LES DIRECTIVES NIS (NETWORK AND INFORMATION SYSTEMS)

SOULEYE NDOUR, EMILIO VAILLANT

11 DÉCEMBRE 2024

Crédit photo : domaine public

DEFINSEEC.COM DEFINSEEC@GMAIL.COM 07 83 51 70 94

INTRODUCTION

Objectifs de l'article :

L'objectif de cet article est d'explorer en détail la directive NIS et son impact sur la cybersécurité en Europe. Nous nous concentrerons sur les principaux enjeux de la directive, son cadre législatif, les obligations qu'elle impose aux acteurs concernés, ainsi que les défis qu'elle comporte. Ce travail permettra de répondre aux questions suivantes :

- Quelle est la portée de la directive NIS et quels secteurs sont concernés ?
- Quelles obligations les opérateurs de services essentiels doivent ils respecter en matière de cybersécurité ?
- Quel est le rôle des autorités nationales et européennes dans la mise en œuvre de la directive ?
- Quelles sont les révisions apportées par la directive NIS2 pour renforcer encore la cybersécurité en Europe ?

En suivant cette analyse, l'article met en lumière l'importance de la directive NIS pour assurer la résilience de l'Europe face aux cybermenaces, tout en soulignant les difficultés rencontrées dans sa mise en œuvre et les évolutions nécessaires à son amélioration.

I. LES ORIGINES DES DIRECTIVES NIS

a. Historique de l'UE et de la législation en matière de cybersécurité

L'UE a pris conscience, dans les années 2000, de l'importance croissante des technologies numériques pour ses économies, ses sociétés et ses gouvernements. Avec la numérisation rapide, l'UE a vu se multiplier les cybermenaces, ce qui a mis en évidence la nécessité de renforcer la cybersécurité au niveau européen.

- **2004** - Création de l'ENISA : L'Agence de l'Union européenne pour la cybersécurité (ENISA) a été créée en 2004 pour aider les États membres à coordonner leurs efforts pour sécuriser les réseaux et les systèmes d'information. Cependant, au début, ENISA n'avait pas de pouvoir législatif direct et son rôle était plus consultatif.

- **2013** - Stratégie pour la cybersécurité de l'UE : L'UE a adopté en 2013 une stratégie pour renforcer la cybersécurité à l'échelle de l'Union. L'objectif était de garantir que les réseaux et systèmes d'information restent sûrs et résilients, tout en améliorant la coopération internationale en matière de sécurité informatique.

- **2016** - Première directive NIS : La Directive NIS a été adoptée pour renforcer la cybersécurité dans les États membres de l'UE. Elle oblige les États membres à mettre en place des mesures de sécurité et de notification des incidents, pour les opérateurs de services essentiels et les fournisseurs de services numériques. Ce fut l'un des premiers efforts législatifs à imposer des exigences de cybersécurité à l'échelle européenne.

- **2022** - Révision de la directive NIS : NIS2 : En réponse à l'évolution rapide des cybermenaces et à l'augmentation des attaques, la directive NIS a été révisée en 2022 sous le nom de NIS2. Adoptée en décembre, cette version améliore l'approche de la cybersécurité en élargissant le champ des secteurs concernés, en augmentant les obligations de sécurité et de notification des incidents, et en renforçant la coopération entre les États membres. Son entrée en vigueur en France s'est faite le 17 octobre 2024.

I. LES ORIGINES DES DIRECTIVES NIS

b. Nécessité d'un cadre européen pour la cybersécurité :

Plusieurs facteurs ont motivé la création d'un cadre européen pour la cybersécurité, dont les suivants :

- **La mondialisation et l'interconnexion des systèmes :** Les infrastructures critiques sont désormais interconnectées à l'échelle mondiale. Une cyberattaque dans un État membre peut avoir des répercussions dans d'autres pays de l'UE. Il est donc crucial que tous les États membres adoptent des normes communes pour prévenir les cyberattaques à grande échelle.

- **Le renforcement des menaces cyber :** Les attaques informatiques ont considérablement augmenté, et les cybercriminels, les groupes étatiques et les hackers individuels utilisent des techniques de plus en plus sophistiquées pour exploiter les vulnérabilités des systèmes. Sans un cadre législatif commun, les États membres risquaient de rester vulnérables à ces menaces globales. Des systèmes d'information de plus en plus critiques : Les infrastructures de communication, d'énergie, de santé, et de transport dépendent de plus en plus de systèmes numériques. Le moindre incident de sécurité dans ces secteurs pourrait entraîner des conséquences graves pour l'économie et la sécurité nationale. Un cadre européen permet de garantir que les États membres prennent des mesures adéquates pour protéger ces systèmes.

- **Le manque d'harmonisation :** Avant l'introduction des directives NIS, chaque État membre avait sa propre approche en matière de cybersécurité, ce qui rendait difficile la coopération transfrontalière. Les entreprises opérant dans plusieurs États membres étaient confrontées à des exigences nationales divergentes. L'harmonisation était donc essentielle pour faciliter la coopération et la mise en œuvre de mesures communes.

- **L'impact économique et géopolitique :** L'UE souhaitait aussi affirmer sa position sur la scène mondiale, en promouvant un modèle de cybersécurité résilient, transparent et interopérable. La cybersécurité est devenue une question géopolitique, les attaques informatiques étant utilisées comme un moyen de pression ou de sabotage économique.

II. PRÉSENTATION DÉTAILLÉE DE LA DIRECTIVE NIS

a. Les Grands Principes de la Directive NIS

Les grands principes de la directive NIS reposent sur un cadre global visant à améliorer la cybersécurité des États membres, des entreprises et des organisations qui gèrent des infrastructures essentielles. Ces principes incluent :

- **Renforcement de la sécurité des réseaux et systèmes d'information** : La directive impose aux entités visées de mettre en œuvre des mesures techniques et organisationnelles pour assurer la sécurité des réseaux et des systèmes d'information sur lesquels reposent des services essentiels.

- **Gestion des risques** : Les entités doivent évaluer de manière régulière les risques auxquels elles sont exposées, en prenant des mesures pour prévenir ou atténuer les menaces qui peuvent affecter la continuité des services.

- **Notification des incidents de cybersécurité** : La directive exige des opérateurs de services essentiels et des fournisseurs de services numériques qu'ils signalent les incidents majeurs de cybersécurité à l'autorité nationale compétente dans un délai très court (généralement 24 heures pour les incidents graves).

- **Coopération et partage d'informations** : La directive encourage la coopération entre les États membres de l'UE, avec un partage d'informations sur les cybermenaces, incidents, et bonnes pratiques afin de renforcer la réponse collective face aux attaques.

- **Responsabilisation des acteurs** : Les entités concernées sont responsables de la gestion de la cybersécurité dans leurs infrastructures et doivent veiller à sensibiliser et former leur personnel aux bonnes pratiques en matière de sécurité numérique.

II. PRÉSENTATION DÉTAILLÉE DE LA DIRECTIVE NIS

b. Les Services Essentiels Couverts par la Directive NIS

Les services essentiels couverts par la directive NIS sont ceux dont l'interruption ou la défaillance pourrait entraîner des conséquences graves sur la société, l'économie, la santé publique, ou la sécurité nationale. Parmi ces services, les plus essentiels comprennent :

- **L’énergie** : L’approvisionnement en énergie, notamment en électricité, gaz et pétrole, est fondamental pour tous les autres secteurs de la société. Sans une infrastructure énergétique fiable, les hôpitaux, les entreprises, et même les systèmes de communication seraient paralysés. Une coupure d’approvisionnement énergétique peut entraîner des pertes économiques massives et affecter la vie quotidienne de la population.

- **Le transport** : Le secteur du transport, qui comprend l’aérien, le ferroviaire, le maritime et le routier, est essentiel pour la mobilité des personnes et des biens. Une perturbation dans ces services, qu’elle soit due à des cyberattaques ou à d’autres causes, peut entraîner des retards importants dans les chaînes d’approvisionnement, ainsi que des crises logistiques qui touchent toutes les industries, y compris la distribution alimentaire et les soins médicaux.

- **Les services financiers** : Les systèmes bancaires et de paiement sont au cœur de l’économie moderne. Si les services financiers sont perturbés, cela peut paralyser les transactions économiques, affecter les économies nationales et internationales, et nuire à la confiance du public dans les institutions financières. Par exemple, une cyberattaque contre une plateforme de paiement pourrait entraîner une perte massive de fonds et de données sensibles.

- **La santé** : Dans le secteur de la santé, les hôpitaux et les systèmes de soins utilisent de plus en plus de technologies pour fournir des services médicaux et gérer les dossiers des patients. Une attaque contre ces systèmes pourrait compromettre non seulement les soins de santé d’urgence mais aussi la confidentialité des données médicales des patients, mettant en danger la santé publique. La résilience des systèmes d’information dans ce secteur est cruciale pour assurer la continuité des soins.

II. PRÉSENTATION DÉTAILLÉE DE LA DIRECTIVE NIS

b. Les Services Essentiels Couverts par la Directive NIS

- **L'approvisionnement en eau** : L'approvisionnement en eau potable est vital pour la santé publique et la sécurité. Des attaques sur les infrastructures de gestion et de distribution de l'eau peuvent entraîner des pénuries, contaminer l'eau ou rendre son accès difficile, ce qui a des répercussions directes sur la vie quotidienne des citoyens et la sécurité alimentaire.

- **Les infrastructures de communication** : Les télécommunications, Internet, et les services numériques jouent un rôle clé dans tous les aspects de la société moderne, que ce soit pour les affaires, les services publics, ou la vie personnelle. Une interruption de ces services peut paralyser la communication, affecter le commerce en ligne, et entraver l'accès à l'information essentielle, notamment en période de crise. Ces secteurs sont interconnectés, et la défaillance de l'un d'entre eux peut avoir un effet domino, provoquant des perturbations massives dans d'autres domaines. C'est pourquoi la directive NIS se concentre particulièrement sur la cybersécurité dans ces domaines afin d'assurer la continuité et la résilience des services critiques.

II. PRÉSENTATION DÉTAILLÉE DE LA DIRECTIVE NIS

C. Objectifs de ces directives

Les trois objectifs majeurs de la directive NIS sont donc : le renforcement de la sécurité des réseaux et des systèmes d'information, la gestion efficace des incidents de cybersécurité, et la coopération renforcée entre les États membres de l'UE.

1. Renforcement de la sécurité des réseaux et des systèmes d'information

Le premier objectif de la directive NIS est de renforcer la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels (OSE) et des fournisseurs de services numériques (FSN) (services de cloud computing, hébergement de site web...). La directive impose aux entités concernées de prendre des mesures adéquates pour prévenir et réduire les risques cybernétiques.
Cela passe par l'adoption de bonnes pratiques en matière de cybersécurité, telles que la mise en œuvre de **mesures techniques** pour protéger les systèmes : pares-feux, systèmes de détection d'intrusion, logiciels antivirus, outils de monitoring, systèmes d’alertes automatisées. Des **mesures organisationnelles** telle que la gestion des accès et des sensibilisation continue du personnel aux bonnes pratiques de cybersécurité,(en organisant des formations régulières pour prévenir les erreurs humaines et renforcer la vigilance face à des risques comme le phishing ou l’utilisation de mots de passe faibles) sont également nécessaire pour assurer une gestion efficace des risques. En outre, les entités doivent réaliser des évaluations de risques régulières, et mettre en place des plans de sécurité pour faire face à des menaces potentielles. Ce renforcement des mesures de sécurité vise à garantir la résilience de ces infrastructures critiques face aux cyberattaques et à limiter l'impact de toute perturbation potentielle.

II. PRÉSENTATION DÉTAILLÉE DE LA DIRECTIVE NIS

OSE :

Les Opérateurs de Services Essentiels doivent mettre en œuvre des mesures techniques et organisationnelles pour gérer les risques menaçant la sécurité des réseaux et et des systèmes d'information

FSN :

Les Fournisseurs de Services Numériques sont tenus de notifier les incidents de sécurité à l'autorité compétente

QUEL PÉRIMÈTRE ?

OSE : Opérateurs de services Essentiels

- *Energie*
- *Banques*
- *Transports*
- *Secteur de la santé*
- *Fourniture et distribution d'eau potable*
- *Infrastructures numériques*
- *Infrastructures de marché financiers*

FSN : Fournisseurs de Services Numériques

- *Les places de marchés en ligne*
  Ex : Amazon, e-Bay, app stores…
- *Les moteurs de recherche*
  Ex : Google, Bing, Yahoo…
- *Les services d'informatique Cloud*
  Ex : Dropbox, Google …

2. Réponse aux incidents de cybersécurité

Le second objectif de la directive NIS est d'améliorer la réponse aux incidents de cybersécurité. Les incidents de cybersécurité sont de plus en plus fréquents et sophistiqués, et peuvent avoir des répercussions graves sur la continuité des services essentiels. Dans ce contexte, la directive impose aux opérateurs de services essentiels et aux fournisseurs de services numériques de notifier rapidement tout incident majeur aux autorités compétentes, généralement dans les 24 heures suivant la détection de l'incident. Cette exigence vise à garantir que les autorités puissent réagir promptement et de manière coordonnée face aux attaques, minimisant ainsi leur impact. En plus de la notification, les entités doivent disposer de plans de gestion des incidents qui incluent des procédures pour isoler et contenir l'incident, restaurer les services affectés, et mener des analyses post-incidents pour améliorer les mesures de sécurité. Une réponse rapide et efficace aux cyberattaques est essentielle pour protéger les infrastructures critiques et maintenir la confiance des citoyens et des entreprises dans les services numériques.

II. PRÉSENTATION DÉTAILLÉE DE LA DIRECTIVE NIS

3. Coopération entre les États membres

Enfin, le troisième objectif de la directive NIS est de renforcer la coopération entre les États membres de l'UE. La cybersécurité étant un défi global et transnational, la directive encourage un partage d'informations et une collaboration accrue entre les pays de l'Union européenne pour mieux prévenir et réagir aux cybermenaces. Chaque État membre doit désigner une autorité nationale compétente en matière de cybersécurité chargée de veiller à ce que les OSE et les FSN respectent les obligations imposées par la directive. et qui permet d'établir un point de contact unique pour coordonner les réponses aux incidents,

En outre, la directive encourage la création de réseaux de coopération, tels que le Groupe de coopération de la directive NIS, pour favoriser les échanges sur les cybermenaces, les bonnes pratiques et les enseignements tirés des incidents.

Les États membres doivent également collaborer avec l'ENISA (Agence de l'Union européenne pour la cybersécurité), qui soutient les efforts collectifs, fournit des conseils, et organise des exercices de simulation pour tester la réactivité des systèmes face à des cyberattaques. Cette coopération est essentielle pour assurer une approche cohérente et efficace de la cybersécurité à l'échelle européenne.

AJOUT DE NOUVEAU SECTEURS SOUS LES DIRECTIVES NIS 2 :

- ENERGIE
- TRANSPORTS
- SANTÉ
- SERVICES FINANCIERS
- EAU
- COMMUNICATION
- + ADMINISTRATIONS PUBLIQUES
- + FOURNISSEURS NUMÉRIQUES
- + SERVICES POSTAUX
- + GESTION DE DECHETS
- + ESPACE
- + NOURRITURE
- + FABRICATION
- + PRODUITS CHIMIQUES
- + RECHERCHE

Le remaniement de la directive a conduit a l'ajout de nouveaux secteurs concernés, formant la directive NIS 2

III. DÉFIS ET LIMITES

La directive NIS a un impact significatif à la fois sur les entreprises et sur les gouvernements, en renforçant la cybersécurité à travers l'Union européenne. Elle impose des exigences strictes aux opérateurs de services essentiels et aux fournisseurs de services numériques, ce qui présente des défis importants pour les entreprises en termes de coûts et de mise en conformité. De plus, elle entraîne des changements au niveau des gouvernements, en les obligeant à renforcer la collaboration et la coordination en matière de cybersécurité à l'échelle européenne.

a. Les défis pour les entreprises : coûts et mise en conformité

Les entreprises doivent faire face à plusieurs défis pour se conformer à la révision de la directive NIS (NIS2), principalement en raison des coûts et des efforts nécessaires pour répondre aux nouvelles exigences de cybersécurité. La mise en conformité avec la directive exige des investissements considérables dans des technologies de sécurité avancées, telles que des systèmes de détection des intrusions, des solutions de cryptage, ainsi que des outils pour garantir la continuité des services en cas d'incident. Les entreprises doivent également investir dans la formation continue de leurs équipes de cybersécurité pour garantir qu'elles sont bien préparées à répondre aux nouvelles menaces et qu'elles respectent les règles de notification rapide des incidents.

De plus, les petites et moyennes entreprises (PME) peuvent rencontrer des difficultés spécifiques en raison de leurs ressources limitées. Elles devront souvent s'appuyer sur des solutions moins coûteuses ou externaliser certains services de cybersécurité, ce qui peut entraîner des coûts supplémentaires. La mise en conformité avec NIS2 exige aussi des révisions des processus internes et des politiques de gestion des risques, ce qui peut perturber les opérations et nécessiter une gestion de projet approfondie. En somme, bien que les mesures de sécurité soient nécessaires pour protéger les données et les infrastructures, le coût de la mise en œuvre et les ressources requises peuvent représenter un frein, surtout pour les entreprises moins équipées.

III. DÉFIS ET LIMITES

b. Les différences entre les États membres

L'un des défis majeurs de la directive NIS réside dans les différences de mise en œuvre entre les États membres de l'Union européenne. Chaque pays a sa propre approche de la cybersécurité, avec des niveaux de maturité et des priorités très variés en fonction de son infrastructure, de ses ressources et de ses capacités en matière de cybersécurité. Par exemple, certains États ont déjà mis en place des structures robustes pour la cybersécurité et disposent de ressources humaines et financières conséquentes, tandis que d'autres, notamment les plus petits ou les moins développés en matière de sécurité numérique, peuvent avoir du mal à se conformer aux exigences de la directive. Cette disparité peut créer des déséquilibres dans la protection des réseaux et des systèmes d'information au sein de l'UE, car des pays avec des infrastructures moins sécurisées pourraient devenir des points faibles dans le système de sécurité global. De plus, les différences en matière de réglementation, d'approches législatives et de coordination intergouvernementale compliquent les efforts de coopération transfrontalière et peuvent retarder la réponse collective aux incidents de cybersécurité.

c. L'évolution rapide des cybermenaces et l'adaptation des législations

Le dynamisme des cybermenaces constitue un autre défi important pour la directive NIS. Les cyberattaques deviennent de plus en plus sophistiquées, diversifiées et difficiles à détecter, ce qui met à l'épreuve les systèmes de cybersécurité existants. Les hackers utilisent de nouvelles techniques, comme les attaques par ransomware, les attaques sur les chaînes d'approvisionnement ou les menaces provenant de l'intelligence artificielle, pour pénétrer les réseaux et causer des dommages. Ces évolutions rendent les normes de cybersécurité définies dans la directive NIS rapidement obsolètes si elles ne sont pas régulièrement mises à jour. Les États membres doivent donc adapter leur législation et leurs pratiques en temps réel pour contrer ces menaces émergentes. Cependant, cette capacité d'adaptation rapide est souvent entravée par des processus législatifs lents, des manques de coordination entre les parties prenantes et des ressources insuffisantes pour surveiller l'évolution des menaces. De plus, la directive NIS2, bien qu'elle soit une révision de la directive NIS, ne peut pas anticiper toutes les menaces futures, et il reste à voir si elle sera suffisamment flexible pour répondre aux défis de demain.

CONCLUSION

En conclusion, les directives NIS, qu'il s'agisse de la version initiale ou de la révision NIS2, restent essentielles pour assurer la cybersécurité en Europe. Elles ont permis de mettre en place un cadre juridique solide pour protéger les infrastructures critiques et les services essentiels contre les cyberattaques, tout en favorisant une meilleure coopération entre les États membres. Cependant, avec l'évolution rapide des cybermenaces, il est nécessaire que cette législation continue à s'adapter pour rester efficace face à de nouvelles menaces. Les perspectives pour l'avenir de la cybersécurité en Europe nécessitent une harmonisation plus forte entre les pays, ainsi qu'une capacité à réagir rapidement aux nouvelles vulnérabilités. L'objectif reste de garantir une protection solide des entreprises et des citoyens, de maintenir une économie numérique sécurisée et d'encourager une collaboration internationale face aux défis mondiaux de la cybersécurité. En fin de compte, ces efforts permettront de renforcer la résilience de la société européenne face aux risques numériques et d'assurer un avenir plus sûr pour tous.

SOURCES

- “Directive NIS 2 : renforcer la cybersécurité en Europe”, CHARLOTTE BARAUDON, via Adimeo
- “Directive NIS 2 : Impacts et enjeux sur les entreprises françaises”, vidéo sur Kaspersky
- “Directive NIS 2 : Comment l’anticiper ? Le compte à rebours est lancé !”, vidéo par les Assises de la cyber, via la plateforme youtube
- “Directive NIS 2 : un tournant majeur pour la cybersécurité en Europe”, NOEMIE LE BOUARD, via le site village de la justice
- “Tout savoir sur les changements de la nouvelle directive NIS 2", article depuis le site site Orange cyberdéfense
- “[Tribune] Sécurité Sanitaire : Les Cyber incidents défient l’UE à repenser sa stratégie de Cybersécurité en 2023", JELLE WIERINGA, via le site Alliancy
- “La directive NIS”, article depuis le site Cyber.gouv
- “La directive NIS 2 : tout savoir sur les changements à venir”, article depuis le site Lovell.consulting
- “Chronologie - cybersécurité”, depuis le site consilium.europa
- “Cybersécurité: comment l'UE lutte contre les cybermenaces” chronologie depuis le site consilium.europa
- “La Directive sur la sécurité des réseaux et des systèmes d'information (Directive NIS)”, article depuis le site itogouvernance
- “En pleine préparation de la NIS V2, mise à jour du tour d’horizon européen de transposition de la directive NIS par les états membres… vers une convergence ?”, article depuis le site riskinsight-wavestone
- “Directive NIS : quels enjeux et comment s’y préparer ?”, article depuis le site riskinsight-wavestone

SUIVEZ DEF'INSEEC SUR

DEFINSEEC.COM DEFINSEEC@GMAIL.COM 07 83 51 70 94