Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre

DOSSIER DE PRESSE

POLITIQUE DE LA FRANCE EN MATIÈRE DE CYBERSÉCURITÉ

20 février 2014

Contact presse

+33 (0)1 71 75 84 04
communication@ssi.gouv.fr
www.ssi.gouv.fr

Sommaire

L'ANSSI

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a été créée en juillet 2009. L'ANSSI assure la sécurité des systèmes d'information de l'État et contribue à celle des opérateurs nationaux d'importance vitale [1], en apportant son expertise et son assistance technique aussi bien en matière de prévention des menaces que dans le traitement des incidents. Elle conçoit et déploie les réseaux sécurisés répondant aux besoins des plus hautes autorités de l'État, elle délivre des labels aux produits et services de sécurité et diffuse les bonnes pratiques d'hygiène informatique.

L'ANSSI est dirigée par Patrick Pailloux, ingénieur général des mines. Elle est rattachée au Secrétaire général de la défense et de la sécurité nationale (SGDSN), autorité chargée d'assister le Premier ministre dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale.

L'ANSSI a trois missions majeures :

- **Prévenir** la menace en anticipant les modes d'attaques, en définissant les mesures de protection, en assistant les administrations et les entreprises critiques, en labellisant des produits et services informatiques de confiance ;
- **Défendre** les systèmes d'information en détectant les failles et incidents, en réagissant au plus tôt en cas de cyber-attaque, en apportant son assistance technique et son expertise ;
- **Informer et sensibiliser** les différents publics sur la nécessaire protection des environnements numériques, en promouvant les bonnes pratiques de cybersécurité et en émettant des recommandations techniques.

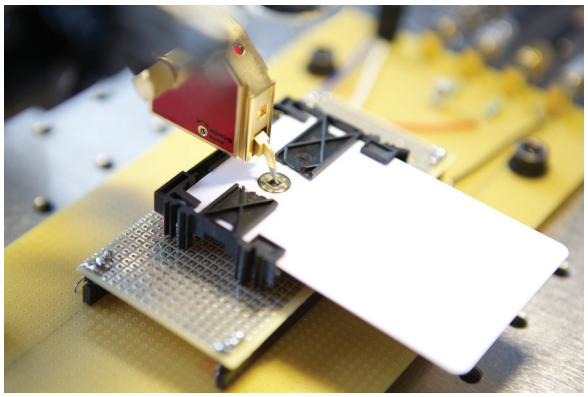
Prévenir

L'ANSSI :

- **élabore** les règles et les mesures à appliquer pour la protection des systèmes d'information de l'État ;
- **développe** et acquiert les produits essentiels à la protection des systèmes d'information de l'État ;
- **conçoit**, fait réaliser et met en œuvre des outils de communication sécurisés nécessaires à la Présidence de la République et au Gouvernement (réseau téléphonique Rimbaud et l'intranet ISIS par exemple) ;
- **assiste** les administrations et les opérateurs d'importance vitale (OIV) dans la sécurisation de leurs systèmes d'information ;
- **mène** des audits et des inspections des systèmes d'information sensibles ;

1 *Le code de la défense définit les opérateurs d'importance vitale comme « des opérateurs publics ou privés exploitant des établissements ou utilisant des installations et ouvrages, dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation ».*

- **délivre** des labels (certification, qualification, agrément) aux produits de sécurité et aux prestataires de services de confiance qui interviennent dans les domaines des technologies de l'information ;
- **contribue** à définir les positions de la France et à assurer la cohérence de l'action gouvernementale en matière de sécurité des systèmes d'information sur le plan international.



Défendre

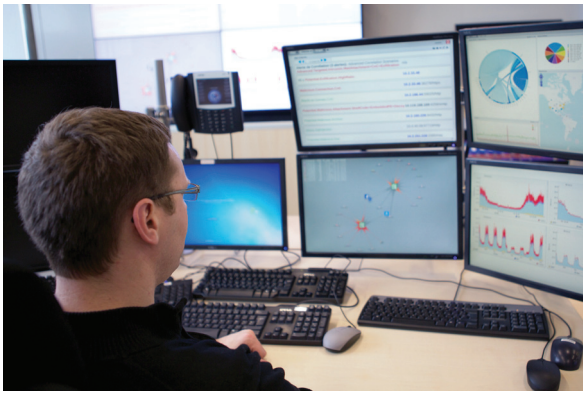
L'ANSSI :

- **décide** des mesures que l'État met en œuvre pour répondre aux crises affectant ou menaçant la sécurité des systèmes d'information des administrations et des opérateurs d'importance vitale et coordonne l'action gouvernementale en cas d'attaque informatique ;
- **met en œuvre** une capacité permanente de veille, d'alerte et d'analyse sur des informations relatives à la sécurité des systèmes d'information (évolution de la menace, vulnérabilités nouvelles de matériels et logiciels, etc.) ;
- **recueille** et analyse les informations techniques, notamment les codes malveillants, relatifs aux incidents affectant les systèmes d'information de l'État et ceux des opérateurs d'importance vitale ;
- **s'appuie** sur un réseau d'alerte permettant l'échange rapide d'informations techniques et opérationnelles utiles à la cybersécurité ;
- **recherche** et détecte, en cas d'attaque, les compromissions du système d'information de la victime, supervise les opérations de traitement d'incident ou de reconstruction du système.

Sensibiliser

L'ANSSI :

- **promeut** les bonnes pratiques de cybersécurité ;
- **assure** la formation des agents de l'État dans les divers aspects de la sécurité des systèmes d'information ;
- **informe** les différents publics sur les menaces et la nécessaire protection des environnements numériques ;
- **contribue** à la promotion des technologies et des savoir-faire nationaux en matière de sécurité des systèmes d'information en France et à l'étranger ;
- **accompagne** la filière cybersécurité dans l'enseignement supérieur et la recherche en liaison avec les ministères concernés ;
- **émet** des recommandations techniques.



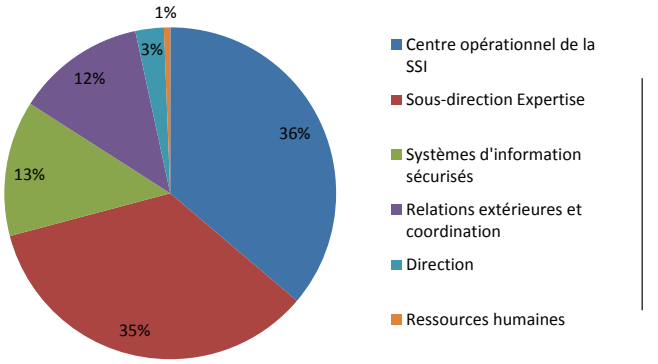
Guide d'hygiène informatique

Publié par l'ANSSI, il présente 40 recommandations pour sécuriser ses systèmes d'information. Il est disponible sur :
http://ssi.gouv.fr/

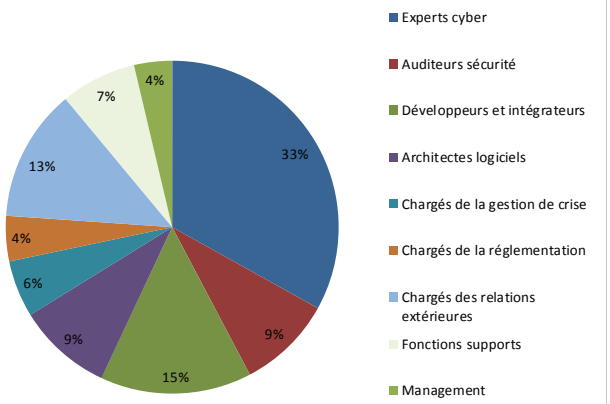
L'ANSSI en chiffres

Chiffres clés

- Personnel : **350** agents aujourd'hui (**500** à l'horizon **2015**) – 100 recrutements prévus en 2014.
- Près de **30** incidents français majeurs (mobilisant plus de deux agents sur plus de quinze jours) ont nécessité la participation des agents de l'ANSSI.



Répartition des agents par sous-directions



les métiers de l'ANSSI

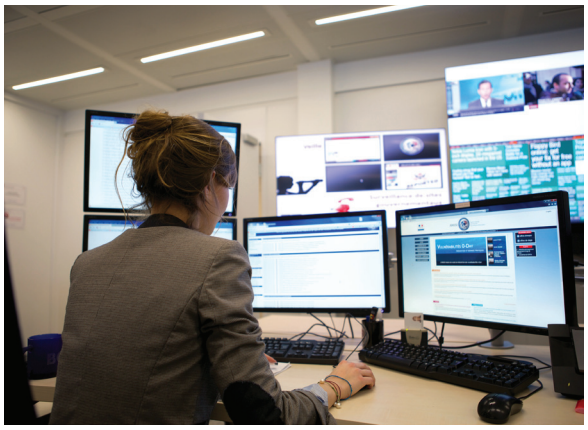
- Budget 2014 : **80** millions d'euros dont 30 millions d'euros consacrés à la masse salariale.
- L'ANSSI gère aujourd'hui les terminaux de haute sécurité au sein des organismes étatiques :
  - Isis (réseaux Intranet sécurisé) : **230** sites raccordés, **2300** abonnés pour **900** postes ;
  - Rimbaud : **2900** terminaux déployés sous la responsabilité de l'ANSSI.
- La sécurité de plus de **25** raccordements Internet de l'État est assurée en permanence par les sondes de détection d'attaques informatiques de l'ANSSI.
- Plus de **400** défigurations de pages Internet ont été traitées en 2013.
- **105** produits ont été labellisés en 2013 par l'ANSSI.
- Plus de **20** publications techniques ont été produites en 2013 par les experts de l'ANSSI (à retrouver sur le site www.ssi.gouv.fr/bonnespratiques/).
- Près de **1 500** agents de l'État sont formés annuellement par l'ANSSI sur les problématiques de sécurité des systèmes d'information.

Le centre de cyberdéfense de l'ANSSI

Le centre de cyberdéfense de l'ANSSI, installé dans la « Tour Mercure », veille à la sécurité des systèmes d'information critiques de la Nation 24 heures sur 24, 7 jours sur 7. Cinquante agents y sont affectés. Cet effectif peut être renforcé pour atteindre quatre-vingt personnes en cas de crise majeure.

Le centre de cyberdéfense remplit trois fonctions :

- **la veille (permanence H24, 7 jours sur 7) :** le bureau veille réceptionne et émet des signalements et des alertes relatifs à la sécurité des systèmes d'information émanant des ministères, des opérateurs d'importance vitale mais aussi des services de police ou de renseignement et des partenaires étrangers de l'ANSSI. Il contrôle la disponibilité et l'intégrité de plus d'un millier de sites Internet gouvernementaux et d'administrations. Il assure également une veille média ;
- **la supervision :** le centre supervise les remontées des sondes de détection déployées au sein des réseaux de l'administration. Il a pour objectif de détecter en temps réel les attaques ou les tentatives d'attaques informatiques contre les systèmes gouvernementaux et de prévenir les opérations d'espionnage. Les informations de sécurité recueillies sont ensuite expertisées par les analystes en liaison avec les organismes ciblés. Puis, lorsqu'un phénomène suspect est mis en évidence, les informations sont transmises aux équipes techniques chargées d'évaluer et de traiter les incidents ;



- **la conduite des opérations de cyberdéfense :** le centre pilote les interventions de l'ANSSI en cas d'attaques avérées ou de suspicion de compromissions. Il assure l'analyse et la synthèse des informations collectées.

Pour réaliser ces missions, le centre de cyberdéfense dispose de moyens de communication protégés et résilients qui lui permettent d'échanger avec les partenaires de l'ANSSI, en France comme à l'étranger.

La co-localisation du centre de cyberdéfense de l'ANSSI avec le centre d'analyse de lutte informatique défensive (CALID) du ministère de la défense permet d'assurer une coordination étroite entre les deux centres et de concentrer sur un même site l'essentiel des capacités nationales de cyberdéfense.

Des capacités nouvelles pour le Premier ministre

au service de la protection des systèmes d'information des « opérateurs d'importance vitale »

La loi de programmation militaire donne des capacités nouvelles au Premier ministre qui désormais :

- **fixe** les règles de sécurité nécessaires à la protection des systèmes d'information critiques des OIV ;
- **reçoit** les notifications des incidents informatiques touchant ces systèmes critiques ;
- **soumet** les systèmes d'information des OIV à des contrôles de leur niveau de sécurité ;
- **décide** des mesures que les OIV doivent mettre en œuvre en cas de crise informatique majeure.

Certaines des attaques informatiques menées à travers le monde contre des entreprises ou des administrations visent à entraver le fonctionnement normal de l'opérateur visé. Ainsi, en août 2012, le pétrolier saoudien Aramco a vu 30 000 ordinateurs de son siège mis hors d'usage par une attaque informatique, perturbant l'ensemble de l'activité de l'entreprise pendant plusieurs semaines.

Contre le danger présenté par ce type d'attaque, le Livre blanc sur la défense et la sécurité nationale a annoncé en 2013 que *« s'agissant des activités d'importance vitale pour le fonctionnement normal de la Nation, l'État fixera, par un dispositif législatif et réglementaire approprié, les standards de sécurité à respecter à l'égard de la menace informatique et veillera à ce que les opérateurs prennent les mesures nécessaires pour détecter et traiter tout incident informatique touchant leurs systèmes sensibles ».*

Le code de la défense définit les opérateurs d'importance vitale (OIV) comme *« des opérateurs publics ou privés exploitant des établissements ou utilisant des installations et ouvrages, dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation »*. Ils sont répartis en douze secteurs d'activités d'importance vitale*.

*** Secteurs d'activités d'importance vitale :**

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.*

Secteurs de la vie économique et sociale de la nation : *énergie ; communication, électronique, audiovisuel et information ; transports ; finances ; industrie.*

La loi de programmation militaire présentée par le gouvernement début août 2013 et votée par le Parlement en décembre, apporte des capacités nouvelles au Premier ministre qui lui permettent notamment de fixer les règles de sécurité nécessaires à la protection des systèmes d'information critiques des opérateurs d'importance vitale (OIV), de recevoir des notifications d'incidents informatiques touchant ces systèmes, et de mener des audits pour évaluer le niveau de sécurité et l'application des règles fixées.

En cas de crise grave, le Premier ministre est désormais en mesure de donner des instructions aux opérateurs concernés pour garantir la défense la Nation contre des attaques en cours.

L'article 21 de la même loi précise que pour la définition de la politique et la coordination de l'action gouvernementale, le Premier ministre dispose de l'autorité nationale de sécurité des systèmes d'information (l'ANSSI).

Un groupe de travail créé en 2013 par l'ANSSI qui rassemblait des équipementiers, des intégrateurs et des opérateurs d'importance vitale a permis d'élaborer et de publier un mois après la promulgation de la loi un guide présentant une méthodologie de classification des systèmes d'information liés à des processus industriels et les règles techniques à appliquer pour les sécuriser.

Avec les ministères concernés, les OIV et l'ensemble des acteurs concernés, l'ANSSI engage un travail collaboratif par secteur d'activité d'importance vitale afin, sur la base du guide élaboré, de caractériser les systèmes critiques des opérateurs et de définir des règles techniques adaptées à leur activité.

A l'issue de ce travail de concertation qui abordera également les questions liées à la notification d'incident, la politique de contrôle et d'audit et les mesures susceptibles d'être prises en cas de crise majeure, les textes réglementaires correspondants seront élaborés et publiés.

Le développement des industries et services de cybersécurité en France et en Europe

Le Livre blanc sur la défense et la sécurité nationale de 2013 soulignait la nécessité pour la France de préserver son autonomie en matière de cybersécurité, notamment en soutenant les compétences scientifiques, technologiques et industrielles françaises en la matière.

« La capacité de produire en toute autonomie nos dispositifs de sécurité, notamment en matière de cryptologie et de détection d'attaque, est à cet égard une composante essentielle de la souveraineté nationale. Un effort budgétaire annuel en faveur de l'investissement permettra la conception et le développement de produits de sécurité maîtrisés. Une attention particulière sera portée à la sécurité des réseaux de communication électroniques et aux équipements qui les composent. Le maintien d'une industrie nationale et européenne performante en la matière est un objectif essentiel.[1] »

La France assure sa souveraineté technologique en matière de cybersécurité mais également en matière de technologies de l'information et de communication afin de répondre aux besoins de sécurité et de confiance de l'État, des opérateurs d'importance vitale (OIV) et des citoyens.

Pour cela, la France doit, en priorité, promouvoir et défendre l'offre industrielle et de services française dans les domaines du numérique et de la cybersécurité.

La France peut s'appuyer sur plusieurs filières d'excellence :

- des industriels du monde de la défense et de la sécurité capables de produire en totale autonomie des produits de très haute sécurité ;
- une industrie du composant unique en Europe ;
- un tissu industriel complet et référent dans le domaine de la carte à puce ;
- une école de cryptologie de renom ;
- une filière de formation dans le domaine du numérique, notamment en matière de logiciel, reconnue mondialement ;
- un tissu actif de PME innovantes

1 *Livre blanc défense et sécurité nationale 2013, page 105.*

Parallèlement, pour la satisfaction de besoins nécessitant des investissements que la France ne pourrait réaliser seule, un effort conjugué au niveau européen doit être réalisé pour aller vers une autonomie numérique européenne.

Le gouvernement a engagé quatre grandes actions :

- Le Premier ministre a installé **le Comité de la filière industrielle de sécurité (CoFIS)** en octobre 2013 afin de faire émerger les besoins en matière de sécurité au moyen d'un dialogue rénové entre les pouvoirs publics, les opérateurs publics et privés, les centres de recherche et l'industrie, et définir sur cette base une méthodologie pérenne du recueil du besoin ainsi qu'une première liste de priorités. Piloté par le secrétariat général de la défense et de la sécurité nationale, le comité de filière comprend un volet cybersécurité ;

- dans le cadre de **la Nouvelle France Industrielle** présentée par le Président de la République en septembre 2013, le « Plan Cybersécurité » réunit les différents acteurs de la filière (ministères, industriels, groupements d'utilisateurs) afin de déterminer les actions à mener pour accompagner le développement des offres de produits et de services nationales. Les travaux comportent la rédaction d'une feuille de route des produits et services de sécurité, des actions de conquête des marchés à l'export et des travaux de valorisation de l'offre auprès des acheteurs. Ce plan est piloté par Patrick Pailloux [1] ;

- **le Fonds souverain pour le numérique :** piloté par la direction générale de la compétitivité, de l'industrie et des services (DGCIS) du ministère du redressement productif et avec le soutien de l'ANSSI, ce fonds, au travers de l'appel à projet « cœur de filière », permet de soutenir le développement d'offres françaises dans des domaines prioritaires : solutions de mobilité sécurisées, outils de détection d'attaques, outils de supervision de la sécurité et outils de protection des systèmes industriels. 18 projets ont été soumis par l'industrie française, et les projets retenus devraient bénéficier d'une enveloppe globale d'environ 20 millions d'euros d'aide de l'État ;

- **la valorisation des produits et services par la labellisation :** les labels attribués par l'ANSSI permettent aux administrations et entreprises de sélectionner des produits de confiance pour la sécurisation de leurs systèmes d'information. L'ANSSI développe par ailleurs des référentiels qui permettront de labelliser des offres de services relevant de la souveraineté : offres d'informatique en nuage *(cloud computing)*, services de détection d'attaques, prestations de supervision de la sécurité, prestations de traitements d'incidents.

L'ensemble de ces actions permettra la valorisation de l'offre française, la consolidation des acteurs majeurs du secteur, le soutien au développement des PME innovantes et l'émergence d'une offre technologique adaptée au marché et bénéficiant d'un haut standard de sécurité.

---

1 Voir www.redressement-productif.gouv.fr/nouvelle-france-industrielle

Décisions du Premier ministre pour renforcer la sécurité des systèmes d'information soutenant la vie de la Nation

Face au développement des attaques informatiques de toutes formes et sur proposition du SGDSN et des ministères concernés, le Premier ministre a pris plusieurs mesures de renforcement de la sécurité des systèmes d'information. Elles portent sur la sécurité des systèmes d'information de l'État, la sécurité des échanges électroniques effectués sur le territoire national, le soutien à l'industrie française de la cybersécurité, la sensibilisation et la formation.

- **la sécurité des systèmes d'information de l'État**
  - le chiffrement des réseaux de l'État sera systématisé ;
  - lors de leurs achats de produits et service de sécurité informatique, les administrations de l'État devront choisir des produits et services labellisés par l'ANSSI.

- **la sécurité des échanges électroniques effectués sur le territoire national**
  - le gouvernement engage avec les fournisseurs d'offres nationales de messagerie électronique une initiative visant à sécuriser les messageries et traiter les messages par des infrastructures situées en France.

- **le soutien à l'industrie française de la cybersécurité**
  - un nouvel appel à projets du fonds souverain pour le numérique (FSN) sera lancé en 2014 ;
  - la France appellera à développer l'autonomie stratégique de l'Union européenne dans le domaine des industries et services européens des technologies de l'information et de la cybersécurité. La France appellera également au soutien de certains secteurs stratégiques comme celui des équipementiers des opérateurs de communications électroniques ou celui des infrastructures et services informatiques en nuage.

- **la sensibilisation et la formation**
  - le ministère de l'Enseignement supérieur et de la Recherche développera la formation de spécialistes en cybersécurité et veillera à ce que toute formation informatique supérieure comporte un socle minimal de connaissance en matière de sécurité des systèmes d'information. Ce socle sera défini en collaboration avec des industriels du secteur et l'ANSSI.