Programme de Développement Concerté de l'Administration Numérique Territoriale

Axe – Socle commun

- ETAT ET TERRITOIRES : LA CYBER-SÉCURITÉ -

Action 8 / semestre 1 : Valoriser les actions de l'ANSSI dans l'offre de services de l'Etat auprès des collectivités territoriales

Version 1

29 juin 2018

Sommaire

Eléments de contexte – P3

- Développement Concerté de l'Administration Numérique Territorial et la problématique SSI
- Agence nationale de sécurité des systèmes d'information, autorité d'Etat

Interlocuteurs ANSSI sur les territoires – P6

Collectivités : dispositions légales et documentation accessible – P7

Outils de formation – P8

Cybermalveillance.gouv.fr – P9

Eléments de contexte

- Développement Concerté de l'Administration Numérique Territorial et la problématique SSI

Action 8 du Programme DCANT 2018-2020

« Valoriser auprès des collectivités territoriales les actions SSI présentes dans l'offre de services de l'Etat »

Mounir MAHJOUBI, Secrétaire d'Etat chargé du numérique
30/10/2017

« On a d'abord protégé l'armée, l'Etat puis les groupes stratégiques. Mais la menace ne vise plus seulement des sites sensibles. On multiplie les actions **pour insuffler la culture de la cyber-sécurité** »

Eléments de contexte

- Agence nationale de la sécurité des systèmes d'information (ANSSI), autorité d'Etat 1/2

Identité de l'ANSSI

- L'ANSSI a été créée par le décret n°2009-834 du 7 juillet 2009 sous la forme d'un service à compétence nationale
- Elle s'est substituée à la direction centrale de la sécurité des systèmes d'information, est rattachée au Secrétariat général de la défense et de la sécurité nationale et en renforce les compétences, effectifs et moyens.

Rapports de l'ANSSI

- Le Livre blanc sur la défense et la sécurité nationale de 2008, qui invite l'Etat à se doter d'une capacité de prévention et de réaction aux attaques informatiques
- Le Livre blanc sur la défense et la sécurité nationale de 2013, qui incite à la prise en compte par l'Etat des besoins en cybersécurité des OIV et qui a donné lieu à la Loi du 19 décembre 2013 permettant à l'ANSSI d'imposer à ces organismes des mesures de sécurité et des contrôles SI dédiés
- La Stratégie nationale pour la sécurité du numérique du 16 octobre 2015, destinée à accompagner la transition numérique de la société française
- La Revue Stratégique de Cyberdéfense du 12 février 2018, véritable Livre blanc de la cyberdéfense, et premier grand exercice de synthèse stratégique dans le domaine.

Eléments de contexte

- Agence nationale de la sécurité des systèmes d'information (ANSSI), autorité d'Etat 2/2

Missions de l'ANSSI

- En collaboration avec les administrations compétentes, l'ANSSI instruit et prépare les décisions gouvernementales relatives à la sécurité du numérique et à celle des données sensibles. Elle participe également à la construction et à la maintenance des réseaux et des terminaux sécurisés pour les services de l'État.
- L'ANSSI accompagne les opérateurs d'importance vitale (OIV) dans la sécurisation de leurs systèmes d'information critiques, rendue obligatoire par la Loi de programmation militaire de 2013.
- L'ANSSI est chargée de la promotion des technologies, des produits et services de confiance, des systèmes et des savoir-faire nationaux auprès des experts comme du grand public. Elle contribue ainsi au développement de la confiance dans les usages du numérique.

Destinataires

- Les opérateurs d'importance vitale (OIV), les administrations centrales, les entreprises, les collectivités territoriales et les particuliers.

Impact sur les territoires

- Indirectement concernées par l'action de l'ANSSI, les collectivités territoriales sont touchées par les problématiques SSI :
  - 100% des petites municipalités interrogées par l'APVF ont fait l'objet d'une attaque informatique ces dix dernières années.
  - La Revue Stratégique en matière de cyber-défense comporte trois recommandations qui concernent directement les territoires :
    1. Encourager la mutualisation des ressources des collectivités territoriales
    2. Favorisation la communication en matière de sécurité numérique avec les collectivités territoriales
    3. Favoriser le développement d'une offre adaptée de produits et de services

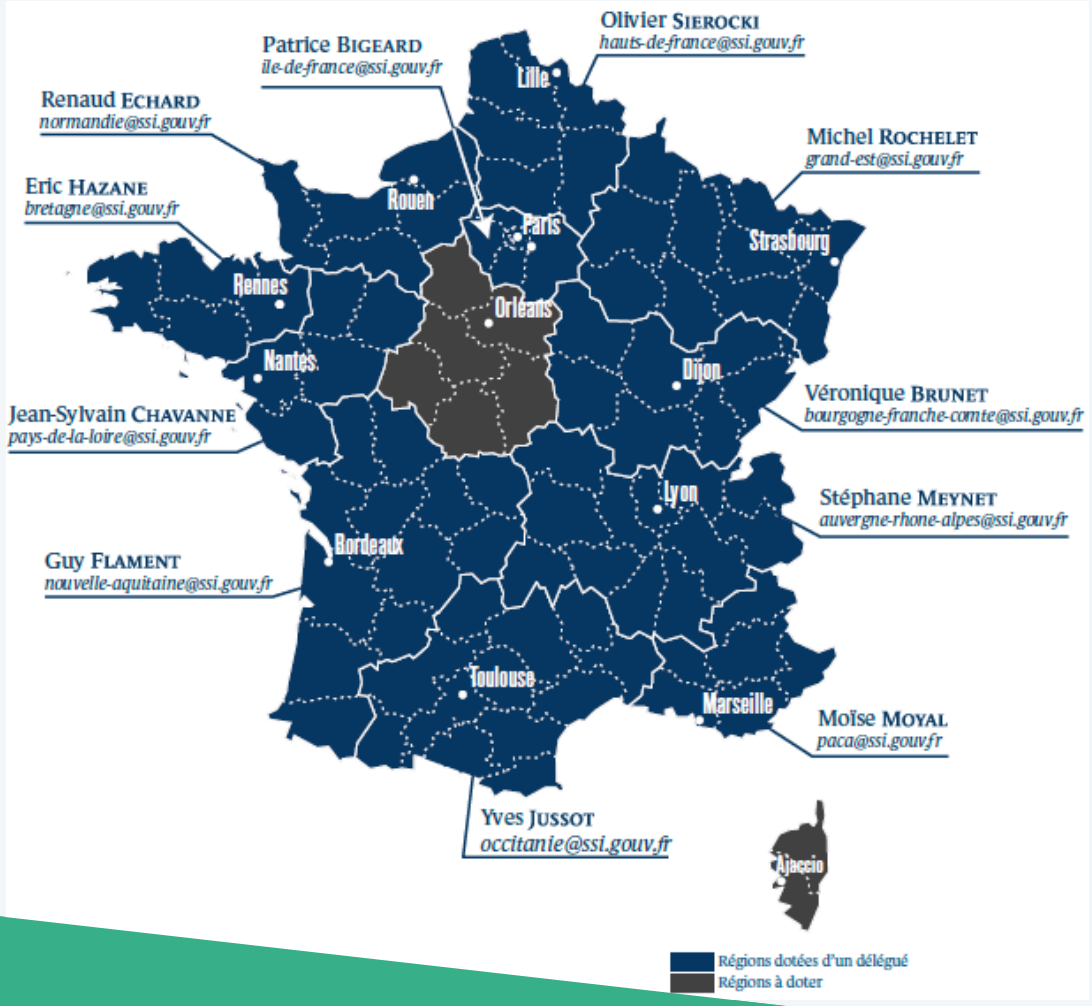
Interlocuteurs ANSSI sur les territoires

Les délégués en région sont chargés de relayer et de coordonner l'action de l'ANSSI dans les territoires ainsi que de contribuer au partage d'expérience et à l'association des acteurs locaux au dispositif national de cybersécurité.

Sensibilisation à destination des collectivités et des entreprises pour renforcer la prise en compte de la SSI

Animation des réseaux et coordination des acteurs locaux

Soutien de proximité aux OIV



Développement de la politique industrielle

Identification des centres de recherche susceptibles de coopérer avec l'ANSSI

Promotion du dispositif de protection du potentiel scientifique et technique de la Nation

Témoignage d'un délégué régional consultable en ligne

Collectivités : dispositions applicables et documentation accessible

Dispositions applicables aux collectivités en matière de SSI

- Pour les collectivités ayant le statut d'Opérateur d'Importance Vitale (OIV) : l'article 22 de la Loi de programmation militaire
- Pour les collectivités ayant le statut d'Opérateur de Service Essentiel (OSE) : la directive européenne NIS (Network Information Security)
- Le règlement européen sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (e-IDAS)
- Le référentiel général de sécurité (RGS)
- La politique de sécurité des systèmes d'information de l'Etat (PSSIE) .

Normes et guides de bonnes pratiques utilisables par les collectivités

- Recommandations mises à disposition par l'ANSSI – consultables en ligne
- Catalogue de solutions qualifiées : « Visas de sécurité ANSSI » permettant la certification entamée par un tiers ou la qualification établie par l'Agence elle-même des prestataires auxquels peuvent recourir les entreprises et toute administration publique : la liste de ces prestataires est accessible en ligne
- Guide d'hygiène informatique – renforcer la sécurité de son système d'information en 42 mesures, notamment :
  - Sensibiliser et former
  - Authentifier et contrôler les accès
  - Sécuriser l'administration
  - Gérer le nomadisme
- Guide de bonnes pratiques de l'informatique, notamment :
  - Choisir avec soin ses mots de passe
  - Mettre à jour régulièrement ses logiciels
  - Bien connaître ses utilisateurs et ses prestataires
  - Effectuer des sauvegardes régulières
  - Télécharger ses programmes sur les sites officiels des éditeurs

Outils de formation SSI

SecNumedu
ANSSI

SecNumacadémie.gouv.fr
Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Formez-vous à la sécurité du numérique

Catalogue des stages 2017-2018 du CFSSI

MOOC

- Des MOOC sur la SSI accessibles aux agents des collectivités désireux de suivre un programme en ligne de sensibilisation à la sécurité numérique. Ces MOOC s'adaptent au besoin de différents publics, non experts, en proposant des contenus pédagogiques ludiques et accessibles à tout moment gratuitement.

Label

- Un label à destination des formations initiales en cyber sécurité susceptibles d'être valorisé par les territoires – ex. Région Bretagne : consultable ici. L'objectif de cette labellisation est d'apporter l'assurance aux étudiants et aux employeurs qu'une formation dans le domaine de la sécurité du numérique répond à une charte et aux critères établis par l'ANSSI.

Stage

- Des stages SSI sont ouverts aux agents des collectivités. Le centre de formation de l'ANSSI en propose une vingtaine, ouverts à titre gratuit à l'ensemble des agents publics. Par ailleurs, le CNPFT dispose d'une offre cyber à destination des agents territoriaux.

Glossaire

- Un glossaire est disponible en ligne.

Guide

- Un guide à destination des collectivités est en cours de réalisation – ANSSI.

Cybermalveillance.gouv.fr

- Dispositif national d'assistance aux victimes d'actes de cyber-malveillance

GIP incubé par l'ANSSI et co-piloté avec le Ministère de l'Intérieur, le dispositif s'appuie sur les Ministères de l'Economie et des Finances et de la Justice

Ouverts aux particuliers, aux entreprises et **aux collectivités territoriales** – hors OIV

Missions

- Assistance aux victimes : accueil via la plateforme numérique permettant la mise en relation avec des prestataires de proximité puis une redirection vers les plateformes existantes ; des fiches réflexes sont également disponibles.
- Prévention et sensibilisation à la sécurité numérique : recommandations ; campagnes de sensibilisation ; aide à la formation
- Création d'un observatoire de la menace numérique : remontées, partage et transmission d'information entre les prestataires et les autorités publiques

Mise en œuvre d'un **kit de sensibilisation** :

- Outils pédagogiques à destination des collaborateurs
- Diffusion de bonnes pratiques
- Inscription en ligne

Programme DCANT 2018-2020 :

- Feuille de route – 2nd semestre 2018

« **Adapter** les dispositifs de sensibilisation à la cyber malveillance aux spécificités des collectivités territoriales avec Cybermalveillance.gouv.fr (GIP ACYMA) »

@Programme_DCANT

#DCANT