Loi de programmation militaire

Foire aux questions (FAQ)

Pourquoi imposer des règles de sécurité aux opérateurs d'importance vitale ?

L'expérience opérationnelle montre que la grande majorité des attaques informatiques peuvent être évitées en respectant quelques bonnes pratiques d'hygiène informatique.

Sur le périmètre des systèmes d'information les plus critiques de la Nation, il est essentiel que ces bonnes pratiques soient systématiquement appliquées. C'est l'objet des règles de sécurité prévues par la LPM.

Quel est l'objectif de la notification des incidents de sécurité à l'ANSSI ?

La notification des incidents de sécurité a pour objectif de permettre à l'ANSSI :

- de proposer à la victime de l'incident une assistance adaptée ;
- d'évaluer la menace au plus vite et de manière plus précise ;
- d'organiser une réponse collective aux attaques informatiques majeures.

Les informations collectées par les notifications d'incidents seront-elles transmises à des tiers ?

La loi prévoit que l'Etat préserve la confidentialité des informations recueillies auprès des opérateurs dans le cadre des notifications d'incidents. Les informations relatives aux incidents de sécurité ne seront donc pas transmises à des tiers.

L'ANSSI pourra utiliser les informations techniques issues des déclarations d'incidents afin d'anticiper et d'analyser les crises. Ces informations, anonymes, pourront notamment être partagées avec les opérateurs d'importance vitale afin de renforcer leur capacité à détecter des attaques sophistiquées.

Existe-t-il des réglementations similaires dans les autres pays européens ?

La France est le premier pays européen à se doter de ce type de réglementation.

La directive NIS (Network and Information Security), en cours de discussion au niveau européen, a notamment pour objectif d'imposer aux Etats membres des obligations similaires en matière de protection de leurs systèmes d'information. La directive prévoit à cet égard que :

- les opérateurs qui seront soumis à ces obligations soient désignés par chaque Etat membre ;
- les règles de sécurité s'appliquant à ces opérateurs soient définies par chaque Etat ;
- les opérateurs doivent notifier les incidents à leur autorité nationale compétente.

En Allemagne, une loi votée en décembre 2014 introduit différentes mesures destinées à renforcer le niveau de cybersécurité des entreprises sensibles, dont l'obligation de notifier les incidents de sécurité à l'agence nationale chargée de la sécurité des systèmes d'information.

Comment les obligations prévues par la LPM s'appliquent-elles aux sous-traitants des OIV ?

Les prestataires qui participent à la sécurité ou au fonctionnement des systèmes d'information d'importance vitale seront soumis aux obligations prévues par la LPM à travers leurs contrats avec les opérateurs d'importance vitale.

La mise en application de ces obligations va-t-elle occasionner un surcoût pour les OIV ?

La sécurité informatique a un coût, mais également un bénéfice : le vol d'informations stratégiques, le sabotage d'une infrastructure ou l'indisponibilité d'un système vital peuvent engendrer des pertes financières bien supérieures au coût de la cybersécurité.

L'objectif des groupes de travail mis en place dans chaque secteur d'activité est d'associer l'ensemble des acteurs concernés afin de définir collectivement des règles de sécurité efficaces, au coût de mise en œuvre soutenable et marginal au regard de l'impact potentiel d'une attaque.

Pour les opérateurs, à terme, une meilleure cybersécurité sera un avantage compétitif.

Quelles seront les conséquences pour un OIV du non-respect d'une règle de sécurité ?

La première conséquence sera l'exposition de ses systèmes vitaux à une menace informatique de plus en plus prégnante. Cela peut avoir un impact sur son activité économique mais engage également sa responsabilité, s'agissant de systèmes dont un dysfonctionnement peut entraîner des conséquences importantes sur la survie de la Nation ou la vie des populations.

Le dispositif LPM prévoit que l'ANSSI, ou des prestataires qualifiés par l'ANSSI, réalisent des contrôles de sécurité ayant notamment pour objectif de vérifier l'application des règles. Si le non-respect d'une règle est constaté lors d'un contrôle, l'opérateur pourra être mis en demeure d'appliquer la règle concernée.

En dernier recours, des sanctions financières, tant pour le dirigeant que pour l'entreprise, sont prévues par la loi.

Quelles sont les prochaines étapes ?

Pour chaque secteur d'activité, un arrêté du Premier ministre précisera :

- les modalités d'identification des systèmes d'information d'importance vitale ;
- les règles de sécurité devant être mises en œuvre sur ces systèmes et les délais de mise en œuvre associés ;
- les modalités de notification à l'ANSSI des incidents de sécurité affectant ces systèmes.

L'objectif des groupes de travail sectoriels mis en place à l'automne 2014 est de préparer ces arrêtés en collaboration avec l'ensemble des acteurs concernés (opérateurs d'importance vitale, ministères coordonnateurs et ANSSI).

A quoi servent les informations que l'ANSSI collecte auprès des opérateurs de communications électroniques en cas de menace informatique ?

Lors d'investigations, l'ANSSI obtient des données techniques concernant des victimes potentielles d'attaques informatiques, mais était jusqu'à présent dans l'incapacité d'identifier le nom et les coordonnées des victimes. Désormais, l'ANSSI pourra obtenir ces informations auprès des opérateurs de communications électroniques, afin d'alerter les victimes et de les accompagner.

Ce dispositif est limité au seul cadre où l'ANSSI agit pour les besoins de la sécurité des systèmes d'information de l'État et des opérateurs d'importance vitale.