PRESENTATION DE LA DIRECTIVE NIS 2

Qu'est-ce que la directive NIS 2 ?

Une directive Européenne

La directive NIS 2 (Network and Information Security 2) a été adoptée le 14 décembre 2022 et publiée au Journal officiel de l'UE le 27 décembre 2022 sous la référence Directive (UE) 2022/2555.
A la différence d'un règlement UE qui s'applique directement et uniformément dans tous les États membres dès son entrée en vigueur, une directive UE fixe des objectifs à atteindre mais laisse aux États le choix des moyens et nécessite une transposition en droit national.

Transposition dans le droit national

Les États membres doivent avoir transposé la directive NIS 2 au plus tard le 17 octobre 2024, pour une mise en application le 18 octobre 2024. Certains Etats ont pris du retard, sans que cela ne remette pas en cause l'émergence d'un cadre européen harmonisé. En France, c'est l'ANSSI qui pilote la transposition en droit national de la directive et assure sa mise en œuvre.

Pour aller plus loin :

- Directive (UE) 2022/2555 : https://eurlex.europa.eu/eli/dir/2022/2555/
- Projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité (PRMD2412608L) : https://www.legifrance.gouv.fr/dossierlegislatif/JORFDOLE000050349138/

Quel sont les objectifs de NIS 2 ?

Dans la continuité de NIS 1

La première directive NIS visait à protéger les acteurs économiques majeurs de l'Union européenne. Cette nouvelle directive élargit le périmètre des entités concernées en ciblant 18 secteurs d'activités. Elle introduit des exigences plus adaptées, en particulier concernant la menace cyber.

Un renforcement sans précédent de la cybersécurité

NIS 2 renforce la cybersécurité dans l'Union européenne, homogénéise les règles entre pays, et élève le niveau global de protection face à la multiplication des cyberattaques. La directive vise notamment les collectivités, la sécurité des chaînes d'approvisionnement industrielles et la protection des infrastructures critiques européennes. Elle se réfère en grande partie à la méthodologie du standard ISO/IEC 27001.

L'accent mis sur la cybersécurité des équipements industriels

En particulier, cette directive fournit un cadre pour les infrastructures dites « industrielles », c'est-à-dire comportant des éléments OT (Operational Technology), ICS (Industrial Control Systems) et IoT (Internet of Things). En effet, la cybersécurité des machines et des objets connectés a longtemps été négligée et représente une vulnérabilité importante et mal maitrisée par la majorité des organisations. Par exemple, un automate programmable utilisé dans une ligne de production peut être exposé si le réseau n'est pas segmenté. NIS2 impose que cette exposition soit évaluée et documentée. NIS 2 remet ainsi la cybersécurité industrielle au cœur des préoccupations, en se référant principalement au standard IEC/ISA 62443.

En résumé

Thème	NIS1 (2016)	NIS2 (2022)
Périmètre	Acteurs majeurs	18 secteurs incluant PME et collectivités
Gouvernance	Moins contraignante	Implication obligatoire de la direction
Sanctions	Limitées	Jusqu'à 10 M€ ou 2 % CA mondial
OT/IoT	Peu abordé	Central avec IEC/ISA 62443

Pour aller plus loin

- Directive (EU) 2016/1148 (NIS 1) : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L1148
- Table d'équivalence de conformité publié par l'ENISA (NIS 2 / ISO 27001 / NIST etc.) : https://www.enisa.europa.eu/sites/default/files/2025-09/ENISA_Technical_Implementation_Guidance_Mapping_table_version_1.2.xlsx

Qu'est-ce qui change avec NIS 2 ?

Une approche systémique de la cybersécurité

La grande nouveauté avec NIS 2 est l'approche systémique de la cybersécurité. S'inspirant des référentiels ISO/IEC 27001 et IEC/ISA 62443, NIS 2 impose aux entités de mettre en place un cadre de gestion du risque qui s'apparente à un Système de Management de la Sécurité de l'Information (SMSI). Ce cadre exige une gestion du risque systématique, intégrée, évaluée périodiquement, mise à jour, et impliquant les parties prenantes tant internes qu'externes.

La gestion des fournisseurs

La gestion des fournisseurs devient un sujet primordial car la chaine d'approvisionnement (supply chain) est un vecteur majeur de vulnérabilité. Par exemple, du matériel électronique compromis introduit des vulnérabilités dans le produit assemblé par le fabricant. NIS 2 insiste donc tout particulièrement sur la gestion du risque de supply chain et exige notamment une évaluation du risque, des exigences cyber contractuelles, ainsi qu'un processus formalisé de suivi et d'audit.

Autres thématiques

Plusieurs autres thématiques font l'objet d'un traitement spécifique : gestion des incidents, gestion de crise, continuité d'activité, formation et sensibilisation des collaborateurs, contrôle d'accès, cryptographie, etc. NIS 2 révolutionne ainsi la gestion du risque cyber et exige que toutes les parties prenantes collaborent pour renforcer la cyber-résilience collective.

Pour aller plus loin

- Règlement d'exécution (UE) 2024-2690 https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=OJ:L_202402690
- Guide de l'ENISA sur les bonnes pratiques en matière de supply chain https://www.enisa.europa.eu/sites/default/files/publications/Good%20Practices%20for%20Supply%20Chain%20Cybersecurity.pdf

Qui est concerné par NIS 2 ?

Deux typologies d'entités

NIS 2 concerne aussi bien les collectivités territoriales, les administrations publiques, les PME et les grandes entreprises. Elle distingue deux catégories d'entités :

- **Entités essentielles** : Au moins 250 salariés ou un chiffre d'affaires annuel supérieur à 50 millions d'euros et un bilan annuel supérieur à 43 millions d'euros,

- **Entités importantes** : qui ne sont pas des entités essentielles et qui emploient au moins 50 salariés ou affichent un chiffre d'affaires et un bilan annuel supérieur à 10 millions d'euros.

Deux typologies de secteurs

En parallèle, NIS 2 identifie 18 secteurs segmentés en deux catégories :

- **Secteurs hautement critiques** : Administrations publiques, Eau potable, Eaux usées, Énergies, Espace, Gestion des services Technologies de l'Information et de la Communication (interentreprises), Infrastructures des marchés financiers, Infrastructures numériques, Santé, Secteur bancaire, Transports,

- **Autres secteurs critiques** : Fabrication, production et distribution de produits chimiques, Fournisseurs numériques, Gestion des déchets, Industrie manufacturière, Production, transformation et distribution de denrées alimentaires, Recherche, Services postaux et d'expédition.

Critères d'applicabilité

Ainsi, une entité satisfaisant aux critères ci-dessous est susceptible d'être concernée par NIS 2 :

- Plus de 50 salariés,
- Plus de 10 millions d'Euros de chiffre d'affaires,
- Intervenant sur l'un des 18 secteurs couverts par NIS 2.

Pour aller plus loin

- Test d'applicabilité de l'ANSSI : https://monespacenis2.cyber.gouv.fr/simulateur

Quelles sont les obligations principales pour les organisations industrielles ?

Examinons quelques exigences de NIS 2 qui, sans être exhaustives, donnent une indication sur le niveau de gestion de risque exigé.

Gouvernance

- Nomination d'un responsable cybersécurité (RSSI ou équivalent).
- Implication obligatoire de la direction générale dans la validation des politiques.
- Mise en place d'un cadre de gestion des risques s'apparentant à un SMSI tel que défini par ISO/IEC 27001.

Gestion des risques

- Inventaire des actifs (OT et IoT), cartographie réseau.
- Segmentation : séparer IT/OT, cloisonner zones sensibles.
- Patch management adapté aux environnements industriels.

Gestion de la supply-chain

- Politique de sécurité de la chaine d'approvisionnement (PSCA).
- Inclusion de clauses de cybersécurité dans les contrats.
- Evaluation et audits continus des fournisseurs critiques.

Détection et notification d'incidents

- Obligation de notifier tout incident majeur dans les 24 heures (notification préliminaire).
- Notification détaillée d'incident sous 72 heures.
- Rapport final attendu sous 1 mois.

Pour aller plus loin

- Guide méthodologique d'application de NIS 2 de l'ENISA : https://www.enisa.europa.eu/sites/default/files/2025-06/ENISA_Technical_implementation_guidance_on_cybersecurity_risk_management_measures_version_1.0.pdf

Quelles sont sanctions prévues par NIS 2 ?

En cas de manquement les pénalités prévues sont conséquentes :

Sanctions pour les entités essentielles

Pour les entités essentielles : amendes jusqu'à **10 millions d'Euros ou 2 %** du chiffre d'affaires annuel mondial (le montant le plus élevé étant retenu).

Sanctions pour les entités importantes

Pour les entités importantes : amendes jusqu'à **7 millions d'Euros ou 1,4 %** du chiffre d'affaires annuel mondial (le montant le plus élevé étant retenu).

Responsabilité des dirigeants

Responsabilité personnelle pour les Dirigeants : Nouveauté majeure, les administrateurs et dirigeants peuvent être sanctionnés directement (interdiction d'exercer, responsabilité civile ou pénale). Cette disposition élève la cybersécurité au rang d'enjeu stratégique pour les conseils d'administration.

Comment se préparer à l'application de NIS 2 ?

Pour bien se préparer à NIS 2, nous recommandons d'aborder le chantier comme une transformation à la fois technique, organisationnelle et managériale :

1. Se former et s'informer

Comprendre le texte et ses implications est indispensable. L'ANSSI recommande de consulter la documentation officielle, de suivre des formations ciblées et de sensibiliser la direction et les équipes clés.

2. Analyser de quelle manière NIS 2 va vous impacter

Etes-vous dans le périmètre d'applicabilité ? Etes-vous fournisseur d'entités essentielles ou importantes qui vont vous imposer des exigences en matière de cybersécurité ? Si vous êtes éligibles à NIS 2, vous devez vous enregistrer auprès de l'ANSSI.

3. Désigner un pilote

Nommer un responsable de projet NIS2. Cette personne (RSSI, DSI, directeur de la conformité…) coordonne la démarche, anime la gouvernance et veille à la documentation des mesures mises en place.

4. Évaluer son niveau de maturité

Réalisez un diagnostic initial de votre posture de cybersécurité. Cet état des lieux doit couvrir : la cartographie des actifs (OT/IoT inclus), la gestion des accès, les capacités de détection et de réponse, ainsi que la gouvernance.

5. Construire un plan d'action

À partir de ce diagnostic, définissez une feuille de route priorisée, incluant des mesures techniques (segmentation, patch management, détection d'incidents), organisationnelles (système de management, procédures de notification, continuité d'activité) et contractuelles (clauses avec les fournisseurs).

6. S'organiser pour la notification d'incidents

Construisez votre procédure de détection-réponse et de notification (préalerte, notification, rapport final) en tenant compte des délais imposés par la directive. C'est un élément qui exige des exercices pratiques et des preuves documentées.

7. Mettre en place des actions de sécurisation

Priorisez les actions à fort impact comme la réduction de la surface d'attaque, le contrôle des accès, les SLA et clauses fournisseurs. Mesurez votre maturité avec des KPI simples (MTTD/MTTR, taux de correctifs). Conservez un « journal de conformité » : ces preuves réduisent le risque réglementaire tout en rendant l'effort opérationnel maîtrisable.

Pour aller plus loin

- Guide ANSSI sur la cartographie du système d'information : https://cyber.gouv.fr/publications/cartographie-du-systeme-dinformation
- Guide ANSSI sur l'élaboration de tableaux de bord de sécurité des systèmes d'information : https://cyber.gouv.fr/publications/tdbssi-guide-delaboration-de-tableaux-de-bord-de-securite-des-systemes-dinformation

Checklist opérationnelle OT/IoT (10 actions clés)

1. Cartographier vos actifs OT/IoT.
2. Identifier vos services critiques.
3. Désigner un responsable cybersécurité.
4. Définir une politique de sécurité approuvée par la direction.
5. Mettre en place une segmentation réseau OT/IT.
6. Renforcer l'authentification et la gestion des accès.
7. Déployer des outils de détection d'incidents OT.
8. Formaliser une procédure de notification d'incidents.
9. Intégrer la sécurité dans vos contrats fournisseurs.
10. Former vos équipes opérationnelles.

Comment AKENATECH vous accompagne ?

Akenatech vous accompagne à chaque étape de votre mise en conformité NIS 2 :

Conseil

Gouvernance, gestion des risques, audit de conformité cyber, préparation de certification.

Intégration

Déploiement de solutions de cybersécurité adaptées aux environnements industriels : durcissement, segmentation, air-gap, protection d'endpoints, etc.

Services managés

RSSI à temps partagé, veille réglementaire et sécurité continue.

Basés à Lyon, nous intervenons partout en France et à l'international.

FAQ

Qui doit se conformer à NIS 2 ?

Toutes les entités essentielles et importantes listées dans les annexes de la directive (ex. énergie, santé, transport, agroalimentaire).

Quels sont les délais de notification d'un incident ?

Notification initiale sous 24 h, rapport intermédiaire sous 72 h, rapport final sous 1 mois.

NIS 2 s'applique-t-elle aux PME ?

Seules les entités dépassant certains seuils (50 salariés / 10 M€ de CA) sont concernées, sauf exceptions pour secteurs critiques.

Quelle différence entre NIS1 et NIS 2 ?

NIS 2 élargit les secteurs, augmente les obligations de gouvernance et renforce les sanctions.

Pour aller plus loin

- FAQ de la Commission Européenne sur la Directive NIS 2 : https://digital-strategy.ec.europa.eu/fr/faqs/directive-measures-high-common-level-cybersecurity-across-union-nis2-directive-faqs

Conclusion

La mise en conformité NIS 2 est obligatoire depuis octobre 2024 pour de nombreuses organisations industrielles. Il ne s'agit pas d'une formalité administrative, mais d'une transformation en profondeur de la gouvernance OT/IoT.

Akenatech vous aide à passer de la théorie à la pratique grâce à nos experts, à nos outils de sécurisation et à nos services managés.

👉 Contactez-nous pour un état des lieux dès aujourd'hui.