Loi de Programmation Militaire 2024-2030

Un renforcement du pouvoir de contrôle de l'ANSSI pour mieux faire face aux attaques cyber

Qu'est-ce qu'une loi de programmation militaire ?

La loi de programmation militaire (LPM) vise à établir une programmation pluriannuelle des dépenses et ressources que l'État doit consacrer à ses forces de défense sur une durée de 4 ans à 6 ans.

Une enveloppe de 413,3 Milliards d'euros sera consacrée pour la LPM 2024-2030

La loi de programmation militaire et la cybersécurité

Au vu du contexte géopolitique actuel et l'intensification des menaces informatique, la LPM 2024-2030 a renforcé le volet (chapitre V) dédié au sujet de la cyberdéfense avec un investissement de **4 milliards d'euros** et un partenariat avec Polytechnique pour monter un centre d'excellence.

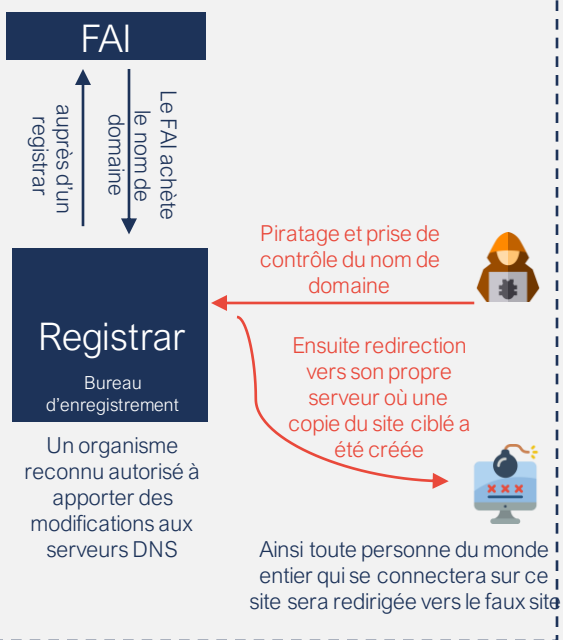
Le chapitre V de la LPM 2024-2030 est composé de 4 articles (de 32 à 35) détaillant les 4 mesures de cyberdéfense mentionnées dans la page suivante.

Le chapitre V de cette loi représente une intensification des pouvoirs de contrôle de l'ANSSI sur **les acteurs de DNS susceptibles d'être concernés par des agissements malveillants** (à savoir les fournisseurs d'accès à Internet FAI, les hébergeurs de données, les bureaux d'enregistrement des noms de domaine en France connus sous le nom de registrars etc.), mais aussi sur les **OCE** (opérateurs de communication électronique), sur **les éditeurs de logiciels,** les **OIV** (opérateurs d'importance vitale) et les **OSE** (opérateurs de services essentiels).

Acteurs concernés

- Éditeurs de logiciels (qui vendent leurs produits en France, fournis à des entreprises dont le siège social est en France ou à des sociétés contrôlées par par des sociétés ayant leur siège social en France)
- Hébergeurs des données
  Fournisseurs d'accès Internet (FAI)
  Registrars
- Opérateurs de communication électronique (OCE)
- Opérateurs d'importance vitale (OIV) et opérateurs de service essentiels (OSE)

Exemple d'attaque sur le DNS



Qu'est-ce qu'un DNS ?

Le **système de noms de domaine (DNS)** est un service utilisé pour assurer la correspondance entre le nom de domaine comme : www.finegan.fr et une adresse IP (composée de chiffres et lettre et donc complexe à retenir).

En effet, **le DNS est très souvent utilisé par les cyber attaquants pour gérer leur infrastructure d'attaque**. La grande majorité des attaques informatiques observées par l'ANSSI ont impliqué l'usage de DNS. Par exemple, le cyber attaquant peut dévier le flux d'un domaine vers un site malveillant qu'il peut contrôler (vers une copie exacte du site d'origine par exemple) afin de voler des données sensibles de l'utilisateur, perturber l'activité du site ou empêcher son utilisation.

Loi de Programmation Militaire 2024-2030

Un renforcement du pouvoir de contrôle de l'ANSSI pour mieux faire face aux attaques cyber

Quels impacts sur les acteurs concernés ?

1 **Filtrage de noms de domaine (DNS)** par les hébergeurs, les fournisseurs d'accès à Internet (FAI) ou registrars en cas de menaces susceptibles de porter atteinte à la sécurité nationale

L'ANSSI a le pouvoir de demander aux acteurs concernés (FAI, registrars ou hébergeurs des données) **le filtrage des noms de domaine** utilisés par les cyberattaquants. Il y a 2 types de filtrages, basés sur la « bonne foi » du titulaire de DNS (soit le titulaire est à l'origine d'une utilisation de DNS malveillante grave pour la sécurité nationale, soit il ne l'est pas).

Ces acteurs seront obligés **d'implémenter les mesures nécessaires pour neutraliser les effets de l'attaque dans des délais prédéfinis par l'ANSSI** sinon elle peut les obliger à bloquer le nom de domaine ou le suspendre. L'ANSSI peut aussi agir **sans délai** pour prendre les mesures nécessaires si le titulaire du DNS est à l'origine du flux malveillant. Il convient de préciser qu'il n'existe à ce jour des sanctions prévues en cas d'inaction de la part de ces acteurs.

2 Obligations des OCE et des fournisseurs de noms de domaine, de **communiquer à l'ANSSI certaines données DNS**, qui seront anonymisées afin de respecter les normes RGPD

Les premiers à être concernés par cet article sont les **: OCE et les fournisseurs de système de résolution de noms de domaine.** Ces acteurs vont devoir prendre en compte un processus de **conservation des journaux de logs** afin d'envoyer une copie des données techniques non identifiantes à l'ANSSI.

Cela n'aura pas d'impact sur la donnée personnelle car les données collectées seront nettoyées de toute adresse IP source. L'objectif étant d'identifier uniquement le type de réseau utilisé par l'attaquant. Donc les OCE et les fournisseurs de noms de domaine devront mettre en place un moyen permettant de copier et de communiquer régulièrement certaines données de cache DNS anonymisées.

3 Obliger **les éditeurs de logiciel victimes d'un incident informatique sur leurs systèmes d'information** ou **ayant une vulnérabilité critique sur un produit ou un service** à en informer l'ANSSI et leurs clients.

Les premiers à être concernés par cet article de loi sont **les éditeurs de logiciel**. En effet, les vulnérabilités IT des produits proposés par ces éditeurs pouvant être exploitées par les cyber attaquants engendrent des risques et des menaces. Ces attaques peuvent engendrer des **coûts de réparation des SI endommagés et des coûts d'image significatifs**.

Les éditeurs de logiciel vont donc **devoir renforcer leur gouvernance cyber et leur processus de gestion des vulnérabilités (patch management),** et prendre en compte des clauses contractuelles concernant la notification de leurs clients des incidents informatiques compromettant la sécurité de leur SI susceptibles d'affecter leurs produits mais également la notification sur les vulnérabilités significatives affectant un de leurs produits. **Si l'éditeur ne se conforme pas à cette obligation**, l'ANSSI **rendra public la vulnérabilité ou l'incident** et rendra public l'injonction quand l'éditeur n'y a pas donné suite. Le champ d'application de cette obligation est large et devrait s'étendre à la plupart des éditeurs de logiciels **y compris les éditeurs de logiciels SaaS** dont ceux établis en dehors de la France.

4 Renforcer les capacités de détection, de caractérisation et de prévention des attaques chez les : **OCE** (considérés comme OIV) **, opérateurs de centre de données, registrars et les sous-traitants des OIV** (opérateurs d'importance vitale), des **OSE** (Opérateurs de services essentiels) et des **autorités publiques**.

L'article étend les pouvoirs de l'ANSSI dans la mise en œuvre de dispositifs de **détection des menaces cyber**, à travers la mise en place de **marqueurs techniques**, afin de recueillir les données des communications qui transitent par les réseaux des acteurs concernés. Cela permettra de collecter des données sur l'attaquant (comme le code malveillant utilisé et ses logs de connexion). L'ANSSI peut aussi obtenir **une copie du serveur utilisé par le cyber attaquant**.

Un décret sera bientôt publié pour préciser la nature des données qui seront collectées par l'ANSSI. Avec l'émergence du Cloud, les opérateurs de centres de données seront concernés par la mise en place des marqueurs techniques (par l'ANSSI) ou le partage d'une copie de leur serveur avec l'ANSSI

tribu-IT2RM@finegan.fr | www.finegan.fr