Directive NIS et NIS 2

Abdelwaheb SEBA - Mohammed Ryad DERMOUCHE

Table des matières

1 Introduction

La cybersécurité est devenue un enjeu crucial à l'échelle européenne avec la multiplication des attaques informatiques. Pour répondre à ces défis, l'Union européenne a introduit la directive **NIS** (Network and Information Security), suivie de sa version améliorée, la **directive NIS 2**.

Ce document présente une version **simplifiée** des deux directives et explique leurs **relations** et **différences** pour une meilleure compréhension.

2 Directive NIS 1 : Explication et Relations entre les Acteurs

2.1 Principes Clés

- **Objectif :** Assurer un niveau élevé de sécurité des réseaux et systèmes d'information dans l'UE.
- **Acteurs Ciblés :** Principalement les **OSE** (Opérateurs de Services Essentiels) et les **FSN** (Fournisseurs de Services Numériques).

2.2 Les Acteurs Principaux et Structures de Coopération

Les acteurs principaux :

- **ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information)** :
  - Rôle principal en France pour superviser la cybersécurité.
  - Contrôle les OSE et les FSN pour s'assurer qu'ils respectent les règles de sécurité.
- **OSE (Opérateurs de Services Essentiels)** :
  - Ce sont des entreprises dont les services sont critiques pour le bon fonctionnement de la société (énergie, transport, santé...).
  - Exemples : EDF, SNCF, hôpitaux.
  - Obligations : Sécuriser leurs systèmes et signaler les incidents à l'ANSSI.
- **FSN (Fournisseurs de Services Numériques)** :
  - Ce sont des entreprises fournissant des services numériques comme :
    - Places de marché en ligne (ex : Amazon),
    - Moteurs de recherche (ex : Google),
    - Cloud (ex : AWS).
  - Obligations : Analyser les risques, sécuriser les systèmes et déclarer les incidents à l'ANSSI.

2.3 Relations entre les termes

- L'ANSSI contrôle les OSE et les FSN pour vérifier qu'ils appliquent les règles de sécurité imposées par la directive NIS.
- Les OSE et les FSN doivent déclarer tout incident majeur à l'ANSSI.
- Les incidents peuvent être partagés entre les pays européens via le réseau des CSIRT pour une réponse rapide.

2.4 Structures de coopération

- **CSIRT (Computer Security Incident Response Team)** :
  - Équipes techniques qui répondent aux incidents de sécurité.
  - En France, c'est le CERT-FR (le CSIRT national géré par l'ANSSI).
  - Les CSIRT collaborent à l'échelle européenne via le CSIRT Network pour partager des informations sur les menaces.
- **Groupe de coopération (au niveau européen)** :
  - Réunit les États membres et la Commission européenne pour :
    - Coordonner les efforts en cybersécurité,
    - Partager des bonnes pratiques,
    - Définir des méthodologies communes.

2.5 Résumé Simplifié

- **NIS 1** impose aux **OSE** et **FSN** de prendre des mesures de cybersécurité et de **déclarer rapidement** tout incident majeur.
- L'**ANSSI** veille au respect de ces mesures en France.
- Les **CSIRT** partagent les informations entre les pays de l'UE pour une réponse rapide et coordonnée.

3 Directive NIS 2 : Évolution et Nouveautés

3.1 Contexte

Face à des cyberattaques **toujours plus complexes** et fréquentes, la directive NIS 2 vient renforcer et étendre les dispositions de NIS 1 pour mieux protéger les entreprises et les administrations.

3.2 Nouveautés Principales

- **Périmètre Élargi :**
  - Couvre davantage de secteurs (administrations publiques, infrastructures critiques, industries de haute technologie, etc.).
- **Obligations Renforcées :**
  - Protection des chaînes d'approvisionnement.
  - Gestion des risques et plans de continuité.
  - Gestion des incidents **plus rigoureuse**.
- **Coopération Européenne Accrue :**
  - Mise en place du réseau **CyCLONe** pour une **gestion de crise** cyber unifiée.
  - Coordination améliorée avec les CSIRT nationaux.
- **Sanctions Plus Strictes :**
  - Amendes plus élevées en cas de non-conformité.
  - Exigence de transparence : incidents graves à rendre publics si nécessaire.

3.3 Comparaison avec NIS 1

- **Élargissement du Périmètre** : NIS 2 inclut plus de secteurs et entités que NIS 1.
- **Renforcement des Obligations** : Des mesures de sécurité plus strictes et des déclarations d'incidents plus rapides.
- **Coopération Internationale** : La directive formalise la coopération via des réseaux comme CyCLONe(Cyber Crisis Liaison Organization Network), améliorant la coordination entre les États membres.
- **Sanctions Renforcées** : Les conséquences du non-respect sont plus sévères, incitant fortement à la conformité.

3.4 Exemple Simplifié : CyCLONe en Action

Exemple simplifié :
Supposons qu'un **ransomware** (logiciel malveillant) infecte simultanément les réseaux électriques en **France**, **Allemagne**, et **Espagne**.

- Chaque pays détecte l'attaque et informe immédiatement **CyCLONe** via son **CSIRT national** (par exemple, en France : le CERT-FR).
- Grâce à **CyCLONe** :
  - Les experts des pays touchés se réunissent rapidement en ligne.
  - Ils partagent les informations techniques sur l'attaque, son origine, et les mesures de protection.
  - Ils coordonnent les réponses communes (par exemple : bloquer certains accès réseau, isoler les systèmes infectés).
  - Si nécessaire, des décisions stratégiques communes sont prises (ex. : mobilisation d'équipes de cybersécurité européennes).

3.5 Résumé Simplifié

- **NIS 2** répond aux cybermenaces modernes avec un **périmètre élargi**, des **obligations renforcées** et une **coopération internationale accrue**.
- **ANSSI**, en France, reste l'autorité compétente pour la mise en application de NIS 2.

4 Conclusion

La transition de **NIS 1** à **NIS 2** marque un tournant majeur dans la réglementation de la cybersécurité en Europe. En élargissant son champ d'application et en renforçant les obligations de sécurité, NIS 2 répond aux défis posés par des **cyberattaques toujours plus sophistiquées**.

L'**ANSSI**, en tant qu'autorité nationale, joue un rôle essentiel pour **accompagner** et **contrôler** les entités concernées, qu'il s'agisse d'Opérateurs de Services Essentiels (**OSE**) ou de Fournisseurs de Services Numériques (**FSN**), mais aussi désormais de nouvelles organisations publiques ou privées.