CONFÉDÉRATION DES PME

10 novembre 2023

Résumé - Directive NIS 2

OBJECTIF DE LA DIRECTIVE

La directive NIS 1, entrée en vigueur en août 2016, a été le premier véritable effort législatif à l'échelle de l'Union européenne pour renforcer la cybersécurité au sein des États membres. L'objectif principal était d'améliorer la sécurité des réseaux et des systèmes d'information en établissant un cadre législatif commun. Deux catégories d'acteurs sont ciblés par cette directive : les opérateurs de services essentiels (acteurs des secteurs de l'énergie, des transports, de la santé, de l'eau et des services financiers, etc.) et les fournisseurs de services numériques (moteurs de recherche, plateformes de vente en ligne, etc.).

Pour faire face à la menace croissante des cyberattaques, qui touche de plus en plus les TPE - PME, il a été décidé, par la Commission européenne, d'étendre le périmètre et les ambitions de la directive et ainsi de passer d'une politique de cybersécurité des opérateurs critiques à une politique de cybersécurité de masse.

C'est dans cet objectif que la directive NIS 1 est révisée pour devenir la directive NIS 2.

PERIMETRE DE LA DIRECTIVE

Les secteurs concernés par la directive NIS 2 sont ceux présents dans les annexes 1 et 2 (voir pp. 5 à 8).

Parmi ces secteurs, une entreprise sera concernée par la directive si elle est considérée comme une entité essentielle ou une entité importante.

Quelles sont les entités essentielles ?

- Ensemble des entités de taille intermédiaire et grande de l'annexe 1

Quelles sont les entités importantes ?

- Ensemble des entités de taille moyenne de l'annexe 1
- Ensemble des entités de taille moyenne, intermédiaire et grande de l'annexe 2

Rappel :

> Une entreprise de taille intermédiaire ou grande est une entreprise qui vérifie au moins une des deux conditions suivantes :
>
> - avoir au moins 250 salariés,
> - avoir au moins 50 millions d'euros de chiffre d'affaires ou un bilan annuel au moins égal à 43 millions d'euros.
>
> Une entreprise de taille moyenne est une entreprise qui vérifie au moins une des deux conditions suivantes :
>
> - avoir entre 50 et 249 salariés,
> - avoir un chiffre d'affaires compris entre 10 et 50 millions d'euros ou un bilan annuel compris entre 10 et 43 millions d'euros.

Sont également considérées comme entités essentielles, et donc concernées par la directive NIS 2 :

- les prestataires de services de confiance qualifiés, les registres de noms de domaine de premier niveau et les fournisseurs de services DNS, quelle que soit leur taille,
- les fournisseurs de réseaux publics de communication électroniques publics ou de services de communications électroniques accessibles au public qui constituent des entreprises de taille moyenne,
- les entités soumises à la directive Résilience des Entités Critiques (REC),
- les entités désignées Opérateur de Service Essentiel au titre de la NIS 1.

Quelles différences entre entités essentielles et entités importantes ?

La directive NIS 2 intègre une proportionnalité entre entités essentielles et entités importantes, à la fois en termes de :

- **mesures de sécurité** : différents niveaux d'exigence seront envisagés, notamment pour prendre en considération les moyens humains et financiers d'une grande entreprises et ceux d'une PME.
- **régulation** : pour les entités essentielles, les contrôles de l'ANSSI pourront se dérouler ex-ante, c'est-à-dire faire l'objet d'une surveillance en l'absence d'incidents de sécurité ; pour les entités importantes, les contrôles se dérouleront uniquement ex-post, c'est-à-dire en cas de connaissance d'une non-conformité.
- **sanction** : différence du montant de sanction selon la nature de l'entité (voir Sanctions, p. 3).

OBLIGATIONS

Les obligations pour les entités sont les suivantes :

- Une obligation d'information :
    - Se notifier auprès de l'ANSSI et communiquer des informations de contact (nom, adresse et coordonnées, secteurs d'activité, liste des Etats membres de l'UE dans lesquels sont fournis les services)

- Rapporter à l'ANSSI les incidents importants[1]. La déclaration se déroulera en plusieurs étapes :
  - une notification au maximum 24 heures après connaissance de l'incident,
  - un rapport d'incident au maximum 72 heures suivant l'incident,
  - un rapport final au maximum un mois suivant l'incident.

- Une application des mesures de sécurité :

  Ces mesures sont les suivantes :

  - les politiques relatives à l'analyse des risques et à la sécurité des systèmes d'information,
  - la gestion des incidents,
  - la continuité des activités (sauvegardes, plan de reprise d'activité gestion des crises),
  - la sécurité de la chaine d'approvisionnement (fournisseurs / prestataires),
  - la sécurité de l'acquisition, du développement et de la maintenance des systèmes d'information,
  - des politiques et des procédures pour évaluer l'efficacité des mesures de gestion des risques en matière de cybersécurité,
  - les pratiques de base (cyberhygiène et formation à la cybersécurité),
  - des politiques et des procédures relatives à l'utilisation de la cryptographie,
  - 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 continue), d'outils de communication sécurisés et de systèmes de communication d'urgence en cas de crise.

SANCTIONS

L'ANSSI, autorité nationale en matière de cybersécurité, disposera d'un pouvoir de surveillance. Elle pourra à ce titre émettre des avertissements à l'encontre des entités contrôlées qui ne respectent pas la directive.

Elle pourra notamment ordonner aux entités concernées, qu'elles soient essentielles ou importantes, de :

- mettre en œuvre les recommandations formulées à la suite d'un audit de sécurité dans un délai raisonnable,
- informer les personnes physiques ou morales à l'égard desquelles elles fournissent des services ou exercent des activités susceptibles d'être affectées par une cybermenace importante et de la nature de la menace, ainsi que de toutes mesures préventives ou réparatrices que ces personnes physiques ou morales pourraient prendre en réponse à cette menace,
- rendre publics les aspects de violation de la directive de manière spécifique.

La directive NIS 2 prévoit par ailleurs la possibilité pour les autorités nationales de prononcer des amendes administratives à l'encontre des entités qui ne respectent pas la directive. Le plafond des amendes, qui reste à déterminer, sera a minima de :

---

[1] La directive considère un incident comme important si :

- Il a causé ou est susceptible de causer une perturbation opérationnelle grave des services ou des pertes financières pour l'entité concernée,
- Il a affecté ou est susceptible d'affecter d'autres personnes physiques ou morales en causant des dommages matériels, corporels ou moraux considérables.

- 10 millions d’euros ou 2 % du chiffre d’affaires annuel mondial pour les entités essentielles.
- 7 millions d’euros ou 1,4 % du chiffre d’affaires annuel mondial pour les entités importantes.

ANNEXE 1 : SECTEURS HAUTEMENT CRITIQUES

Secteur	Sous-secteur	Type d'entité
1. Énergie	a) Électricité	Entreprises d'électricité au sens de l'article 2, point 57), de la directive (UE) 2019/944 du Parlement européen et du Conseil, qui remplissent la fonction de « fourniture » au sens de l'article 2, point 12), de ladite directive
		Gestionnaires de réseau de distribution au sens de l'article 2, point 29), de la directive (UE) 2019/944
		Entreprises d'électricité au sens de l'article 2, point 57), de la directive (UE) 2019/944 du Parlement européen et du Conseil, quiremplissent la fonction de «fourniture» au sens de l'article 2, point 12), de ladite directive
		Gestionnaires de réseau de distribution au sens de l'article 2, point 29), de la directive (UE) 2019/944
		Gestionnaires de réseau de transport au sens de l'article 2, point 35), de la directive (UE) 2019/944
		Producteurs au sens de l'article 2, point 38), de la directive (UE) 2019/944
		Opérateurs désignés du marché de l'électricité au sens de l'article 2, point 8), du règlement (UE) 2019/943 du Parlement européen et du Conseil
		Acteurs du marché au sens de l'article 2, point 25), du règlement (UE) 2019/943 fournissant des services d'agrégation, de participationactive de la demande ou de stockage d'énergie au sens de l'article 2, points 18), 20) et 59), de la directive (UE) 2019/944
		Exploitants d'un point de recharge qui sont responsables de la gestion et de l'exploitation d'un point de recharge, lequel fournit un service de recharge aux utilisateurs finals, y compris au nom et pour le compte d'un prestataire de services de mobilité
	b) Réseaux de chaleur et de froid	Opérateurs de réseaux de chaleur ou de réseaux de froid au sens de l'article 2, point 19), de la directive (UE) 2018/2001 du Parlement et du Conseil
	c) Pétrole	Exploitants d'oléoducs
		Exploitants d'installations de production, de raffinage, de traitement, de stockage et de transport de pétrole
		Entités centrales de stockage au sens de l'article 2, point f), de la directive 2009/119/CE du Conseil
	d) Gaz	Entreprises de fourniture au sens de l'article 2, point 8, de la directive 2009/73/CE du Parlement européen et du Conseil
		Gestionnaires de réseau de distribution au sens de l'article 2, point 6, de la directive 2009/73/CE
		Gestionnaires de réseau de transport au sens de l'article 2, point 4, de la directive 2009/73/CE
		Gestionnaires d'installation de stockage au sens de l'article 2, point 10, de la directive 2009/73/CE
		Gestionnaires d'installation de GNL au sens de l'article 2, point 12, de la directive 2009/73/CE
		Entreprises de gaz naturel au sens de l'article 2, point 1, de la directive 2009/73/CE
		Exploitants d'installations de raffinage et de traitement de gaz naturel
	e) Hydrogène	Exploitants de systèmes de production, de stockage et de transport d'hydrogène
2. Transports	a) Transports aériens	Transporteurs aériens au sens de l'article 3, point 4), du règlement (CE) n° 300/2008 utilisés à des fins commerciales
		Entités gestionnaires d'aéroports au sens de l'article 2, point 2), de la directive 2009/12/CE du Parlement européen et du Conseil, aéroports au sens de l'article 2, point 1), de ladite directive, y compris les aéroports du réseau central énumérés à l'annexe II, section 2,du règlement (UE) n° 1315/2013 du Parlement européen et du Conseil, et entités exploitant les installations annexes se trouvant dans les aéroports
		Services du contrôle de la circulation aérienne au sens de l'article 2, point 1), du règlement (CE) n° 549/2004 du Parlement européen etdu Conseil

Secteur	Sous-secteur	Type d'entité
	b) Transports ferroviaires	Gestionnaires de l'infrastructure au sens de l'article 3, point 2), de la directive 2012/34/UE du Parlement européen et du Conseil
		Entreprises ferroviaires au sens de l'article 3, point 1), de la directive 2012/34/UE, y compris les exploitants d'installation de service ausens de l'article 3, point 12), de ladite directive
	c) Transports par eau	Sociétés de transport par voie d'eau intérieure, maritime et côtier de passagers et de fret, telles qu'elles sont définies pour le domaine du transport maritime à l'annexe I du règlement (CE) n° 725/2004 du Parlement européen et du Conseil, à l'exclusion des navires exploités à titre individuel par ces sociétés
		Entités gestionnaires des ports au sens de l'article 3, point 1), de la directive 2005/65/CE du Parlement européen et du Conseil, y compris les installations portuaires au sens de l'article 2, point 11), du règlement (CE) n° 725/2004, ainsi que les entités exploitant des infrastructures et des équipements à l'intérieur des ports
		Exploitants de services de trafic maritime (STM) au sens de l'article 3, point o), de la directive 2002/59/CE du Parlement européen et du Conseil
	d) Transports routiers	Autorités routières au sens de l'article 2, point 12), du règlement délégué (UE) 2015/962 de la Commission chargées du contrôle de la gestion de la circulation, à l'exclusion des entités publiques pour lesquelles la gestion de la circulation ou l'exploitation de systèmes de transport intelligents constituent une partie non essentielle de leur activité générale
		Exploitants de systèmes de transport intelligents au sens de l'article 4, point 1), de la directive 2010/40/UE du Parlement européen et du Conseil
3. Secteur bancaire		Établissements de crédit au sens de l'article 4, point 1), du règlement (UE) n° 575/2013 du Parlement européen et du Conseil
4. Infrastructures des marchés financiers		Exploitants de plates-formes de négociation au sens de l'article 4, point 24), de la directive 2014/65/UE du Parlement européen et du Conseil
		Contreparties centrales au sens de l'article 2, point 1), du règlement (UE) n° 648/2012 du Parlement européen et du Conseil
5. Santé		Prestataires de soins de santé au sens de l'article 3, point g), de la directive 2011/24/UE du Parlement européen et du Conseil
		Laboratoires de référence de l'Union européenne visés à l'article 15 du règlement (UE) 2022/2371 du Parlement européen et du Conseil
		Entités exerçant des activités de recherche et de développement dans le domaine des médicaments au sens de l'article 1er, point 2, de la directive 2001/83/CE du Parlement européen et du Conseil
		Entités fabriquant des produits pharmaceutiques de base et des préparations pharmaceutiques au sens de la NACE Rév. 2, section C, division 21
		Entités fabriquant des dispositifs médicaux considérés comme critiques en cas d'urgence de santé publique (liste des dispositifs médicaux critiques en cas d'urgence de santé publique) au sens de l'article 22 du règlement (UE) 2022/123 du Parlement européen et du Conseil
6. Eau potable		Fournisseurs et distributeurs d'eaux destinées à la consommation humaine au sens de l'article 2, point 1) a), de la directive (UE) 2020/2184 du Parlement européen et du Conseil (22), à l'exclusion des distributeurs pour lesquels la distribution d'eaux destinées à la consommation humaine constitue une partie non essentielle de leur activité générale de distribution d'autres produits et biens
7. Eaux usées		Entreprises collectant, évacuant ou traitant les eaux urbaines résiduaires, les eaux ménagères usées ou les eaux industrielles usées au sens de l'article 2, points 1), 2) et 3), de la directive 91/271/CEE du Conseil, à l'exclusion des entreprises pour lesquelles la collecte, l'évacuation ou le traitement des eaux urbaines résiduaires, des eaux ménagères usées ou des eaux industrielles usées constituent une partie non essentielle de leur activité générale
8. Infrastructure numérique		Fournisseurs de points d'échange internet
		Fournisseurs de services DNS, à l'exclusion des opérateurs de serveurs racines de noms de domaine
		Registres de noms de domaine de premier niveau
		Fournisseurs de services d'informatique en nuage
		Fournisseurs de services de centres de données
		Fournisseurs de réseaux de diffusion de contenu

Secteur	Sous-secteur	Type d'entité
		Prestataires de services de confiance
		Fournisseurs de réseaux de communications électroniques publics
9. Gestion des services TIC		Fournisseurs de services gérés
		Fournisseurs de services de sécurité gérés
10. Administration publique		Entités de l'administration publique des pouvoirs publics centraux définies comme telles par un État membre conformément au droitnational
		Entités de l'administration publique au niveau régional définies comme telles par un État membre conformément au droit national
11. Espace		Exploitants d'infrastructures terrestres, détenues, gérées et exploitées par des États membres ou par des parties privées, qui soutiennent lafourniture de services spatiaux, à l'exclusion des fournisseurs de réseaux de communications électroniques publics

ANNEXE 2 : AUTRES SECTEURS CRITIQUES

Secteur	Sous-secteur	Type d'entité
1. Services postaux et d'expédition		Prestataires de services postaux au sens de l'article 2, point 1 bis), de la directive 97/67/CE, y compris les prestataires de services d'expédition
2. Gestion des déchets		Entreprises exécutant des opérations de gestion des déchets au sens de l'article 3, point 9), de la directive 2008/98/CE du Parlement européen et du Conseil, à l'exclusion des entreprises pour lesquelles la gestion des déchets n'est pas la principale activité économique
3. Fabrication, production et distribution de produits chimiques		Entreprises procédant à la fabrication de substances et à la distribution de substances ou de mélanges au sens de l'article 3, points 9 et 14, du règlement (CE) n° 1907/2006 du Parlement européen et du Conseil et entreprises procédant à la production d'articles au sens de l'article 3, point 3), dudit règlement, à partir de substances ou de mélanges
4. Production, transformation et distribution des denrées alimentaires		Entreprises du secteur alimentaire au sens de l'article 3, point 2), du règlement (CE) n° 178/2002 du Parlement européen et du Conseil (3) qui exercent des activités de distribution en gros ainsi que de production et de transformation industrielles
5. Fabrication	a) Fabrication de dispositifs médicaux et de dispositifs médicaux de diagnostic in vitro	Entités fabriquant des dispositifs médicaux au sens de l'article 2, point 1), du règlement (UE) 2017/745 du Parlement européen et du Conseil (4) et entités fabriquant des dispositifs médicaux de diagnostic in vitro au sens de l'article 2, point 2), du règlement (UE) 2017/746 du Parlement européen et du **Conseil, à l'exception des entités fabriquant des dispositifs médicaux mentionnés à l'annexe I, point 5, cinquième tiret, de la présente directive**
	b) Fabrication de produits informatiques, électroniques et optiques	Entreprises exerçant l'une des activités économiques visées dans la NACE Rév. 2, section C, division 26
	c) Fabrication d'équipements électriques	Entreprises exerçant l'une des activités économiques visées dans la NACE Rév. 2, section C, division 27
	d) Fabrication de machines et équipements n.c.a.	Entreprises exerçant l'une des activités économiques visées dans la NACE Rév. 2, section C, division 28
	e) Construction de véhicules automobiles, remorques et semi-remorques	Entreprises exerçant l'une des activités économiques visées dans la NACE Rév. 2, section C, division 29
	f) Fabrication d'autres matériels de trans- port	Entreprises exerçant l'une des activités économiques visées dans la NACE Rév. 2, section C, division 30
6. Fournisseurs numériques		Fournisseurs de places de marché en ligne
		Fournisseurs de moteurs de recherche en ligne
		Fournisseurs de plateformes de services de réseaux sociaux
7. Recherche		Organismes de recherche