NIS2

La directive NIS 2 | ANSSI (cyber.gouv.fr)

Directive - 2022/2555 - EN - EUR-Lex (europa.eu)

sécurité informatique (cours-cherry.fr)

La norme NIS2, ou Directive sur la sécurité des réseaux et des systèmes d'information révisée, est un cadre réglementaire de l'Union européenne conçu pour améliorer la sécurité informatique à travers ses États membres. Voici un document détaillé en deux parties, explorant d'abord les principes et objectifs de cette directive, puis les implications et les exigences pour les organisations concernées.

I. Présentation et objectifs de la NIS2

1. Contexte et évolution

La directive NIS originale a été le premier pas vers une législation européenne unifiée sur la cybersécurité, établie pour répondre aux défis croissants posés par les cyberattaques. Avec l'évolution rapide des technologies et l'augmentation des menaces, la révision de cette directive était nécessaire. Adoptée en 2023, la NIS2 remplace la directive NIS de 2016, en élargissant son champ d'application et en renforçant les exigences de sécurité.

2. Principaux objectifs

La directive NIS2 vise à atteindre plusieurs objectifs clés :

- **Renforcer les niveaux de sécurité cybernétique** dans toute l'Union européenne pour les opérateurs de services essentiels et les fournisseurs de services numériques.
- **Harmoniser les exigences de sécurité** pour assurer une approche cohérente et coordonnée à l'échelle de l'UE.
- **Améliorer la coopération entre les États membres**, notamment par le partage d'informations sur les incidents et les menaces cybernétiques.

3. Champ d'application

La NIS2 étend son champ d'application par rapport à la directive originale, couvrant plus de secteurs et incluant de nouvelles catégories d'entités telles que les centres de traitement des données, les fabricants de dispositifs médicaux critiques, et les entreprises des secteurs énergétiques, des transports, de la santé, et numérique, entre autres.

II. Implications et exigences pour les organisations

1. Exigences de sécurité

Sous la NIS2, les entités concernées doivent adopter des mesures techniques et organisationnelles appropriées pour gérer les risques de sécurité des réseaux et de l'information. Cela comprend :

- **Gestion des incidents** : mise en place de procédures pour détecter, répondre et récupérer après des incidents de sécurité.
- **Mesures de sécurité proactives** : utilisation de la cryptographie, de la sécurité physique, et de la sécurité des applications pour protéger contre les menaces.

- **Politiques de sécurité** : développement de politiques internes pour la formation, les audits, et la gestion des risques.

2. Notification des incidents

Les entités doivent notifier les incidents significatifs aux autorités nationales compétentes dans un délai rapide. Cette exigence permet une réaction coordonnée à l'échelle de l'UE et aide à prévenir la propagation des dommages.

3. Sanctions et conformité

La directive établit des sanctions en cas de non-conformité, qui peuvent inclure des amendes substantielles. Les États membres doivent établir des autorités réglementaires compétentes pour surveiller l'application de la NIS2 et imposer des mesures correctives si nécessaire.

4. Coopération internationale

La NIS2 encourage la coopération non seulement entre les États membres de l'UE mais aussi avec des pays tiers, pour améliorer la réponse globale aux cybermenaces internationales.

III Entreprises concernées

1. Entités Essentielles (EE)

Les "Entités Essentielles" sont des organisations qui sont vitales pour le maintien de services critiques. Elles sont donc soumises à des exigences réglementaires plus strictes en vertu de la NIS2.

Caractéristiques des EE:

- **Secteurs d'activité:** Ces entités opèrent généralement dans des secteurs considérés comme critiques pour l'infrastructure nationale, tels que l'énergie, les transports, la santé et la fourniture d'eau potable.
- **Exigences:** Les EE doivent adopter des mesures de cybersécurité avancées pour prévenir, détecter, et répondre à des incidents. Elles doivent également signaler les incidents de sécurité à des autorités nationales dans un délai très court.
- **Surveillance réglementaire:** Elles sont soumises à une surveillance plus intensive de la part des autorités nationales compétentes, qui peuvent effectuer des audits réguliers et demander des rapports de conformité détaillés.

2. Entités Importantes (EI)

Les "Entités Importantes" sont également soumises à la directive NIS2 mais avec un degré de régulation légèrement moindre comparé aux EE. Ces entités sont importantes pour la continuité des services, mais leur impact en cas de défaillance est considéré comme moins critique que celui des EE.

Caractéristiques des EI:

- **Secteurs d'activité:** Les EI peuvent également opérer dans des secteurs critiques, mais leur rôle ou leur impact est généralement perçu comme moins direct sur la sécurité nationale ou la vie quotidienne des citoyens.
- **Exigences:** Les EI doivent aussi mettre en place des mesures de sécurité appropriées et signaler les incidents, mais les délais de notification et les critères de rapport peuvent être moins stricts que pour les EE.
- **Surveillance réglementaire:** Bien que régulées, les vérifications et les exigences de conformité pour les EI peuvent être moins fréquentes ou moins approfondies que pour les EE.

Application et Conformité

Dans la pratique, les États membres de l'UE sont responsables de la définition précise de quelles entités sont classées comme EE ou EI, basé sur les directives de la NIS2. Ils doivent également mettre en place des cadres réglementaires pour assurer que ces entités respectent les obligations de sécurité et de rapport définies par la directive.

La distinction entre EE et EI aide à prioriser les ressources et les efforts de conformité, en s'assurant que les entités les plus critiques pour la société bénéficient de la protection la plus robuste, tout en maintenant un niveau de sécurité adéquat pour d'autres entités importantes.