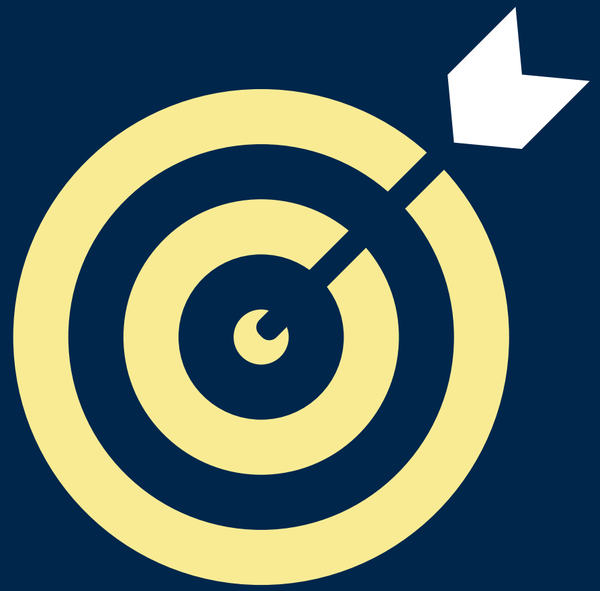
LPM : Quels impacts pour les éditeurs de logiciels ?



Article 66 de la loi de programmation militaire (LPM) 2024-2030 & décret n° 2024-421 du 10 mai 2024 : Quelles consequences pour les éditeurs de logiciels ?

Sommaire

01

Contexte

Contexte

Aux seules fins de garantir la défense et la sécurité nationale, l'ANSSI :

1. peut procéder aux opérations techniques nécessaires à la caractérisation de l'attaque et à la neutralisation de ses effets en accédant aux systèmes d'information qui sont à l'origine de l'attaque pour répondre à une attaque informatique qui vise les systèmes d'information affectant le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation ;

   (Art. **L2321-2** du Code de Défense)

2. peut mettre en œuvre, sur le réseau d'un opérateur de communications électroniques ou sur le système d'information des fournisseurs de services d'hébergement, des fournisseurs d'accès à internet ou d'un opérateur de centre de données des dispositifs permettant de caractériser la menace, lorsqu'elle a connaissance d'une menace susceptible de porter atteinte à la sécurité des systèmes d'information des autorités publiques ou des opérateurs.

   (Art. **L2321-2-1** du Code de la Défense)

De nouvelles opportunités ? De nouveaux risques ?

Que retenir ?

Introduction d'un **nouvel article L2321-4-1** dans le Code de la Défense

- **Exigence clé :** Notification à l'Autorité Nationale de la Sécurité des Systèmes d'Information (ANSSI)
- **Portée** : Application aux éditeurs de logiciels
- **Risque** : nouveau risque d'image / réputationnel

> **Éditeur de logiciel** : toute personne physique ou morale qui conçoit ou développe un produit logiciel ou fait concevoir ou développer un produit logiciel et qui le met à la disposition d'utilisateurs, à titre onéreux ou gratuit.

02

Quelles obligations pour les éditeurs de logiciels ?

Quelles obligations pour les éditeurs de logiciels ?

- Notification à **l'ANSSI**:
  - toute « *vulnérabilité significative* » dans un produit (quel que soit leur mode de distribution)
  - tout incident
  - l'analyse des causes et des conséquences.
- Information **des utilisateurs sur**
  - la vulnérabilité du produit concerné
  - l'incident informatique

03

Quels signalements des vulnérabilités et incidents ?

—

Quels sont les 6 critères pour apprécier la nature significative ?

« *Art. R. 2321-1-16.-I.-Lorsque l'éditeur de logiciel mentionné à l'article L. 2321-4-1 a connaissance* ***d'une vulnérabilité*** *affectant un de ses produits ou en* ***cas d'incident informatique*** *compromettant la sécurité de son système d'information et susceptible d'affecter un de ses produits,* ***il en apprécie le caractère significatif, notamment au regard des critères suivants :***

« 1° Le nombre d'utilisateurs concernés par la vulnérabilité ou l'incident affectant le produit ;
« 2° Le nombre de produits intégrant le produit affecté ;
« 3° L'impact technique, potentiel ou actuel, de la vulnérabilité ou de l'incident sur le fonctionnement attendu du produit. Selon les fonctionnalités du produit, cet impact est évalué au regard de critères de sécurité tels que la disponibilité, l'intégrité, la confidentialité ou la traçabilité ;
« 4° Le type de produit au regard de ses usages et de l'environnement dans lequel il est déployé ;
« 5° L'exploitation imminente ou avérée de la vulnérabilité ;
« 6° L'existence d'une preuve technique d'exploitabilité ou d'un code d'exploitation. »

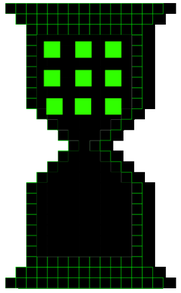
Formulaire disponible sur le site de l'ANSSI !

Quels délais à respecter par les éditeurs de logiciels ?

Le décret n°2024-421 du 10 mai 2024 precise la procedure de

- Notification à l'ANSSI :
  - Lorsque la vulnérabilité ou l'incident a été notifié par l'ANSSI à l'éditeur de logiciel, ce dernier dispose d'un délai fixé par l'autorité pour apprécier son **caractère significatif.**
  - Le délai ne peut être inférieur à **48h.**

- Information des utilisateurs :
  - Après analyse conjointe de la vulnérabilité ou de l'incident avec l'éditeur, **l'ANSSI notifie** à ce dernier le **délai dans lequel il doit informer les utilisateurs.**
  - Ce délai ne peut pas être inférieur **à 10 JOURS OUVRABLES.**
  - Il existe une exception : en cas de **risques pour la défense et la sécurité nationale, l'information est sans délai.**



04

Quels changements pour l’ANSSI ?

Quels sont les nouveaux pouvoirs de l'ANSSI ?

Le décret n°2024-421 du 10 mai 2024 precise la procédure d’injonction :

- A défaut d'information des utilisateurs par l'éditeur : **injonction possible de l'ANSSI**
  - L’injonction est motivée et mentionne le délai imparti qui ne peut être inférieur à 10 jours, ainsi que les mesures requises pour s’y conformer.

- Capacité à **rendre publics les vulnérabilités et incidents**
  - L’ANSSI peut procéder à l’inf**ormation des utilisateurs ou du public** via le site du centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques.
  - Elle peut également **rendre publique l'injonction**, sur son site Internet, lorsque celle-ci a été partiellement ou totalement inexécutée

05

Quel recueil de données ?
Quelle compensation des surcoûts ?

—

Quels dispositifs ? Quelle nature des données recueillies ?

Les marqueurs techniques définis par le décret :

- « Les marqueurs techniques exploités par les dispositifs mentionnés au I de l'article R. 2321-1-1 sont des **éléments techniques** caractéristiques d'un mode opératoire **d'attaque informatique**, permettant de détecter une **activité malveillante ou d'identifier une menace susceptible d'affecter la sécurité des systèmes d'information.** » (**Art. R2321-1-4** du Code de la Défense)
- permettent la détection des communications et programmes informatiques malveillants ainsi que le recueil et l'analyse des seules données techniques nécessaires à la prévention et à la caractérisation de la menace

Les dispositifs permettent le recueil de données :

- sur le réseau d'un opérateur de communication électronique d'un opérateur de communications électroniques ou sur le système d'information d'une personne ou d'un opérateur de centre de données affecté par la menace (**Art. L2321-2-1** du Code de la Défense) ;
- relatives aux communications électroniques émises et reçues par un équipement affecté par la menace (**Art. R. 2321-1-1** du Code de la Défense) ;
- sur un équipement affecté par la menace (**Art. R. 2321-1-1** du Code de la Défense).

Leurs finalités : détecter et caractériser des événements susceptibles d'affecter la sécurité

- des systèmes d'information des autorités publiques,
- des opérateurs mentionnés aux articles L. 1332-1 et L. 1332-2 du Code de la Défense,
- des opérateurs publics ou privés participant aux systèmes d'information de ces entités.

(**Art. L2321-2-1** du Code de la Défense)

Comment sont compensés les surcoûts ?

1

« Les surcoûts liés à la **réalisation de prestations dont la compensation est établie sur la base du montant hors taxes de tarifs fixés par arrêté** conjoint du Premier ministre et du ministre chargé des communications électroniques. »

L'Etat procède, sur **présentation d'une facture**, au paiement des compensations correspondant aux surcoûts justifiés.

2

« Les surcoûts liés à la **conception et au déploiement des systèmes d'information** ou, le cas échéant, à leur **adaptation**, permettant la mise en place d'un dispositif exploitant des **marqueurs techniques** ou le **recueil** des données ainsi que les surcoûts liés au **fonctionnement et à la maintenance de ces systèmes**. »

L'opérateur adresse à l'ANSSI un **document assorti des justificatifs** nécessaires permettant d'établir le nombre et la nature des interventions nécessaires.

L'Etat procède, après analyse du document transmis, et sur **présentation d'une facture**, au paiement des compensations correspondant aux surcoûts justifiés;

Art. **R. 2321-1-6**
du Code de la Défense

06

Comment vous préparer ?

Comment vous préparer ?

- Actions recommandées pour les éditeurs de logiciels :

  - Audits réguliers de vulnérabilités des logiciels commercialisés ou mis à disposition à titre gratuit
  - Politiques de gestion des incidents
  - Définition d'une organisation interne permettant la notification à l'ANSSI et l'information des utilisateurs, ainsi que la gestion de leurs conséquences *(remontée d'informations, auteur de la notification, suivi de la notification et de l'information aux utilisateurs…)*
  - Plan de communication envers les utilisateurs

Suivez votre actualité, abonnez-vous !

Au quotidien

Une newsletter offerte

L'actualité décryptée pour vous

Mathias | Avocats

Contactez-nous !

Vous accompagner dans le développement de vos projets, former vos équipes :

nous mettons nos expertises à votre service !

Catalogue des formations

19 rue Vernier 75017 PARIS
+33 (0)1 43 80 02 01
contact@avocats-mathias.com

@MathiasAvocats

https://www.avocats-mathias.com/