Directive NIS 2 : Renforcement de la Cybersécurité en UE

Fiche pratique publié le **29/11/2023**, vu **584 fois**, Auteur : Blog de Le Bouard Avocats Versailles

Explorez la directive NIS 2, ses impacts sur la cybersécurité, obligations des entités, rôle de l'ANSSI et préparation à la conformité en UE.

I. Introduction à la Directive NIS 2

Contexte et objectifs de la directive NIS 2

La Directive NIS 2, successeur de la première Directive sur la sécurité des réseaux et des systèmes d'information (NIS), représente un jalon crucial dans le renforcement de la cybersécurité au sein de l'Union européenne. Son objectif principal est d'améliorer la résilience et la sécurité des réseaux et systèmes d'information essentiels dans l'UE. Cette directive vise à établir un niveau élevé et commun de sécurité pour les réseaux et les systèmes d'information à travers les États membres, en réponse à l'évolution rapide des menaces cybernétiques.

Date de publication et délai de transposition par les États membres

La Directive NIS 2 a été publiée au Journal officiel de l'Union européenne le 27 décembre 2022. Les États membres de l'UE sont tenus de transposer cette directive dans leur législation nationale d'ici le 17 octobre 2024. Ce délai de transposition est crucial pour assurer une mise en œuvre harmonisée et efficace de la directive, permettant ainsi une meilleure protection contre les cyberattaques et renforçant la coopération entre les États membres dans le domaine de la cybersécurité.

II. Champ d'Application et Nouveaux Secteurs Concernés

A. Critères d'application de la directive NIS 2

La directive NIS 2 (Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022) constitue une avancée significative dans le renforcement de la sécurité des réseaux et des systèmes d'information au sein de l'Union européenne. Cette directive vient abroger et remplacer la directive NIS 1 (Directive (UE) 2016/1148) et élargit considérablement son champ d'application.

Les critères d'application de la NIS 2 sont plus étendus et détaillés que ceux de son prédécesseur. Premièrement, la directive s'applique à toutes les entités de taille moyenne et grande, contrairement à la NIS 1 qui se concentrait principalement sur les opérateurs de services essentiels et les fournisseurs de services numériques. De plus, la NIS 2 introduit des critères

spécifiques pour déterminer l'importance systémique des entités, en se basant sur des facteurs tels que la fourniture de services essentiels, l'impact sur l'économie et la société, et la dépendance d'autres secteurs à leurs services.

B. Présentation des nouveaux secteurs d'activité visés

La directive NIS 2 élargit de manière significative le nombre de secteurs d'activité concernés. Outre les secteurs déjà couverts par la NIS 1, tels que l'énergie, les transports, la santé et les services financiers, la NIS 2 englobe désormais des secteurs tels que les administrations publiques, les services postaux, la gestion des déchets, la fabrication de produits pharmaceutiques, et les entreprises du secteur de l'espace. Cette extension reflète la prise de conscience de l'importance croissante de la cybersécurité dans tous les aspects de l'économie et de la société.

C. Comparaison avec la directive NIS 1

En comparant la directive NIS 2 avec la NIS 1, plusieurs différences majeures sont à souligner. Premièrement, la NIS 2 impose des obligations plus strictes en matière de gestion des risques et de déclaration des incidents. Elle exige également des États membres qu'ils établissent des cadres de sanctions pour les non-conformités, renforçant ainsi l'aspect coercitif de la réglementation.

De plus, la NIS 2 introduit des dispositions spécifiques pour les groupes d'entreprises, exigeant une approche cohérente de la cybersécurité à travers toutes leurs filiales dans l'UE. Elle met également l'accent sur l'importance de la coopération internationale en matière de cybersécurité, en reconnaissant que les menaces numériques ne connaissent pas de frontières.

La directive NIS 2 marque une étape importante dans l'évolution de la législation européenne en matière de cybersécurité. En élargissant son champ d'application et en renforçant les obligations des entités concernées, elle vise à établir un niveau de sécurité plus élevé et plus uniforme dans l'ensemble de l'Union européenne.

III. Identification des Entités Essentielles et Importantes

A. Définition des Entités Essentielles et Importantes

Dans le cadre de la directive NIS 2, l'identification des entités joue un rôle crucial. Cette directive, qui vise à renforcer la sécurité des réseaux et des systèmes d'information au sein de l'Union européenne, distingue deux catégories d'entités : les entités essentielles et les entités importantes.

Les entités essentielles, selon l'article 3, paragraphe 2, de la directive NIS 2, sont celles qui fournissent des services indispensables au maintien de fonctions sociétales ou économiques critiques. Ces entités incluent, mais ne se limitent pas à, les secteurs de l'énergie, des transports, de la santé et des services financiers. La perturbation ou l'indisponibilité de leurs services pourrait avoir un impact significatif sur la sécurité nationale, la santé publique ou la sécurité économique.

D'autre part, les entités importantes, définies dans l'article 3, paragraphe 3, de la même directive, sont celles dont les services ne sont pas considérés comme essentiels au même degré, mais dont l'interruption pourrait néanmoins causer un impact considérable. Ces entités peuvent appartenir à

un éventail plus large de secteurs, y compris les administrations publiques et certains services numériques.

B. Critères pour Déterminer l'Applicabilité de la Directive aux Différentes Entités

Pour déterminer si une entité relève de la catégorie des entités essentielles ou importantes, plusieurs critères sont pris en compte. Ces critères sont énoncés dans les articles 4 et 5 de la directive NIS 2.

- **Taille de l'Entité :** La directive s'applique aux entités de taille moyenne et grande, excluant ainsi les petites et micro-entreprises, conformément à la définition donnée par la Commission européenne.
- **Nature et Importance des Services Fournis :** Les services fournis par l'entité doivent être essentiels pour le maintien de fonctions sociétales ou économiques critiques. Cela inclut l'évaluation de l'impact potentiel d'une interruption de service.
- **Impact sur la Sécurité Publique, la Santé ou la Sécurité Économique :** Pour les entités essentielles, il est crucial d'évaluer si leur incapacité à fournir des services pourrait compromettre la sécurité nationale, la santé publique ou la stabilité économique.
- **Dépendance d'Autres Secteurs :** L'interdépendance avec d'autres secteurs est également un critère important. Si d'autres secteurs critiques dépendent fortement des services fournis par une entité, cela peut justifier son classement comme entité essentielle.
- **Risque et Exposition aux Menaces :** L'évaluation des risques et de la vulnérabilité aux menaces cybernétiques est un autre critère déterminant pour l'application de la directive.

La directive NIS 2 établit un cadre clair pour l'identification des entités essentielles et importantes, en se basant sur des critères précis et mesurables. Cette approche permet une application cohérente et efficace de la directive, en veillant à ce que les entités les plus critiques pour la société et l'économie européennes soient adéquatement protégées contre les risques cybernétiques.

Dans le cadre de la directive NIS 2, les entités essentielles et importantes sont tenues de mettre en œuvre un ensemble de mesures de cybersécurité. Ces mesures, détaillées dans les articles 20 et 21 de la directive, visent à garantir un niveau de sécurité adéquat face aux risques cybernétiques. Parmi ces mesures, on retrouve :

- Les entités doivent établir et maintenir des systèmes de gestion des risques pour prévenir et minimiser l'impact des incidents de sécurité.
- Cela inclut le contrôle d'accès, la sécurisation des réseaux, la protection des données, et la mise en place de procédures de réponse aux incidents.
- Les entités sont tenues de notifier rapidement les incidents de sécurité aux autorités compétentes.

- Les plans de continuité d'activité doivent être élaborés pour assurer la résilience des services en cas d'incident.
- Des évaluations régulières des risques et des tests de sécurité (par exemple, des audits et des tests de pénétration) sont requis pour identifier et corriger les vulnérabilités.

La directive NIS 2 introduit une obligation d'accountability, obligeant les entités à démontrer activement leur conformité avec les exigences de la directive. Selon l'article 23, les entités doivent tenir à jour une documentation complète sur les mesures de sécurité mises en place, les évaluations des risques effectuées, et les incidents survenus. Cette documentation doit être disponible pour les autorités compétentes, facilitant ainsi les contrôles et les audits.

Un aspect crucial de la directive NIS 2 est l'accent mis sur la formation et la sensibilisation des organes de direction en matière de cybersécurité. L'article 22 stipule que les membres de la direction doivent recevoir une formation adéquate pour comprendre et gérer les risques cybernétiques. Cette formation doit couvrir les aspects techniques et organisationnels de la cybersécurité, ainsi que les implications légales et réglementaires. L'objectif est de garantir que les décisions stratégiques prises par les organes de direction tiennent compte des risques et des défis liés à la cybersécurité.

En conclusion, la directive NIS 2 impose un ensemble de mesures de cybersécurité robustes, accompagnées d'une obligation d'accountability et d'une exigence de formation pour les organes de direction. Ces dispositions visent à renforcer la résilience des entités essentielles et importantes face aux menaces cybernétiques, tout en assurant une gouvernance efficace et informée des risques cyber.

V. Rôle et Pouvoirs de l'ANSSI

A. Autorité de l'ANSSI dans le Cadre de la Directive NIS 2

L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) joue un rôle central dans la mise en œuvre de la directive NIS 2 en France. En tant qu'autorité nationale en matière de cybersécurité, l'ANSSI est chargée de superviser l'application des dispositions de la directive, en collaboration avec les autres autorités compétentes désignées au niveau national.

Selon l'article 8 de la directive NIS 2, l'ANSSI est investie de plusieurs responsabilités clés, notamment l'identification des entités opérant des services essentiels, l'évaluation des risques de sécurité des réseaux et des systèmes d'information, et la vérification de la mise en œuvre des mesures de sécurité appropriées par ces entités. L'agence est également responsable de la collecte et de l'analyse des notifications d'incidents, ainsi que de la coordination des réponses aux incidents à l'échelle nationale.

B. Injonctions et Avertissements Émis par l'ANSSI

Dans l'exercice de ses fonctions, l'ANSSI dispose de la capacité d'émettre des injonctions et des

avertissements aux entités non conformes aux exigences de la directive. Conformément à l'article 19 de la directive NIS 2, l'ANSSI peut exiger des entités concernées qu'elles prennent des mesures spécifiques pour remédier aux manquements identifiés dans leurs systèmes de cybersécurité. Ces injonctions peuvent être accompagnées de délais précis pour leur mise en œuvre.

En cas de non-respect des injonctions, l'ANSSI est habilitée à émettre des avertissements publics ou privés. Ces avertissements servent à alerter l'entité concernée sur les conséquences potentielles de la non-conformité, y compris les risques pour la sécurité des réseaux et des systèmes d'information.

C. Capacité de l'ANSSI à Imposer des Amendes

L'article 23 de la directive NIS 2 confère à l'ANSSI le pouvoir d'imposer des amendes administratives en cas de non-conformité avérée. Ces amendes peuvent être significatives et sont déterminées en fonction de la gravité et de la durée du manquement, ainsi que de la capacité financière de l'entité concernée. L'objectif de ces sanctions est de garantir le respect des normes de cybersécurité et de dissuader les comportements non conformes.

En conclusion, l'ANSSI joue un rôle crucial dans l'application de la directive NIS 2 en France. Ses pouvoirs d'injonction, d'avertissement et de sanction sont des outils essentiels pour assurer la conformité des entités aux exigences de cybersécurité et pour protéger les infrastructures critiques nationales contre les risques cybernétiques. La directive NIS 2 renforce ainsi la capacité de l'ANSSI à agir efficacement dans le domaine de la cybersécurité, contribuant à la sécurité globale des systèmes d'information en France.

VI. Impact de la Directive sur les Entités Concernées

A. Conséquences pour les Entités ne Respectant pas la Directive

La directive NIS 2, en tant que cadre réglementaire européen, impose des exigences strictes en matière de cybersécurité aux entités essentielles et importantes. Le non-respect de ces exigences peut entraîner des conséquences significatives pour les entités concernées. Ces conséquences se manifestent principalement sous deux formes : les sanctions administratives et les répercussions opérationnelles.

1. Sanctions Administratives : Selon l'article 23 de la directive NIS 2, les entités qui ne se conforment pas aux exigences peuvent être sujettes à des amendes administratives. Ces amendes sont calculées en fonction de la gravité et de la durée du manquement, ainsi que de la taille et de la nature de l'entité. Elles visent à encourager la conformité et à dissuader les comportements négligents ou non conformes.
2. Répercussions Opérationnelles : Au-delà des sanctions financières, le non-respect de la directive peut entraîner des perturbations opérationnelles majeures. Cela inclut la perte de confiance des clients et des partenaires, des dommages à la réputation, et des interruptions potentielles des services, qui peuvent avoir un impact économique direct sur l'entité.

B. Importance de la Conformité pour la Sécurité Publique et Économique

La conformité à la directive NIS 2 est essentielle non seulement pour éviter les sanctions, mais aussi pour maintenir la sécurité publique et économique. Les entités essentielles et importantes jouent un rôle crucial dans le fonctionnement de la société et de l'économie. Une défaillance dans leurs systèmes de cybersécurité peut avoir des conséquences désastreuses, allant de la perturbation des services essentiels à des atteintes à la sécurité nationale.

La directive vise donc à garantir un niveau élevé de sécurité des réseaux et des systèmes d'information, ce qui est fondamental pour la protection des infrastructures critiques et la continuité des services vitaux pour la société.

VII. Conclusion

A. Résumé des Enjeux Majeurs de la Directive NIS 2

La directive NIS 2 représente un jalon important dans l'évolution de la législation européenne en matière de cybersécurité. Elle élargit le champ d'application par rapport à la directive NIS 1, couvrant un plus grand nombre d'entités et imposant des exigences plus strictes. Les enjeux majeurs de cette directive résident dans la nécessité d'assurer un niveau élevé de sécurité des réseaux et des systèmes d'information à travers l'Union européenne, en réponse à l'augmentation des menaces cybernétiques.

B. Importance de la Préparation des Entités pour la Mise en Conformité

Pour les entités concernées, la préparation et la mise en conformité avec la directive NIS 2 sont cruciales. Cela implique non seulement l'adoption de mesures techniques et organisationnelles adéquates, mais aussi une compréhension approfondie des exigences réglementaires et des risques associés. La formation des organes de direction, la mise en place de systèmes de gestion des risques efficaces, et la préparation à la notification et à la gestion des incidents sont des aspects clés de cette préparation.

En conclusion, la directive NIS 2 constitue un pas en avant significatif dans la protection contre les risques cybernétiques en Europe. Sa mise en œuvre réussie dépendra de la capacité des entités concernées à comprendre, à se préparer et à se conformer à ses exigences, garantissant ainsi la sécurité et la résilience des infrastructures critiques au sein de l'Union européenne.

https://www.lebouard-avocats.fr/

https://www.avocatsversailles.fr/