NIS 2

"TOUT CE QUE VOUS AVEZ TOUJOURS VOULU SAVOIR SUR NIS 2 SANS JAMAIS OSER LE DEMANDER"

ÉPISODE 1

BILAN DE LA DIRECTIVE NIS 1 ET CADRE GÉNÉRAL POUR NIS 2

Avec l'entrée en vigueur de la directive NIS 2, le cadre de régulation de la cybersécurité en Europe se renforce considérablement. Cette nouvelle directive est issue d'un bilan de la première directive (NIS 1) qui a conduit à des évolutions tangibles.

Bilan de la première directive NIS 1 :
La directive NIS 1 élaborée en 2016 a été considérée comme un succès à bien des égards même si elle a été transposée de manière très hétérogène par les États membres. Cela a conduit à des distorsions à l'échelle européenne.

Parallèlement, la menace cybercriminelle a explosé à partir de 2020 conduisant à des impacts très lourds sur une grande variété de victimes : PME, ETI, collectivités territoriales. Les entreprises de services numériques (ESN) constituent un type de victime spécifique avec un possible effet de levier vis-à-vis de leurs clients. Tous ces acteurs étaient en dehors du champ des entités régulées de la directive NIS 1.

Les nouveautés de la directive NIS 2 :
La directive NIS 2 définit ainsi des règles beaucoup plus précises et structurées dont l'objectif est de conduire à une transposition bien plus homogène et cohérente de la directive dans les textes nationaux des différents États membres.

Du fait de l'explosion de la menace, la directive NIS 2 étend son champ d'application à de nouveaux secteurs et à un périmètre plus large de types d'entités. Pour respecter un principe de proportionnalité, deux catégories d'entités ont été créées : les entités essentielles (EE) - qui correspondent, pour simplifier, aux actuels opérateurs de services essentiels (OSE) de la directive NIS 1 - et les entités importantes (EI). Cela devrait conduire le périmètre des entités régulées en France d'environ 500 à 15 000.

La notion de système d'information essentiel (SIE) est abandonnée. C'est l'ensemble des systèmes d'information d'une entité qui sont concernées dans la nouvelle directive NIS 2.

ÉPISODE 2

QUELS SONT LES CRITÈRES POUR FAIRE PARTIE DES FUTURES 15 000 ENTITÉS CONCERNÉES PAR LA DIRECTIVE ?

Pour respecter un principe de proportionnalité, deux catégories d'entités ont été créées : Les entités essentielles (EE), qui correspondent, pour simplifier, aux actuels opérateurs de services essentiels (OSE) de la directive NIS 1, et une nouvelle catégorie, les entités importantes (EI).

On devrait donc avoir la répartition suivante en France :
Environ 500 à 1000 entités essentielles et plus de 10 000 entités importantes.
Le principe général est que les entités de taille moyenne, intermédiaire ou grande, réalisant des activités dans les annexes 1 et/ou 2 de la directive, seront concernées par la directive NIS 2 en tant qu'entité essentielle (EE) ou entité importante (EI).

Sauf exceptions (notamment pour les fournisseurs de services numériques), le tableau de synthèse pour savoir si une entité est concernée est dans l'image attachée à ce post. Le premier critère sur le nombre d'employés est autonome ; les 2 critères financiers sont à prendre ensemble. En résumé, nombre d'employés OU chiffre d'affaires annuel ET bilan annuel.

Par exemple : si une entité dont le secteur d'activité est référencé dans l'annexe 1 a plus de 250 salariés, alors cette entité est désignée comme entité essentielle, même si son chiffre d'affaires annuel est inférieur à 50 M€.

Secteurs des entités essentielles (EE) - Annexe I de la directive :
- Énergie, transports, secteur bancaire, infrastructures des marchés financiers.
- Santé, eau potable, eaux usées, infrastructures numériques.
- Gestion des services des technologies de l'information et de la communication, administrations publiques, espace.

Dans le cadre du projet de loi présenté en conseil des ministres le 17 octobre 2024, les collectivités territoriales couvrant plus de 30 000 habitants sont désormais désignées comme entités essentielles (EE).

Secteurs des entités importantes (EI) - Annexe II de la directive :
- Services postaux et d'expédition, gestion des déchets.
- Fabrication, production et distribution de produits chimiques.
- Production alimentaire et industries manufacturières.
- Fournisseurs de services numériques, recherche, etc.

ÉPISODE 2

QUELS SONT LES CRITÈRES POUR FAIRE PARTIE DES FUTURES 15 000 ENTITÉS CONCERNÉES PAR LA DIRECTIVE ?

ÊTES-VOUS CONCERNÉ PAR LA DIRECTIVE NIS 2 ?

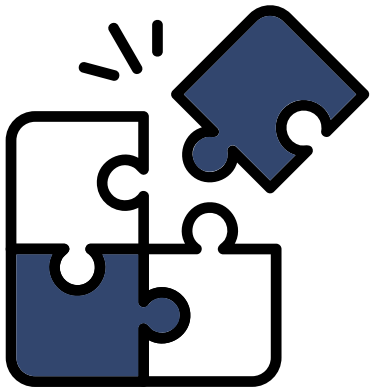
Vérifiez dans quel secteur vous êtes :

- Si votre entité n'est pas identifiée dans l'un des secteurs de l'annexe 1 ou de l'annexe 2, vous n'êtes pas concerné par cette réglementation.
- Si vous êtes dans l'annexe 1 ou 2, consultez le tableau ci-dessous pour déterminer si votre organisation relève de la Directive NIS 2.

ATTENTION AUX EXCEPTIONS

Certaines activités, notamment pour les fournisseurs de services numériques, ont certaines obligations spécifiques.
Pour connaître les exceptions spécifiques, veuillez vous référer au lien suivant : monespacenis2.cyber.gouv.fr

Taille d'entité	Nombre d'employés	Chiffre d'affaires (M€)	Bilan annuel (M€)	Secteurs de l'annexe 1	Secteurs de l'annexe 2	Autres secteurs
Intermédiaire et grande	≥ 250	≥ 50	≥ 43	Entités essentielles	Entités importantes	Entités non concernées
Moyenne	≥ 50 et > 250	≥ 10 et > 50	≥ 10 et > 43	Entités importantes	Entités importantes	Entités non concernées
Micro et petite	< 50	< 10	< 10	Entités non concernées	Entités non concernées	Entités non concernées



ÉPISODE 3

QUELLES SONT LES OBLIGATIONS DES FUTURES 15 000 ENTITÉS CONCERNÉES PAR LA DIRECTIVE ?

Le champ d'application de la directive a été largement étendu à une estimation d'environ 15 000 entités en France contre moins d'un millier dans le cadre de la directive actuelle. Dans cet épisode, nous explorons les obligations imposées aux acteurs régulés.
Les obligations se renforcent tout en respectant le principe de proportionnalité avec des obligations différenciées entre les entités essentielles et les entités importantes.

Quelles sont les obligations pour les entités régulées ?

- S'auto-déclarer à l'ANSSI si son entité est concernée en tant que EE ou EI et de communiquer les informations de contacts ;
- Déclarer obligatoirement les incidents majeurs (*) à l'ANSSI, selon le même principe que pour le RGPD en cas de violation de données personnelles. L'entité doit faire une notification initiale dans les 24 heures puis mettre à jour sa notification initiale suivant les résultats des investigations réalisées ;
- Mettre en œuvre des mesures de sécurité différenciées si on est EE ou EI.

La définition de la notion d'incident majeur fait l'objet de discussions et sera certainement précisée dans les textes d'application de la loi. Dans la directive 2022/2555, un incident est défini comme « un événement compromettant la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données stockées, transmises ou faisant l'objet d'un traitement, ou des services que les réseaux et systèmes d'information offrent ou rendent accessibles ».

Quelles sont les mesures de sécurité à mettre en œuvre pour les entités régulées ?
De manière générale, les mesures à mettre en œuvre sont définies comme suit : mettre en place un pilotage de la sécurité de l'information adaptée, assurer la protection des réseaux et des systèmes d'information, mettre en place les processus et moyens pour assurer la défense des réseaux et systèmes d'information et gérer les incidents et garantir la résilience des activités.

Pour respecter le principe de proportionnalité, la différenciation des règles entre les entités importantes et essentielles devrait se concrétiser comme suit :

- Entités importantes : se conformer aux règles du guide d'hygiène de sécurité de l'ANSSI.
- Entités essentielles : se conformer à un système de règles de sécurité constituant un système de management de la sécurité de l'information complet proche de la norme ISO 27001:2022.

ÉPISODE 4

QUEL EST LE RÉGIME DE RÉGULATION ET DE SANCTION DES FUTURES 15 000 ENTITÉS CONCERNÉES PAR LA DIRECTIVE ?

Dans cet épisode, nous explorons le régime de régulation et de sanction de la directive NIS 2 en cas de non-conformité.

Nouveautés principales :
Du fait du changement d'échelle du périmètre régulé, l'initiative revient aux entités elles-mêmes, notamment pour s'auto-désigner vis-à-vis de l'autorité nationale. Le régime de régulation et de sanction est largement renforcé. Pour les sanctions, il s'aligne sur celui du RGPD : un montant d'amende qui peut théoriquement monter à 10 M€ ou 2 % du CA annuel mondial pour les entités essentielles (EE), et un peu moins pour les entités importantes (EI). Ce renforcement et les possibles sanctions associées rendent plus opérant la contrainte des exigences demandées aux entités régulées.

Les lignes directrices de l'ANSSI sur la mise en œuvre de la régulation ont été dévoilées :

- L'auto-déclaration, qui consiste à se faire connaître auprès de l'autorité via un formulaire, doit se faire rapidement après l'entrée en vigueur de la loi.
- La déclaration des incidents majeurs se fera via une procédure qui sera explicitée par l'ANSSI au moment de l'entrée en vigueur de la loi de transposition.
- Des délais de mise en conformité concernant la mise en œuvre effective des règles de sécurité seront accordés, avec un délai indicatif de 3 ans avant les premières sanctions.

Renforcement du rôle de l'autorité nationale :
L'ANSSI voit son rôle largement évolué avec un renforcement de son activité de contrôle. Elle pourra notamment effectuer des inspections sur place ou à distance, réaliser des scans automatisés et émettre des injonctions.

Par exemple :
Demander l'application d'un correctif de sécurité d'une vulnérabilité critique et possiblement demander la suspension temporaire d'exercer des responsabilités dirigeantes pour la personne physique exerçant des responsabilités dirigeantes à un niveau de directeur général ou de représentant légal.

Sanctions confiées à une commission indépendante : Le cadre du texte de transposition nationale propose de confier le rôle de sanction à une commission des sanctions distincte de l'ANSSI.

LES SECTEURS

ENTITÉS ESSENTIELLES (ANNEXE I)
Rôle vital pour le fonctionnement de la société et de l'économie :

Énergie :
- Production, transport et distribution d'électricité.
- Extraction et distribution de gaz et de pétrole.

Transports : Infrastructures et services ferroviaires, routiers, maritimes, et aériens.
Secteur bancaire et infrastructures des marchés financiers : Institutions financières critiques, infrastructures de paiement et de compensation.
Santé : Hôpitaux, cliniques, laboratoires médicaux, et autres prestataires de soins essentiels.
Eau potable et eaux usées : Réseaux d'approvisionnement en eau potable et de traitement des eaux usées.
Infrastructures numériques et TIC : Réseaux et centres de données, services de cloud, et infrastructures critiques des télécommunications.
Administration publique : Services publics essentiels aux citoyens (mairies, préfectures, organismes sociaux, etc.).
Secteur spatial : Exploitation et gestion des infrastructures spatiales essentielles (satellites, données spatiales).

Collectivités territoriales :
Les collectivités couvrant une population supérieure à **30 000 habitants** sont désignées entités essentielles dans le cadre du projet de loi présenté en conseil des ministres le 17 octobre 2024.

ENTITÉS IMPORTANTES (ANNEXE II)
Essentielles à la continuité des activités économiques et sociales :

Services postaux et d'expédition : Livraison de courriers, colis, et services logistiques.
Gestion des déchets : Collecte, traitement, et recyclage des déchets industriels et ménagers.
Industrie chimique : Fabrication, production, stockage, et distribution de produits chimiques.
Production alimentaire : Transformation, production, et distribution des denrées alimentaires essentielles.
Industries manufacturières : Secteurs liés à la production industrielle, tels que l'automobile, l'aéronautique, et l'électronique.
Fournisseurs de services numériques : Plateformes en ligne, services numériques, et entreprises technologiques.
Recherche : Laboratoires et instituts de recherche, en particulier ceux liés aux technologies critiques ou émergentes.

Pour plus d'informations détaillées, consultez : monespacenis2.cyber.gouv.fr