CONFÉDÉRATION DES PME

26 avril 2024

Position - Directive NIS 2

OBJECTIF DE LA DIRECTIVE

La directive NIS 1, entrée en vigueur en août 2016, a été le premier effort législatif à l'échelle de l'UE pour renforcer la cybersécurité au sein des États membres. L'objectif principal était d'améliorer la sécurité des réseaux et des systèmes d'information via l'établissement d'un cadre législatif commun.

Pour faire face à la menace croissante des cyberattaques, qui touchent de plus en plus les TPE - PME, la Commission européenne a décidé 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. Si la directive a été adoptée dans le but louable de renforcer la cybersécurité au sein de l'Union européenne, l'examen des implications pour les moyennes entreprises met en évidence les défis potentiels que la mise en œuvre de la directive NIS pourrait poser.

LES POINTS A CONNAITRE DE LA DIRECTIVE

Seraient concernées par la directive :

- les entreprises de taille intermédiaire (ETI) et grandes entreprises (GE) de 18 secteurs (annexes 1 et 2[1])
- les entreprises moyennes de 11 secteurs (annexe 1)

Cela représente, selon les estimations, entre 10 000 et 15 000 entreprises.

Les obligations pour les entités seront :

- le partage d'informations : se notifier auprès de l'ANSSI comme entrant dans le champ des entreprises concernées et communiquer les informations de contact,
- l'application de mesures de sécurité contre les risques cyber : gestion des risques, mise en place de mesures adaptées (sécurité de la chaine d'approvisionnement, des ressources humaines, des politiques de contrôle d'accès et de la gestion des actifs, etc.),
- la déclaration des incidents.

[1] Voir pages 4 à 7.

L'ANSSI disposera d'un pouvoir de surveillance. Elle pourra émettre des avertissements à l'encontre des entités contrôlées qui ne respectent pas la directive et prononcer des amendes (jusqu'à 10 millions d'euros ou 2 % du chiffre d'affaires mondial des entités).

PROBLEMES POTENTIELS

Les problèmes pour les moyennes entreprises sont de plusieurs ordres :

- **Complexité et coûts :** Les PME ont souvent des ressources limitées en termes de budgets et de personnel dédié à la cybersécurité. La conformité à la directive NIS 2 pourrait entraîner des coûts substantiels liés à la mise en œuvre de mesures de sécurité spécifiques, ainsi qu'à la formation du personnel et à la conformité réglementaire. Entre les coûts de mise en conformité la première année et les dépenses récurrentes les années suivantes, l'impact financier sera substantiel pour les PME.

- **Exigences de notification** : La directive impose aux entreprises de signaler sans délai les incidents de sécurité majeurs aux autorités compétentes, ainsi qu'aux destinataires de leurs services. Ce délai accroît la charge administrative des PME, qui pourraient ne pas disposer des ressources nécessaires pour répondre aux exigences de notification dans des délais stricts, et ralentirait les équipes chargées du redémarrage de l'activité de l'entreprise suite à la cyberattaque. Un délai de 3 jours, comme l'exige la loi LOPMI, serait plus conforme à la réalité des entreprises.

- **Conformité technique** : La directive NIS exige que les entreprises mettent en place des mesures de sécurité techniques spécifiques pour protéger leurs réseaux et systèmes d'information. Cela peut poser un défi particulier pour les PME qui pourraient manquer d'une expertise technique interne nécessaire pour mettre en œuvre ces mesures de manière efficace.

- **Dépendance aux fournisseurs certifiés** : Les entreprises concernées par la directive doivent se prévaloir de fournisseurs ou de prestataires certifiés pour certains produits ou services liés à la cybersécurité. Cela peut entraîner une dépendance aux fournisseurs certifiés et aussi limiter la flexibilité des entreprises pour choisir des solutions qui répondent le mieux à leurs besoins spécifiques. De plus, il sera difficile pour les PME de trouver des experts externes au regard du nombre d'entreprises concernées par la directive et du faible nombre d'experts (200 entreprises labellisées Expert cyber, qui sont par ailleurs inégalement réparties sur le territoire. Un effort des pouvoirs publics doit permettre d'augmenter sensiblement le nombre de fournisseurs certifiés.

- **Partage d'informations sensibles** : Le partage d'informations entre l'ANSSI et d'autres entités, y compris des organismes internationaux ou des Etats tiers, posent un problème de confidentialité et de protection des données pour les PME. Bien que la coopération soit importante pour contrer les menaces, les entreprises pourraient craindre une fuite de leurs informations sensibles, ce qui pourrait avoir des répercussions négatives sur leur activité.

- **Dépendance à l'égard des fournisseurs tiers :** Les entreprises qui dépendent de fournisseurs tiers pour des services informatiques ou de cybersécurité peuvent être confrontées à des défis supplémentaires pour s'assurer que ces fournisseurs respectent les exigences de la loi, ce qui pourrait augmenter la complexité et les risques.

RECOMMANDATIONS

Pour répondre aux problèmes potentiels, la CPME demande :

- **de ne pas surtransposer la directive** : La CPME reconnait l'importance la nécessité pour les PME d'avoir une bonne sécurité contre les cyberattaques. Elle estime toutefois qu'il n'est pas utile que la réglementation aille au-delà de ce qui est notifié dans la directive, car les obligations sont déjà suffisamment complexes et lourdes à mettre en œuvre pour les PME. Pour exemple, le projet de loi prévoit une interdiction pour tout dirigeant d'exercer ses responsabilités en cas de manquement alors que la directive n'évoque cette possibilité qu'en derniers recours.

- **une assistance technique et financière** : La mise en place de programmes d'assistance technique conçus spécifiquement pour aider les PME à se conformer à la directive NIS est vitale, notamment en fournissant un soutien pour la formation, la sensibilisation et la mise en œuvre des mesures de sécurité (ex : FAQ). Au regard du coût que cela va engendrer, un soutien financier est, de plus, nécessaire, sans quoi, les entreprises n'auront pas les ressources pour se protéger.

- **une flexibilité, une proportionnalité et un cadencement de la mise en œuvre de la réforme** : La CPME demande à ce que les autorités compétentes adoptent une approche flexible et proportionnée lors de l'application de la directive aux PME, en tenant compte de leurs ressources et de leur taille. Du fait qu'il sera difficile pour les PME de recourir rapidement à une expertise technique, il serait inconcevable que ces entreprises soient sanctionnées dans les mois qui suivront la transposition de la directive. A l'instar de ce qui a été opéré pour le RGPD, un délai de 3 ans est jugé utile et nécessaire. Les entreprises, en particulier les PME, attendent des autorités compétentes un accompagnement (ex : mise en place de programmes de sensibilisation et de formation) plutôt qu'une action répressive.

- **une priorisation des risques :** Tous les risques de cyberattaques ne sont pas égaux en termes de fréquence et de gravité. Les autorités compétentes doivent identifier et prioriser les types d'attaques les plus courantes et les plus préjudiciables pour les PME. Pour ce faire, des données et des analyses sur les tendances des cyberattaques peuvent être utilisées pour déterminer les menaces les plus pertinentes, pour enfin fournir aux PME des conseils et des directives spécifiques pour se protéger contre ces types d'attaques.

- **une étude d'impact** : Aucune étude d'impact n'a, à ce stade, été réalisée alors que le coût pour les PME devrait être astronomique (plusieurs dizaines, voire centaines de milliers d'euros pour une entreprise de 50 salariés pour se mettre en conformité).

POINT D'ATTENTION

- Le projet de loi ne donne pas les détails de la réglementation (ex : secteurs concernés). Il sera en effet complété par décrets. Il est important que la CPME soit associée à en amont à l'élaboration de ces décrets, notamment pour connaitre le champ d'application de la réglementation.

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