23 JANVIER 2018

DOSSIER DE PRESSE

SECURITÉ DU NUMÉRIQUE & EUROPE

2018, UNE ANNÉE DÉTERMINANTE À L'ÉCHELLE EUROPÉENNE

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI

SOMMAIRE

Conférence de presse
23 janvier à 14h30 - Salon presse Lille Grand Palais

COMMUNIQUÉ DE PRESSE - FIC 2018

SÉCURITÉ DU NUMÉRIQUE : 2018, UNE ANNÉE DÉTERMINANTE À L'ÉCHELLE EUROPÉENNE

Transposition de la directive NIS, négociations sur la feuille de route sur la cybersécurité présentée par la Commission européenne… l'année 2018 verra naître ou se concrétiser de nombreux projets structurants en matière de cybersécurité à l'échelle européenne. En tant qu'autorité nationale en matière de cybersécurité et de cyberdéfense, l'ANSSI s'est fortement impliquée dans les travaux menés par l'Union européenne et ses homologues européens. Son objectif : le développement d'un cyberespace ouvert, stable, sûr et de confiance.

Une ambition pour l'ANSSI : tirer profit des enseignements nationaux en matière de réglementation, de certification, de recherche ou encore de sensibilisation, pour construire ensemble l'autonomie stratégique de l'Union et renforcer la sécurité de l'écosystème européen, en complémentarité des responsabilités propres aux Etats membres.

Le **Forum International de la Cybersécurité** (FIC) sera l'occasion pour Guillaume Poupard de présenter les objectifs de l'ANSSI à l'occasion de sa conférence de presse :

RENFORCER LA SÉCURITÉ DU NUMÉRIQUE EN EUROPE

La sécurité de la France dépend de l'Europe, et inversement. Une Europe forte et de confiance c'est donc à la fois des capacités nationales réelles des Etats membres en matière de cybersécurité et la mise en place d'une coopération efficace.

De nombreux projets vont contribuer au développement d'un socle de capacités de cybersécurité dans tous les Etats membres, et favoriser l'émergence de cadres de coopération pour faire face aux cyberattaques. L'ANSSI accueille très favorablement le d**éveloppement du réseau des CSIRT**, une base précieuse d'échanges entre les Etats qui permettra à terme une réponse collective et coordonnée en cas de cyberattaques.

La feuille de route de l'exécutif européen en matière de sécurité du numérique dévoilée par la Commission européenne en septembre 2017, qui contient des propositions à cet égard, donnera lieu à de nombreux échanges dans les enceintes européennes.

L'ANSSI prendra ainsi activement part aux négociations sur la **révision du mandat de l'ENISA**, introduit dans le « paquet cyber » de la Commission européenne. L'ANSSI continuera de soutenir les efforts capacitaires et de coordination entre Etats membres portés par l'agence européenne, notamment en participant à l'exercice de gestion de crise **Cyber Europe**.

CONCILIER DÉVELOPPEMENT DU NUMÉRIQUE ET RÉGULATION À L'ÉCHELLE EUROPÉENNE

Le marché seul ne peut pas tout faire, les Etats membres ont un rôle à jouer pour construire collectivement les conditions de sécurité indispensables pour accompagner la transformation numérique de l'Union européenne.

L'ANSSI défend l'idée que l'Union européenne doit préserver sa capacité à protéger les citoyens, les entreprises et les Etats membres en matière numérique.

Les 28 Etats membres doivent ainsi transposer dans leur droit national **la directive Network and Information Security (NIS)** pour mai 2018. Forte des enseignements tirés de la mise en œuvre du dispositif de cybersécurité des opérateurs d'importance vitale (OIV) introduit par la loi de programmation militaire de 2013, l'ANSSI est en charge d'élaborer un nouveau dispositif de sécurité à destination des opérateurs de services essentiels (OSE).

CONSTRUIRE UNE INDUSTRIE ET UNE RECHERCHE EUROPÉENNES FORTES

L'Europe est l'échelon naturel pour accompagner le développement d'une industrie forte, compétitive et innovante, tirant pleinement profit de l'expertise développée par les Etats membres.

L'ANSSI, avec l'appui des acteurs publics et privés, défend la mise en œuvre d'une politique industrielle européenne ambitieuse ainsi que le développement d'une R&D de pointe, deux axes indispensables au déploiement de technologies et de services numériques de confiance. Dans le cadre des négociations au niveau européen, l'agence s'attache à promouvoir l'adoption d'un **cadre européen de certification de sécurité robuste**, qui tirera pleinement bénéfice du retour d'expérience des Etats précurseurs.

Enfin, l'ANSSI est activement impliquée dans les travaux pilotés dans le cadre de la mise en œuvre du **Partenariat Public-Privé européen pour la cybersécurité (cPPP)** et en particulier la définition des projets de cybersécurité financés par le fonds européen H2020.

SENSIBILISER LES EUROPÉENS AUX ENJEUX DE LA CYBERSECURITÉ

Un mot d'ordre : la sécurité du numérique est à portée de clic !

Dernière séquence européenne de l'année 2018 : l'ANSSI, en lien avec ses partenaires nationaux, pilotera en France l'édition 2018 du **Mois européen de la cybersécurité**, une campagne de sensibilisation européenne organisée en octobre, et aujourd'hui, un évènement incontournable en Europe.

RENFORCER LA SÉCURITÉ DU NUMÉRIQUE EN EUROPE

La sécurité de la France dépend de l'Europe, et inversement. Une Europe forte et de confiance c'est donc à la fois des capacités nationales réelles des Etats membres en matière de cybersécurité et la mise en place d'une coopération efficace.

Les attaques du printemps 2017 « wannacry » et « notPetya » ont démontré à la fois l'ampleur internationale des cyberattaques, que l'on soit ciblé ou non, mais aussi l'interdépendance de nos sociétés et notre vulnérabilité partagée, victime des effets «collatéraux» de certaines attaques. D'où l'importance à la fois de renforcer les capacités de cybersécurité de tous les Etats membres et des institutions européennes (Cert-EU), et de faire émerger des cadres de coopération efficicace pour faire face aux risques ensemble efficacement.

De nombreux projets, dont la transposition de la directive NIS par les 28 Etats membres de l'Union, vont contribuer à ces deux objectifs (cf. schéma p6). L'ANSSI accueille en particulier très favorablement le d**éveloppement du réseau des CSIRT**, une base précieuse d'échanges entre les Etats qui permettra à terme une réponse collective et coordonnée en cas de cyberattaques.

Depuis près de 20 ans, l'ANSSI à travers le CERT-FR représente la France dans de nombreux groupement de CERT européens et internationaux. La multiplication des vagues d'attaques sans frontières ont mis en évidence la nécessité de pouvoir s'appuyer sur un réseau global de vigilance à l'échelle européenne. La formalisation d'un réseau des CSIRT nationaux des 28 états membres contribuera à assurer un niveau élevé commun de sécurité grâce à des échanges opérationnels sur des attaques ciblant des pays européens, et ce 24 heures sur 24.

L'ANSSI suit de près les nombreux échanges dans les enceintes européennes. suite à la publication à la rentrée de la feuille de route de l'exécutif européen, connue sous le terme de «paquet cyber» (cf. encadré). L'ANSSI prendra notamment activement part aux négociations sur la **révision du mandat de l'ENISA**.

L'agence, qui soutient de longue date l'ENISA et en assure la présidence du Conseil d'administration, plaide pour une agence européenne au mandat ambitieux, avec des missions renforcées et complémentaires aux prérogatives des Etats notamment :

- en soutien des Etats membres, pour le renforcement de leurs capacités nationales techniques et opérationnelles ;
- en appui à la coopération entre les Etats membres.

Ce rôle de coordination entre les Etats membres sera mis à l'épreuve lors de la prochaine édition de l'exercice de crise **CyberEurope**, pour lequel l'ANSSI jouera pleinement son rôle d'autorité nationale et de membre actif du réseau d'échanges des CSIRTs.

LE «PAQUET CYBER» EN BREF

La Commission européenne a présenté, le 13 septembre dernier, un "paquet cybersécurité" qui constitue la feuille de route de l'exécutif européen pour la fin de son mandat, jusqu'en 2019.

Il est composé de plusieurs textes :

- une communication chapeau « sur la résilience, la dissuasion et la défense pour la cybersécurité de l'UE » listant les actions prioritaires pour les prochaines années, dans laquelle est annoncée la création d'un centre européen consacré à la recherche et la compétence cyber, dont les missions sont à ce stade principalement centrées sur la R&D ;

- une proposition de règlement européen incluant un nouveau mandat de l'agence européenne de sécurité des réseaux et de l'information (ENISA) renommée « agence européenne de cybersécurité » et la création d'un cadre européen de certification de sécurité, visant à l'élaboration de schémas de certification ;

- une recommandation proposant un cadre européen de réponse aux crises cyber (« blueprint ») ;

- une communication précisant certaines modalités de mise en œuvre de la directive NIS (sécurité des réseaux et des systèmes d'information), adoptée en juillet 2016.

LA DIRECTIVE NETWORK AND INFORMATION SECURITY (NIS) EN BREF

Renforcement des capacités nationales des Etats membres par la mis en oeuvre de dispositifs de cybersécurité nationaux

une autorité nationale, le point de contact privilégié

une stratégie nationale en matière de cybersécurité

un centre de réponse aux incidents

Coopération entre les Etats membres sur des aspects politiques et opérationnels reposant sur deux enceintes

un groupe de coopération des Etats membres

un réseau européen des CSIRT des Etats membres

Renforcement de la cybersécurité des opérateurs de services essentiels au fonctionnement de l'économie et de la société (OSE)

Identification des OSE et des systèmes d'information essentiels (SIE)

Application de mesures de sécurité et mise en place de contrôle de sécurité

Déclaration des incidents critiques sur les SIE

Renforcement de la cyber-sécurité des fournisseurs de service numérique (FSN) : places de marché en ligne, moteur de recherche, services d'informatiques en nuage

Identication des FSN et des systèmes d'information nécessaires à la fourniture de leurs services

Respect des exigences de sécurité

Déclaration des incidents critiques sur les SI

CONCILIER DÉVELOPPEMENT DU NUMÉRIQUE ET RÉGULATION À L'ÉCHELLE EUROPÉENNE

Le marché seul ne peut pas tout faire, les Etats membres ont un rôle à jouer pour construire collectivement les conditions de sécurité indispensables pour accompagner la transformation numérique de l'Union européenne.

L'approche française, de plus en plus partagée en Europe, défend l'idée que l'Union européenne doit préserver sa capacité à protéger les citoyens, les entreprises et les Etats membres en matière de sécurité du numérique. Cette protection peut prendre une forme réglementaire, adaptée aux exigences du marché mais aussi aux valeurs communes aux pays européens et portée par les Etats membres.

L'un des principaux enjeux de l'année 2018 est ainsi la transposition de la **directive Network and Information Security (NIS)** en France. Cheffe de file des négociations de la directive, adoptée par les institutions européennes le 6 juillet 2016, l'ANSSI mène depuis plus d'un an les travaux de transposition, en concertation avec les ministères et les différentes parties-prenantes nationales.

La proposition de loi a été étudiée par le Conseil d'Etat et adoptée en première lecture par le Sénat. Elle poursuit son parcours législatif par un passage à l'Assemblée nationale prévue le 31 janvier.

La directive poursuit un objectif principal : assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information de l'Union européenne. L'un des volets du texte prévoit notamment la définition et l'identification de nouveaux acteurs, essentiels pour la vie quotidienne des Français, à protéger grâce à la mise en oeuvre d'un dispositif de cybersécurité dédié : les **opérateurs de services essentiels (OSE).**

Un OSE fournit un service essentiel (SE) dont l'interruption aurait un impact significatif sur le fonctionnement de l'économie ou de la société.

Ces OSE devront garantir un socle minimal de cybersécurité pour se protéger d'une attaque cyber aux conséquences majeures sur le fonctionnement de l'économie et de la société.

La protection de ces opérateurs, privés ou publics, intervient en complémentarité du dispositif de cybersécurité des **opérateurs d'importance vitale (OIV)** introduit par la loi de programmation militaire (LPM) de 2013 face à l'augmentation en quantité et en sophistication des attaques informatiques, et à leurs impacts potentiellement destructeurs sur la Nation.

Un OIV exploitent ou utilisent des installations jugées indispensables pour la survie de la Nation.

Après de nombreuses consultations, l'ANSSI a défini un cadre réglementaire - une première en Europe - avec pour objectif d'accompagner les OIV dans la sécurisation de leurs systèmes d'information sensibles. Pour mener les travaux de transposition de la directive, l'ANSSI a capitalisé sur la méthodologie appliquée au niveau national et un premier retour d'expérience suite à la publication des premiers arrêtés sectoriels en juillet 2016.

CONSTRUIRE UNE INDUSTRIE ET UNE RECHERCHE EUROPÉENNES FORTES

L'Europe est l'échelon naturel pour accompagner le développement d'une industrie forte, compétitive et innovante, tirant pleinement profit de l'expertise développée par les Etats membres.

Un cyberespace sûr et de confiance doit pouvoir se reposer sur un écosystème de la cybersécurité compétent, fiable et responsable. A l'échelle nationale, l'ANSSI a toujours valorisé les échanges avec les acteurs publics et privés qui évoluent au sein de cet écosystème pour mettre en place des réglementations claires, justes et adaptées aux exigences du marché.

La sortie des **«Visas de sécurité ANSSI»** notamment répond à cet objectif de lisbililté et de valorisaton de l'expertise française dans son ensemble en matière de cybersécurité et cyberdéfense. C'est cette vision que l'agence soutiendra à l'échelle européenne dans les prochains mois lors des négociations de la feuille de route cybersécurité de la Commission européenne.

L'ANSSI défend ainsi l'adoption d'un **cadre européen de certification de sécurité robuste**, qui tirera pleinement bénéfice du retour d'expérience des Etats précurseurs et de l'industrie européenne depuis plus de vingt ans. Reconnue de niveau mondial, cette expertise, française et allemande notamment, sera incontournable dans la gouvernance de la certification.

Afin d'élever le niveau de sécurité en Europe, il est crucial que ce cadre permette de couvrir tout l'éventail des niveaux de sécurité, jusqu'aux plus élevés. Pour ces derniers, l'ANSSI soutient que la résistance des produits aux capacités des attaquants doit être démontrée.

Au-delà d'un cadrage commun des activités existante, l'ANSSI, avec l'appui des acteurs publics et privés, défend la mise en œuvre d'une **politique scientifique, technologique et industrielle ambitieuse**. Seule le développement d'une R&D innovante et de pointe apportera aux adminsitrations, aux entreprises et aux citoyens européens des solutions numériques sécurisées et de confiance, en phase avec les évolutions technologiques actuelles.

L'ANSSI s'implique donc naturellement dans les travaux pilotés dans le cadre de la mise en œuvre du **Partenariat Public-Privé européen pour la cybersécurité (cPPP)** et en particulier la définition des projets de cybersécurité financés par le fonds européen H2020. Enfin, l'agence participe à la création du réseau des centres de cybersécurité, avec à son coeur, un centre de recherches et de compétences, un projet annoncé dans la feuille de route de la Commission européenne.

SENSIBILISER LES EUROPEENS AUX ENJEUX DE LA CYBERSECURITE

Un mot d'ordre : la sécurité du numérique est à portée de clic !

Vol d'information ou de propriété intellectuelle, atteinte aux données personnelles, attaques de rançongiciels… La sécurité du numérique ne peut se faire sans l'implication des citoyens. L'ANSSI, ses homologues européennes et les institutions de l'Union, s'engagent pleinement en faveur de la sensibilisation des Européens vis-à-vis des risques associés aux usages du numérique et la diffusion de bonnes pratiques.

L'Agence, en lien avec ses partenaires nationaux, pilotera à nouveau en 2018 l'édition française du « **Mois européen de la cybersécurité** ». Cette campagne de sensibilisation dans l'ensemble de l'Union s'inscrit déjà comme un rendez-vous incontournable de la cybersécurité en Europe pour 2018.

Pourquoi ce mois de sensibilisation est-il important ?

Cette campagne de sensibilisation contribue à la nécessaire **prise de conscience globale et collective** des enjeux liés à la sécurité du numérique par tous les acteurs de la société, des entreprises aux citoyens européens pour élever le niveau de sécurité global ;

Une mobilisation soutenue et partagée par tous les acteurs nationaux de la sécurité du numérique permettra de valoriser et de confirmer le **rôle d'acteur européen de premier plan** joué par la France en matière de sensibilisation, en complémentarité des travaux ménés au niveau réglementaire, capacitaire et technologique.

La participation à un événement d'envergure européenne est l'occasion de faire connaître les problématiques et activités de sensibilisation définis au niveau européen, en lien avec l'ENISA, et les autres pays européens.

A 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

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
SGDSN

CONTACT PRESSE :

Anne-Charlotte Brou
anne-charlotte.brou@ssi.gouv.fr
01 71 75 82 97

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