niveau la sécurité des réseaux et des systèmes d'information, en national mais également à l'échelle européenne* »

Guillaume Poupard, directeur général de l'ANSSI



26 février 2018

Promulgation de la loi n° 2018-133 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité

25 mai 2018

Publication du décret n° 2018-384 du 23 mai 2018

13 juin 2018

Publication de l'arrêté portant sur les modalités de déclaration des incidents

1^{er} août 2018

Publication de l'arrêté relatif au coût des contrôles par l'ANSSI

29 septembre 2018

Publication de l'arrêté sur les règles de sécurité des OSE et leurs délais d'application

La directive NIS responsabilise les OSE, nouveaux acteurs sur la scène cyber. L'Appel de Paris tend vers cette même logique de responsabilisation et vise les Etats, les acteurs privés et la société civile.

L'Appel de Paris invite Etats, organisations et société civile à s'engager

Suite à la publication de la Revue stratégique de cyberdéfense en février 2018, le ministère de l'Europe et des affaires étrangères et l'ANSSI ont défini l'ambition française visant à préciser et **renforcer les responsabilités des acteurs privés de l'écosystème numérique**.

Une ambition soulignée lors de l'Appel de Paris pour la confiance et la sécurité dans le cyberspace, lancé en novembre dernier par le président de la République. Il invite les États, utilisateurs et acteurs économiques à assumer une responsabilité partagée dans la stabilisation du cyberspace.

« La France a fait de la promotion de la paix et du renforcement de la stabilité du cyberspace l'une de ses priorités. »
Guillaume Poupard, directeur général de l'ANSSI

Une « zone d'incertitude » sur ce qu'il est permis ou non de faire existe aujourd'hui, porteuse de flou juridique et d'instabilité. De plus, l'absence d'obligations pour les acteurs privés de concevoir et de maintenir des solutions numériques parfaitement sécurisées accroît le risque de déstabilisation à l'échelle internationale. Des situations qu'il est nécessaire de clarifier et de traiter au niveau national comme international, tant pour les acteurs privés que pour les services de l'État.

« La France défend le besoin d'objectiver les termes du débat sur des problématiques comme le hackback et la cyberdéfense active. Seule cette approche permettra de dépassionner les échanges et de fixer collectivement les limites de ces pratiques. »
Yves Verhoeven, sous-directeur Stratégie de l'ANSSI



Pour en savoir plus sur l'Appel de Paris et la responsabilité des acteurs privés, rendez-vous à la page 27 du rapport annuel 2018 de l'ANSSI.

L'Appel de Paris a été un moment fort de 2018. Cette année a également été déterminante pour les pays membres de l'Union européenne (UE) et pour l'ENISA, grâce à la concrétisation du *Cybersecurity Act*.

Cybersecurity Act : une avancée déterminante les pays membres de l'UE et pour l'ENISA

Issu de la feuille de route de la Commission européenne en matière de sécurité du numérique, le *Cybersecurity Act* a fait l'objet d'intenses négociations depuis un an.

Le règlement européen traite deux sujets distincts mais complémentaires. D'une part, il permet l'adoption d'un **mandat permanent pour l'ENISA**, l'Agence européenne pour la cybersécurité, valorisant et développant son rôle de facilitateur des échanges entre les Etats membres. D'autre part, il définit un **cadre européen de certification de cybersécurité** pour harmoniser à l'échelle européenne les méthodes d'évaluation et les différents niveaux d'assurance de la certification.

« L'ANSSI a plaidé pour que l'UE se dote d'un mécanisme de reconnaissance mutuelle des certificats de cybersécurité. C'est pourquoi nous étions satisfaits que la Commission européenne propose la mise en place d'un cadre européen de certification européen. »

Amélie Perron, chargée de mission affaires politiques européennes et internationales de l'ANSSI

En tant que cheffe de file des autorités françaises, l'ANSSI se félicite de l'adoption par le Parlement européen et le Conseil de l'Union européenne du *Cybersecurity Act*, qui marque une **véritable avancée pour l'autonomie stratégique européenne**.

« Forte de vingt années d'expérience en matière de certification, la France a joué un rôle moteur lors des négociations européennes, avec pour objectif d'élever le niveau de sécurité en Europe. Il est primordial de réconcilier la croissance du marché avec les enjeux de cybersécurité »

Guillaume Poupard, directeur général de l'ANSSI



Pour en savoir plus sur le *Cybersecurity Act*, rendez-vous à la page 29 du rapport annuel 2018 de l'ANSSI.

Année riche et prometteuse, 2018 a permis à l'ANSSI de resserrer ses liens avec ses partenaires, au niveau national, comme européen, afin de construire ensemble la société numérique de demain. Pour aller au-delà et anticiper les problématiques du futur, l'agence a développé de nouveaux cadres d'échanges.

III- CRÉER DE NOUVEAUX CADRES D'ÉCHANGES POUR GARDER UN TEMPS D'AVANCE

Forte de son expérience et de son expertise, l'ANSSI mobilise son écosystème pour avancer dans un élan collectif vers les sujets d'avenir. L'anticipation a été le mot-clé de 2018 et trace la voie pour les années à venir.

ANTICIPER : UN PRÉREQUIS POUR L'AVENIR

Les technologies de demain, comme l'intelligence artificielle, la santé connectée ou l'informatique quantique vont bouleverser la manière de travailler de l'ANSSI et de son écosystème. Face à ce constat, l'activité de recherche de l'agence entre dans une nouvelle dynamique pour relever, aux côtés d'experts reconnus, les nouveaux défis de la sécurité numérique.

Un groupe de travail stratégique pour anticiper les usages

L'ANSSI assume une mission de vigie technologique. Elle doit anticiper suffisamment tôt les ruptures technologiques et l'évolution des usages pour les accompagner efficacement. C'est pourquoi l'agence a créé en 2018 un groupe de travail interne, pour identifier et comprendre les grandes tendances des usages émergents chez ses publics.

Les travaux en cours sur la perte de notion de périmètre du système d'information, les systèmes cyber-physiques et l'intelligence artificielle ont vocation à être commentés et enrichis par d'autres.



Pour en savoir plus sur le groupe de travail sur les usages, rendez-vous à la page 50 du rapport annuel 2018 de l'ANSSI.

Ce groupe de travail interne s'ouvre à l'avis et aux contributions d'acteurs extérieurs. Dans cette même logique d'ouverture, l'ANSSI a créé en 2018 le conseil scientifique.

Le conseil scientifique

Très à l'écoute de l'avis de ses pairs, la division Scientifique et technique de l'ANSSI a constitué un conseil scientifique, dont l'activité débutera au cours du premier semestre 2019. Pour générer des résultats, la réflexion doit être collective, ouverte et associer une diversité d'expertises. C'est pourquoi le conseil scientifique regroupe des experts extérieurs à l'agence. Il a été mis en place pour faciliter les interactions entre l'ANSSI et le monde académique et pour orienter les travaux scientifiques de l'agence.

« La création du conseil scientifique, grande nouveauté de 2018, marque la volonté d'ouverture de l'ANSSI »

Vincent Strubel, sous-directeur Expertise de l'ANSSI



Pour en savoir plus sur le conseil scientifique, sur les usages, rendez-vous à la page 48 du rapport annuel 2018 de l'ANSSI.

L'anticipation, qui s'est imposée comme un axe de travail majeur pour l'ANSSI en 2018, se développe dans une logique d'ouverture et partage.

L'OUVERTURE ET LE PARTAGE POUR MOTS D'ORDRE

Face à l'immensité des travaux à mener dans le cyberspace, l'ANSSI ne peut pas avancer seule. L'ouverture et le partage sont des leviers décisifs pour l'agence, qui travaille de plus en plus en Open Source.

Open Source : un acte de transparence

Progressivement, l'ANSSI ouvre ses productions à l'appréciation de ses publics. Elle rejoint des espaces de dialogue et en crée d'autres avec un objectif clair : favoriser la transmission de compétences et de connaissances.

« Nous sommes persuadés que l'Etat doit activement participer à l'Open Source. Ces projets et la communauté qui les anime ont un potentiel considérable. »

Yann Bonnet, directeur de cabinet de l'ANSSI

L'ANSSI contribue actuellement à 13 projets Open Source, à retrouver sur le GitHub de l'agence. Renforcée par le succès des récentes expériences, cette démarche Open Source se développe de plus en plus.

« Nous croyons fermement en la capacité des projets Open Source à diffuser une culture de la sécurité numérique. »

Timothée Ravier, chef de la cellule de développement CLIP OS de l'ANSSI

Plusieurs projets Open Source se sont concrétisés en 2018, notamment CLIP OS et l'outil ORADAD pour évaluer le niveau de sécurité de son *Active Directory*.

Evaluer le niveau de sécurité de son *Active Directory* avec l'outil **ORADAD**

Les audits et les opérations de cyberdéfense menés par l'ANSSI montrent un manque de maturité critique récurrent sur la sécurité des annuaires *Active Directory* (AD)*, point névralgique dans les systèmes d'information *Windows*. L'agence constate même que le niveau de sécurité des annuaires AD baisse au fur et à mesure du temps et de la vie du système d'information. L'ensemble affaiblit significativement le niveau global de sécurité du système.

Face à ce constat, le bureau Audits de l'ANSSI a développé un nouveau service. Il propose d'auditer régulièrement, à la demande et de manière autonome, le niveau de sécurité des AD des ministères. A l'issue de l'audit, l'ANSSI transmet une indication globale (sur une échelle de 1 à 5) du niveau de sécurité de la configuration de l'AD, avec des recommandations adaptées.

Dans une démarche de transparence, l'agence a publié le code source de **l'outil de collecte ORADAD** sur GitHub. Développé en amélioration continue, ce nouveau service bénéficie des retours et commentaires de ses utilisateurs.

* *Active Directory* (AD) est un annuaire introduit par Windows 2000 Server. Son implémentation permet de centraliser des informations relatives aux utilisateurs et aux ressources d'une entreprise en fournissant des mécanismes d'identification et d'authentification tout en sécurisant l'accès aux données. Un annuaire AD contient des secrets des utilisateurs, comme, par exemple, leurs informations d'identification. Il constitue donc une cible privilégiée pour une personne malveillante.



Pour en savoir plus sur ce nouveau service, rendez-vous à la page 47 du rapport annuel 2018 de l'ANSSI.

CLIP OS

L'ANSSI a élaboré un système d'exploitation multiniveaux sécurisé dénommé CLIP OS. Basé sur un noyau Linux et capable de gérer des informations de plusieurs niveaux de sensibilité, CLIP OS est disponible en Open Source. L'objectif est de l'enrichir sur la durée, grâce aux développements de l'ANSSI et aux contributions de la communauté, afin de mieux répondre aux usages et aux besoins spécifiques de chaque déploiement.

« La sortie de CLIP OS en septembre 2018 a suscité de nombreuses réactions. Je retiens tout particulièrement le Paris Open Source Summit de décembre qui nous a permis d'échanger directement avec des membres de la communauté très attentifs au développement de telles initiatives. »

Timothée Ravier, chef de la cellule de développement CLIP OS de l'ANSSI

Après la sortie de la version Alpha du système en septembre 2018, l'agence travaille désormais à une version Bêta disposant des briques de base indispensables à un déploiement à plus grande échelle.



Pour en savoir plus sur CLIP OS, rendez-vous à la page 45 du rapport annuel 2018 de l'ANSSI.



Le constat est sans appel : 2018 prouve une nouvelle fois que le risque numérique doit être au cœur de nos préoccupations. Les attaques informatiques touchent toute la société, c'est pourquoi nous devons tous nous emparer du sujet.

L'année 2018 nous a donné l'occasion d'exprimer collectivement cette conviction. L'Appel de Paris, le *Cybersecurity Act*, les accords de coopération sectoriels ou encore la participation de l'agence à la communauté Open Source en sont de parfaits exemples. En prenant un temps d'avance sur les tendances scientifiques, l'ANSSI entraîne avec elle une large communauté d'acteurs qui, plus que jamais, doivent s'approprier les enjeux de sécurité numérique.

À PROPOS DE L'ANSSI

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a été créée par le décret n° 2009-834 du 7 juillet 2009 sous la forme d'un service à compétence nationale.

L'agence assure la mission d'autorité nationale en matière de défense et sécurité des systèmes d'information. Elle est rattachée au secrétaire général de la défense et de la sécurité nationale, sous l'autorité du Premier ministre.

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI — 51, boulevard de la Tour-Maubourg — 75 700 PARIS 07 SP

www.ssi.gouv.fr — communication@ssi.gouv.fr





CONTACTS PRESSE:

communication@ssi.gouv.fr

Margaux Vincent
margaux.vincent@ssi.gouv.fr
01 71 75 84 04