RECOMMANDATIONS DE LA REVUE STRATEGIQUE DE CYBERDEFENSE 12 FEVRIER 2018

Le Premier ministre a chargé le Secrétaire général de la défense et de la sécurité nationale de conduire une revue stratégique nationale et globale de cyberdéfense. Après une communication en Conseil des Ministres le 7 février 2018, cette revue vient d'être remise officiellement au Gouvernement et rendue publique sous forme d'un livre blanc.

Vous trouverez ci-après les préconisations de la revue qui a été pilotée par Mme Agathe Cagé, Inspectrice Générale de l'Administration au Ministère de l'Intérieur.

Consolidation de l'organisation de cyberdéfense française

- Mettre en place 4 chaînes opérationnelles : chaîne « protection », chaîne « action militaire », chaîne « renseignement », chaîne « investigation judiciaire ».
- Mettre en place un comité directeur cyber chargé de suivre la mise en œuvre des décisions prises en matière de développement et d'organisation générale du domaine par le Conseil de Défense et de Sécurité Nationale (CDSN).
- Mettre en place un comité de pilotage de la cyberdéfense qui s'attache à améliorer la connaissance de la menace d'origine cyber, à élaborer une politique industrielle, réglementaire et normative de souveraineté numérique et à mettre en place une doctrine officielle de réponse globale à une crise cyber.
- Mettre en place un centre de coordination des crises cyber (C4) chargé de la gestion des crises non majeures.
- Adopter un schéma de prise de décision en cas d'attaque cyber.

Renforcement de la sécurisation des systèmes d'information de l'Etat

- Soumission pour avis à l'ANSSI des projets informatiques les plus importants et les plus sensibles de l'Etat dès leur phase de lancement.
- Raccordement progressif de tous les ministères à la plateforme d'accès à Internet du réseau interministériel de l'Etat (RIE) et pleine utilisation des services qu'elle offre.
- Imposer la couverture complète par un dispositif de supervision de la sécurité des services informatiques utilisés par l'Etat, y compris dans les cas où ces services sont externalisés, et permettre à l'ANSSI d'imposer à cette fin la mise en place de ses systèmes de détection ou de systèmes de détection équivalents.

Renforcement de la protection des opérateurs d'importance vitale (OIV)

- Renforcement du niveau d'exigence des règles de sécurité qui s'appliquent aux OIV des secteurs des communications électroniques et de l'approvisionnement en énergie électrique.

Renforcement de la protection des activités essentielles

- Un socle commun de règles élémentaires de sécurité proportionnée permettant de protéger les acteurs fournissant des services essentiels.
- Recherche d'une harmonisation au sein de l'Union européenne des règles de cybersécurité s'appliquant aux opérateurs de services essentiels

Implication accrue des opérateurs de communications électroniques et des hébergeurs

- Permettre à l'ANSSI de s'appuyer sur des systèmes de détection mis en œuvre par les opérateurs de communications électroniques pour détecter les attaques informatiques
- Permettre à l'ANSSI, lorsqu'elle a connaissance d'une menace particulièrement sérieuse, de mettre en place sur le réseau d'un opérateur de communications électroniques ou le système d'information d'un hébergeur, un dispositif de détection local et temporaire

Amélioration de la cyberprotection des collectivités territoriales

- Soutien à la création, par les collectivités territoriales elles-mêmes, d'un réseau de correspondants en cybersécurité
- Amélioration de l'intégration des besoins et des contraintes spécifiques aux collectivités territoriales dans les référentiels de l'ANSSI et dans ses catalogues de produits et services qualifiés

Renforcement de la lutte contre la cybercriminalité

- Conduite d'une réflexion sur la pertinence d'enquêter de manière plus systématique sur les actes de cybercriminalité, y compris en l'absence de plainte, lorsque les informations recueillies laissent entrevoir l'existence probable d'infractions pénales.
- Action d'entrave contre les plateformes criminelles les plus populaires afin de diminuer le sentiment d'impunité qui anime un certain nombre de cybercriminels.
- Développement d'un réseau de collaboration actif entre magistrats et enquêteurs en Europe et à l'international.

Promotion de normes de comportement responsable dans le cyberespace

- Renforcement des mécanismes de contrôle des exportations dans le domaine cyber pour les éléments les plus dangereux.
- Création, au niveau français ou européen, d'un think tank de portée internationale dédié aux questions géostratégiques et juridiques de cyberdéfense au sein duquel les idées de la France pourraient trouver un relais.

Encadrement de l'activité des acteurs privés dans le cyberespace

- Lancement d'une initiative française dans le cadre du G20 en vue de réguler les activités du secteur privé ayant un impact sur la sécurité internationale du cyberespace.
- Promouvoir l'interdiction du Hackback par des acteurs du secteur privé dans le cyberespace.
- Poser au niveau international un principe de responsabilité de sécurité des acteurs privés systémiques dans la conception et la maintenance de leurs produits et services numériques.

Définition d'une doctrine d'action face à une attaque cyber

- Adoption d'un schéma de classement des attaques informatiques.
- Définition des options de réponse aux incidents cyber

Structuration d'une politique industrielle en matière numérique reposant sur la maîtrise de technologies clés

- Mise en place d'une équipe interministérielle chargée d'analyser les technologies clés et de faire émerger des solutions de confiance en lien avec les industriels (veille technologique et proposition de choix dédiés à l'émergence des technologies clés

- Maintien d'une industrie nationale à la pointe dans le domaine du chiffrement des communications.
- Développement d'une nouvelle génération de radios professionnelles mobiles au profit des forces de sécurité et des unités de secours.
- Soutien à la recherche et développement dans le domaine de l'intelligence artificielle appliquée à la cyberdéfense.

Communications sécurisées

- Identifier un composant critique maitrisé par la France et intégré dans des équipements terminaux pour pouvoir faire de la téléphonie mobile sécurisée.
- Développer des techniques de chiffrement et de cloisonnement logiciels
- Etudier de nouveaux services, apparentés à la radio professionnelle, basés sur les technologies civiles (5G) pour apporter de la résilience.

Cloud

- Etablir une politique globale de l'Etat de recours au cloud.
- Encourager le développement de solutions de chiffrement pour le cloud.
- Soutenir une autonomie stratégique dans ce domaine.
- Etablir un cadre de confiance global afin d'orienter le marché vers des produits qualifiés SecNimCloud.

Amélioration du cadre actuel de certification afin de contribuer à l'amélioration de la sécurité des produits

- Mise en place d'une certification élémentaire de cybersécurité, sur le modèle du marquage « CE » requis pour la commercialisation de certains biens ou services au sein de l'espace européen.

Consolidation de notre base industrielle nationale de confiance dans le domaine de la cyberdéfense

- Réaliser et entretenir une cartographie industrielle
- Soutien à l'émergence d'au moins un acteur industriel national de référence dans le domaine de la Threat intelligence (analyse de la menace) et de l'élaboration de marqueurs apte à concurrencer les grandes entreprises américaines, russes et israéliennes du domaine.

Soutenir les acteurs privés

- Inciter les grands industriels français à compléter leur offre de produits et de service à destination du domaine civil, afin qu'ils y deviennent des champions internationaux de la cybersécurité capables de concurrencer les géants de la cybersécurité américains, russes, chinois ou israéliens.
- Soutien aux stratégies de croissance externe des PME dédiées à la cyberdéfense les plus performantes par la mobilisation des fonds d'investissement intéressés par le domaine de la cyberdéfense pour favoriser la création d'entreprises de taille intermédiaire (ETI) françaises dans ce secteur.

- Soutien à la mise en place d'accélérateurs, de start-ups studios et plus généralement de structures d'accompagnement des start-ups dédiés à la cyberdéfense, en concentrant les efforts sur les entreprises innovantes dont la stratégie peut leur permettre d'atteindre une empreinte mondiale.

Appui à la prise en compte par le secteur privé des enjeux cyber

- Soutien à l'apparition d'acteurs nationaux ou européens de notation cyber.
- Etudier le soutien au développement d'un mécanisme d'assurance cyber pertinent en aidant à mieux estimer les risques.
- Soutien à la mise en place d'une valorisation du risque CYBER au sein des normes comptables et à la prise en compte dans les documents comptables et financiers

Intégration des règles de la cybersécurité dans les apprentissages transmis par l'Ecole de l'école élémentaire à la classe de terminal

- Une éducation au numérique incluant la maîtrise des exigences en matière de cybersécurité à l'école élémentaire, au collège et dans tous les cursus du lycée.
- Des MOOCS sur la transmission des règles de cybersécurité dédiés aux enseignants en formation initiale et en formation continue conçus par le ministère de l'Education nationale avec le fort soutien de l'ANSSI.

Diffusion de la culture de la sécurité numérique dans toute la société

- Création par l'ANSSI d'une application ludique, disponible sur smartphone, permettant aux Français de tester leur niveau de connaissances dans le domaine de la culture de la sécurité numérique et leur proposant de nombreux défis.
- Etude de l'apport des nudges pour le développement de l'autonomie des citoyens en matière de cybersécurité.
- Intégration d'une dimension cybersécurité au programme de soutien à la transformation numérique des entreprises du ministère de l'économie et des finances et du secrétariat d'état au numérique.
- Perfectionnement de la gestion des compétences dans les services chargés de la cyberdéfense de l'Etat.