Directive NIS 2

Champ d'application, exigences de sécurité, sanctions, compétences et contrôles

Présentation à l'OSSIR – 13/02/2024

Maxime ANTOINE

Sommaire

01

Contexte : De NIS 1 à NIS 2

Contexte : De NIS (=SRI) à NIS 2 (=SRI 2)

NIS
DIRECTIVE (UE) 2016/1148

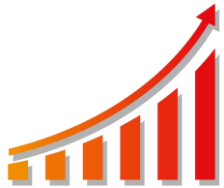
NIS 2
DIRECTIVE (UE) 2022/2555

Transposition Octobre 2024

Règles pour l'accompagnement

Règles plus coercitives

Socle de sécurité



Augmentation des exigences et des sanctions

Opérateurs de services essentiels

Fournisseurs de service numérique

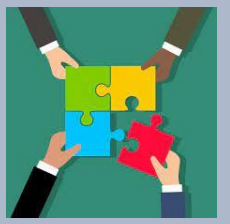
Entités essentielles

Entités importantes

Désignation des entités

Déclaration des entités
au plus tard à partir du 17 janvier 2025

Ce qui ne change pas



Coopération entre les Etats, la Commission et l'ENISA

Réseau des CSIRT

Partage d'information volontaire

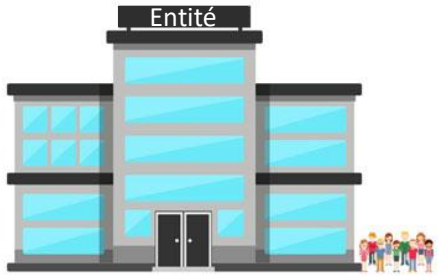
Harmonisation minimale ou désharmonisation maximale ?

02

LE CHAMP D'APPLICATION

Le champ d'application de NIS 2
Une règle générale (art. 2, 1.)

Une personne dotée de la la personnalité juridique



Une personne physique ou morale ayant, en son nom propre, la capacité d'être titulaire de droits et d'obligations

D'une certaine taille

Moyenne entreprise	Grande entreprise
Chiffre d'affaires annuel > 10 millions €	Chiffre d'affaires annuel > 50 millions €
OU	OU
Bilan annuel > 10 millions €	Bilan annuel > 43 millions €
OU	OU
Effectif >= 50	Effectif >= 250

Recommandation 2003/361/CE, article 2

Qui fournit un certain service ou exerce une certaine activité

Activité hautement critique

Activité critique

Au sein de l'Union européenne

Exercer ou fournir au sein de l'UE n'implique pas d'y être établi

Le champ d'application de NIS 2
Plusieurs exceptions (art. 2, 2. à 4.)

L'entité est opérateur de service essentiel au sens de la Directive NIS 1

L'entité est critique au sens de la Directive sur la Résilience des Entités Critiques (CER)

L'entité est désignée par un Etat membre car elle fournit un service :

- nécessaire au maintien d'activités sociétales ou économiques critiques et pour lequel elle est le seul acteur à le fournir; ou
- dont la perturbation pourrait avoir un impimpact important sur la sécurité publique, la sûreté publique ou la santé publique ; ou
- Dont la perturbation pourrait induire un risque systémique important ; ou

L'entité est critique en raison de son importance spécifique au niveau national ou régional pour le secteur ou le type de service en question, ou pour d'autres secteurs interdépendants dans l'État membre.

L'entité est une entité de l'administration publique particulière

L'entité est un fournisseur de service numérique particulier

Le champ d'application de NIS 2

Les entités essentielles et importantes (art. 2 et 3 pris ensemble)

Catégories d'entités	Très petites ou petites entreprises	Moyennes entreprises	Grandes entreprises
Entités d'un type visé à l'annexe I	N/A	Entités importantes	Entités essentielles
Entités d'un type visé à l'annexe II	N/A	Entités importantes	Entités importantes
Prestataires de services de confiance qualifiés	Entités essentielles		
Registres de noms de domaine de premier niveau	Entités essentielles		
Fournisseurs de services DNS	Entités essentielles		
Fournisseurs de réseaux publics de communications électroniques publics	N/A	Entités essentielles	
Fournisseurs de services de communications électroniques accessibles au public	N/A	Entités essentielles	
Entités fournissant des services d'enregistrement de noms de domaine	Entités importantes		
Entités d'un type visé à l'annexe I ou II identifiée par un État membre en tant qu'entité essentielle en vertu de l'article 2, paragraphe 2, points b) à e)	Entités essentielles		
Entités d'un type visé à l'annexe I ou II identifiée par un État membre en tant qu'entité importante en vertu de l'article 2, paragraphe 2, points b) à e)	Entités importantes		
Entités critiques au sens de la directive (UE) 2022/2557	Entités essentielles		
Entités identifiées avant le 16/01/2023 comme Opérateurs de services essentiels au sens de la directive (UE) 2016/1148	Entités essentielles		
Entités de l'administration publique des pouvoirs publics centraux tels qu'ils sont définis par un État membre conformément au droit national	Entités essentielles		
Entité de l'administration publique au niveau régional, tel qu'il est défini par un État membre conformément au droit national, qui, à la suite d'une évaluation basée sur les risques, fournit des services dont la perturbation pourrait avoir un impact important sur des activités sociétales ou économiques critiques	Entités importantes		

Le champ d'application de NIS 2

Secteurs dont les activités sont hautement critiques ou critiques (annexes I et II)

Activités hautement critiques (annexe I)

- Electricité
- Réseaux de chaleur et de froid
- Pétrole
- Gaz
- Hydrogène
- Transports aériens
- Transports ferroviaires
- Transports par eau
- Transports routiers
- Secteur bancaire
- Infrastructures des marchés financiers
- Santé
- Eau potable
- Eau usée
- Infrastructure numérique
- Gestion des services TIC
- Administration publique
- Espace

Activités critiques (Annexe II)

- Services postaux et d'expédition
- Gestion des déchets
- Fabrication, production et distribution de produits chimiques
- Production, transformation et distribution des denrées alimentaires
- Fabrication de dispositifs médicaux et de dispositifs médicaux de diagnostic in vitro
- Fabrication de produits informatiques, électroniques et optiques
- Fabrication d'équipements électriques
- Fabrication de machines et équipements n.c.a.
- Construction de véhicules automobiles, remorques et semi-remorques
- Fabrication d'autres matériels de transport
- Fournisseurs numériques
- Recherche

Le champ d'application de NIS 2
Les interrogations qui persistent concernant le champ d'application

1- Un effet de bord lié à la possible applicabilité de l'article 6 de la Recommandation 2003/361/CE

L'article 2 de la directive NIS 2 n'exclut expressément que l'applicabilité de l'article 3, §4 concernant les PME dont une partie du capital ou des droits de vote sont contrôlés par un/des organisme(s) publique(s) ou collectivité(s) publique(s).

L'article 6 de la recommandation, non expressément exclu par la Directive, prévoit que les seuils applicables à une entité partenaires ou liées sont déterminées sur la base des comptes et effectifs globaux/consolidés du groupe.

En conséquence, une entité ne dépassant pas les seuils, lorsqu'elle est prise unitairement, pourrait toutefois être soumise à la Directive NIS 2 si elle fait partie d'un groupe d'entités.

2- L'indétermination lorsqu'une entité fournit différents services ou exerce différentes activités au sein de l'UE

Quid d'une entité qui serait concernés à la fois par l'annexe I et par l'annexe II ?

3- L'applicabilité délicate de la Directive pour des activités / services opérés conjointement par des entités d'un groupe

Y'aura-t-il l'ajout de la notion de groupe de sociétés dans les transpositions ?

4- L'indétermination concernant l'identification par les Etats d'entités supplémentaires soumises à la Directive NIS 2

Quid de l'appréciation des Etats concernant les entités qu'ils détermineront eux-mêmes comme essentielles ou importantes ?

Toutes ces interrogations sont d'autant plus importantes que chaque Etat pourrait avoir une appréciation différente de ces problématiques dans leur texte de transposition respectif

03

EXIGENCES DE SÉCURITÉ ET OBLIGATIONS D'INFORMATION

Les exigences minimales de sécurité

Gouvernance
(art. 20)

Les organes de direction
- approuvent les mesures de gestion des risques en matière de cybersécurité ;
- supervisent sa mise en œuvre ;
- sont responsables du non-respect des obligations.

Les membres de l'organe de direction doivent suivre des formations pour être en mesure d'appréhender et évaluer
- les risques ;
- les pratiques de gestion en matière de cybersécurité ;
- les incidences sur les activités de l'entité.

Les membres de l'organe de direction doivent offrir régulièrement une formation similaire aux membres de leur personnel.

Mesures de gestion des risques en matière de cybersécurité fondées sur une approche « tous risques »
(art. 21)

- **Des politiques pour l'analyse des risques et de sécurité des systèmes d'information**
- **La gestion des incidents**
- **La continuité des activités et la gestion des crises**
- **La sécurité de la chaîne d'approvisionnement**
- **La sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information**
- **Des politiques et des procédures pour évaluer l'efficacité des mesures de gestion des risques**
- **Les pratiques de base en matière de cyberhygiène et la formation à la cybersécurité**
- **Des politiques et des procédures relatives à l'utilisation de la cryptographie et, le cas échéant, du chiffrement**
- **La sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs**
- **L'utilisation de solutions d'authentification à plusieurs facteurs ou d'authentification continue et de communications sécurisées**

Pour vos mesures, tenir compte :
- de l'état des connaissances ;
- des normes applicables ;
- du coût de mise en œuvre.

Mais aussi :
- du degré d'exposition aux risques
- de la taille de l'entité
- de la vraisemblance du risque
- des impacts des risques

Les obligations d'information (art. 23)

« 3. Un incident est considéré comme important si:

- Perturbation opérationnelle grave pour l'entité
- Perte financière pour l'entité
- Dommages matériels, corporels ou moraux considérables potentielles pour d'autres personnes

Notifications d'un incident important au CSIRT ou à l'autorité compétente

Incident important

24H max

72H max

1 mois max après la notification d'incident
OU
1 mois max après le traitement de l'incident

1. **Alerte précoce** concernant l'incident important précisant si l'on suspecte qu'il résulte d'un acte malveillant ou illicite et s'il peut avoir un impact transfrontière
2. **Notification d'incident** avec mise à jour des informations de l'alerte et fourniture d'une évaluation initiale de l'incident, comprenant gravité, impact et indicateurs de compromission (si disponible)
3. **Rapport(s) intermédiaire(s)** sur les mises à jour pertinentes de la situation sur demande d'un CSIRT ou de l'autorité compétente
4. **Rapport d'avancement** si l'incident n'est pas traité 1 mois après la notification d'incident
5. **Rapport final** comprenant :
   1. une description détaillée de l'incident, y compris de sa gravité et de son impact
   2. le type de menace ou la cause profonde qui a probablement déclenché l'incident;
   3. les mesures d'atténuation appliquées et en cours;
   4. le cas échéant, l'impact transfrontière de l'incident;

Notifications aux destinataires des services

Informations concernant les incidents importants susceptibles de nuire à la fourniture de ces services

Informations concernant la cybermenace importante et toutes les mesures ou corrections que ces destinataires peuvent appliquer en réponse à cette menace

sans retard injustifié
(pas de délai précis pour le moment)

04

Sanctions

Les sanctions minimales

1- Sanctions non-pécuniaires (art.32 et 33)

A l'encontre des entités importantes ou essentielles

- Avertissement en cas de non-conformité
- Ordre d'informer les acteurs concernés ou les personnes potentiellement touchées par une cybermenace *(nature de la menace et mesures préventives)*
- Ordre de rendre public les aspects de violation des exigences de sécurité
- Ordre :
  - de mettre un terme à un comportement non-conforme ;
  - de mettre en œuvre la réglementation ;
  - de mettre en œuvre des recommandations suite à un audit ;
  - de garantir la conformité des mesures

A l'encontre des entités essentielles

- Ordre de désigner, pour une période déterminée, un responsable du contrôle chargé de veiller au respect de la réglementation par l'entité *(délégué temporaire à la protection des SI)*
- Interdiction temporaire aux personnes physiques d'exercer une fonction de direction ou de représentation légale
- Suspension d'une certification ou d'une autorisation concernant tout ou partie des services ou activités

2- Sanctions pécuniaires (art. 34)

A l'encontre des entités importantes	A l'encontre des entités essentielles
• jusqu'à 7 M€ ou 1,4% chiffre d'affaires annuel mondial total d'une entité importante • des astreintes afin de contraindre une entité essentielle ou importante à cesser une infraction	• jusqu'à 10 M€ ou 2 % chiffre d'affaires annuel mondial total d'une entité essentielle • des astreintes afin de contraindre une entité essentielle ou importante à cesser une infraction

Pas de cumul de sanction si l'entité est sanctionnée pour les mêmes non-conformités sur le fondement du RGPD (art.35)

05

Compétence territoriale et contrôles

La compétence territoriale des autorités

En principe, l'autorité compétente est celle du pays dans lequel l'entité est établie (siège social)

Pour :
- **les fournisseurs de réseaux de communications électroniques publics**
- **les fournisseurs de services de communications électroniques accessibles au public**

L'autorité compétente est celle du pays de l'UE dans lequel ils fournissent leurs services

Les entités de l'administration publique sont placées sous l'autorité de l'Etat membre qui les a établies

Pour les FSN

Il faut procéder par élimination.

L'autorité compétente est celle de l'Etat membre de l'UE dans lequel le FSN :

1. **est établi ; ou à défaut**
2. **prend, en UE, les principales décisions relatives aux mesures de gestion des risques en matière de cybersécurité ; ou à défaut**
3. **effectue des opérations de cybersécurité ; ou à défaut**
4. **possède l'établissement comptant le plus grand nombre de salariés ; ou à défaut**
5. **a désigné un représentant** (ce représentant devant être dans un des Etats membres dans lesquels les services sont fournis)

Deux principaux écueils possibles avec cette répartition des compétences

1. la Directive NIS 2 vise les entités juridiques unitairement et jamais les groupes de société, ce qui rend théoriquement inopérant la désignation de l'autorité compétente sur le fondement des critères exposés pour les FSN.
   Toutefois, c'est une directive à harmonisation minimale qui n'empêche donc pas les Etats d'inclure des exigences pour les groupes de sociétés
2. le forum shopping est ouvert pour les FSN étranger sans aucun établissement identifiable dans l'UE

Les moyens de contrôles minimaux
(art. 32 et 33)

A l'encontre des entités importantes ou essentielles
Inspections sur place et surveillance à distance ex post
Audits de sécurité ciblés fondés sur des évaluations des risques ou sur des informations disponibles ayant trait aux risques
Scans de sécurité fondés sur des critères d'évaluation des risques objectifs, équitables et transparents
Demandes de toutes informations nécessaires à l'évaluation ex post des mesures de cybersécurité, notamment les politiques de cybersécurité consignées par écrit, ainsi que du respect de l'obligation de notifier l'ENISA
Demandes d'accès à des données, à des documents et/ou à des informations nécessaires à l'accomplissement de leurs missions de surveillance

A l'encontre des entités essentielles
Des audits réguliers
Demandes de preuves de la mise en œuvre de politiques de cybersécurité, telles que les résultats des audits de sécurité effectués par un auditeur qualifié et les éléments de preuve sous-jacents correspondants

Merci