Renforcement de la cybersécurité
Synthèse des principales mesures

1. Renforcer les capacités opérationnelles d'intervention de l'État

Création d'un « groupe d'intervention rapide »

Objectif

Être en mesure d'intervenir sur les systèmes d'information de l'État et des opérateurs critiques pour réaliser trois grandes missions :

- **rechercher et détecter** les compromissions ;
- **superviser** les opérations de traitement d'incident ou de reconstruction des systèmes ;
- **porter assistance à nos alliés** en cas de crise informatique.

Ce groupe d'intervention interviendra dans les administrations et les organismes publics ou chez les opérateurs critiques, notamment les opérateurs d'importance vitale, lorsque des indices laissent à penser qu'ils ont été l'objet d'une attaque informatique susceptible de présenter un danger pour la sécurité de leur activité, de menacer l'intégrité de leur patrimoine informationnel, de déséquilibrer le fonctionnement économique du pays ou de porter atteinte à la vie quotidienne des Français.

Dans le cas où une compromission grave serait découverte, le groupe d'intervention rapide sera en mesure, à la demande et en appui des équipes de l'administration, de l'entreprise et d'éventuels prestataires, d'élaborer les plans de reconstruction des systèmes d'information compromis et de superviser leur mise en œuvre, voire d'y contribuer directement.

Par ailleurs, doté de moyens aptes à être projetés, le groupe d'intervention rapide donnera à la France une capacité d'assistance à ses alliés en cas de crise majeure de nature informatique. Il permettra ainsi de connaître au plus tôt les caractéristiques des attaques dont nos partenaires sont l'objet et de prendre sans délai, en France, les mesures de protection nécessaires.

2. Augmenter le niveau de sécurité des systèmes d'information de l'État

Mise en place d'une politique interministérielle de sécurité

Objectif

Élever et homogénéiser le niveau de sécurité de l'ensemble des systèmes d'information de l'État.

Une grande partie des problèmes de sécurité seront évités ou détectés de manière précoce grâce à la mise en œuvre de règles de sécurité minimales communes aux systèmes d'information de l'État.

L'hétérogénéité des pratiques et des règles de sécurité actuelles nuit gravement à leur compréhension et à leur application. La mise en application d'une politique de sécurité commune et la clarification qui en résultera seront de nature à favoriser le respect de ces règles par l'ensemble des agents de l'État.

Déploiement de la « carte agent »

Objectif

Améliorer très significativement la sécurité des systèmes d'information de l'administration par la mise en place généralisée de cartes à puce.

La carte à puce est un système d'authentification forte, alors que les simples mots de passe ne résistent guère à des attaquants déterminés, même de faible niveau technique.

Le déploiement d'un système d'authentification forte permettant l'accès aux systèmes d'information de l'administration limitera fortement le risque d'accès illégitimes ou frauduleux aux systèmes d'information par des attaques informatiques internes ou externes.

Cette authentification forte s'appuiera sur un système à carte à puce, domaine d'excellence française, tant en matière industrielle que dans le domaine de la recherche.

Le projet est piloté par l'agence nationale des titres sécurisés en liaison avec l'ANSSI.

Renforcement de la cybersécurité
Synthèse des principales mesures

Recours par les administrations à des produits et services labellisés

Objectif

Augmenter le niveau de sécurité des systèmes d'information des administrations par l'utilisation de produits et de services ayant fait l'objet d'une évaluation positive et d'une labellisation par l'État.

Comme le prévoit le référentiel général de sécurité (RGS – décret n° 2010-112 du 2 février 2010 et arrêté du 18 mai 2010), les administrations auront recours, pour l'ensemble de leurs systèmes d'information, à des produits et à des services ayant fait l'objet d'une qualification.

L'ANSSI, autorité nationale de sécurité des systèmes d'information, dispose des compétences nécessaires pour organiser et prononcer cette labellisation des produits et des services concourant à la sécurité des systèmes d'information, attestant ainsi de la confiance qui peut leur être accordée. Cette démarche s'appuie notamment sur des centres d'évaluation de la sécurité des technologies de l'information (CESTI), eux-mêmes agréés par l'ANSSI.

Déploiement d'un intranet interministériel résilient

Objectif

- Permettre la continuité de l'action gouvernementale et administrative en cas de dysfonctionnement grave d'internet ;
- limiter le nombre de passerelles d'interconnexion entre les administrations et l'internet, points de fragilité potentiels, et améliorer ainsi la détection des attaques au niveau des passerelles et notre capacité à y réagir ;
- réduire les coûts de communications électroniques de l'État en réduisant le nombre de réseaux.
- conserver la maîtrise technologique des systèmes d'information de l'État en développant un réseau « à l'état de l'art ».

La construction d'un réseau interministériel protégé et résilient, développé « à l'état de l'art », présente également l'opportunité de repenser l'architecture des réseaux ministériels actuels et de favoriser l'adoption d'une politique de sécurité interministérielle unique. Ce sera aussi l'occasion de réduire le nombre de réseaux, et donc de rationaliser les ressources qui y sont dédiées.

Plusieurs de nos partenaires internationaux ont d'ores et déjà fait le choix d'un tel réseau pour des raisons de sécurité.

3. Promouvoir la cybersécurité dans l'enseignement supérieur et la recherche

Création d'une fondation et d'un centre de recherche en cybersécurité

Objectif

Soutenir la recherche en sécurité des systèmes d'information en partenariat avec l'industrie par :

- la contribution au financement de projets, de thèses et de post-doctorants ;
- l'analyse stratégique des besoins ;
- l'orientation de la recherche en amont ;
- le soutien au transfert de l'innovation.

En France, ces dernières années, plusieurs initiatives de recherche ont vu le jour en matière de sécurité des systèmes d'information. Elles restent toutefois ponctuelles et ne peuvent être pérennisées, faute de crédits ou de pilotage stratégique global.

Une fondation sera créée, sous la forme d'un partenariat public-privé, pour soutenir les capacités de recherche nationales et développer un centre spécifiquement dédié à la recherche en sécurité des systèmes d'information, dans les domaines techniques et non techniques (politique, géostratégique, économique, etc.).

Insertion de la sécurité des systèmes d'information dans les formations supérieures, notamment informatiques

Objectif

Sensibiliser et former tous les étudiants aux questions de sécurité des systèmes d'information.

Trop d'ingénieurs ou d'universitaires, y compris dans les filières techniques, arrivent aujourd'hui sur le marché du travail sans avoir jamais été formés à « l'hygiène numérique ».

Dans le domaine de l'informatique comme dans celui de la santé, les risques d'infection peuvent être fortement limités par l'application de principes techniques par les professionnels et de bonnes pratiques par les usagers. Ces principes et pratiques sont actuellement trop souvent ignorés. A l'image du monde de la santé, où l'hygiène fait partie de la formation de base de tout professionnel et de l'éducation des citoyens, il est essentiel que les règles élémentaires de sécurité informatique soient systématiquement enseignées dans les formations d'ingénieur et, sous forme de sensibilisation, dans l'ensemble de nos formations supérieures.

4. Améliorer la sécurité des d'infrastructures vitales

Établissement d'un partenariat avec les opérateurs d'infrastructures vitales

Objectif

L'établissement d'un partenariat entre l'État et les opérateurs critiques doit notamment :

- permettre aux opérateurs critiques de mieux connaître les faiblesses de leurs systèmes d'information et leur apporter l'éventuel appui technique nécessaire ;
- prévenir les attaques sur les systèmes critiques ;
- améliorer la compétence et la sensibilisation des opérateurs à la sécurité des systèmes d'information ;
- définir des chaînes de compétence et de responsabilité en matière de sécurité des systèmes d'information.

Il s'agit de développer les échanges d'informations entre l'État et les opérateurs critiques, le partage et l'analyse des remontées d'incidents ainsi que les audits de sécurité. Ces évolutions permettront de renforcer la sécurité des systèmes d'information industriels les plus critiques et de veiller à leur défense permanente.

Création d'un réseau d'alerte en cas d'attaque informatique

Objectif

Mettre en place un réseau permanent d'échange d'informations techniques et opérationnelles utiles à la cybersécurité des opérateurs d'importance vitale.

Lorsque l'État a connaissance d'une attaque informatique visant des opérateurs d'infrastructures vitales ou des établissements sensibles il doit être en mesure de contacter ceux-ci en temps réel.

Il en est de même dans l'éventualité d'une découverte de faille de sécurité grave touchant par exemple un système industriel spécifique.

L'ANSSI doit donc disposer d'un réseau d'alerte maintenu à jour et régulièrement validé par des exercices *ad hoc*.