Directive NIS 2 : un nouveau mécanisme pour renforcer la cybersécurité en Europe

Fiche pratique publié le **26/03/2024**, vu **1058 fois**, Auteur : Blog de Le Bouard Avocats Versailles

En vigueur depuis 2016,la Directive (NIS) est l'un des principaux piliers de la stratégie de cybersécurité de l'Union européenne. La directive NIS 2 doit être transposée dans le droit français d'ici à octobre 2024.

Transposition de la directive européenne NIS 2 prévue en octobre 2024

En vigueur depuis 2016, la directive Network and Information Security (NIS) est l'un des principaux piliers de la stratégie de cybersécurité de l'Union européenne. La directive NIS 2, sa version améliorée, doit être transposée dans le droit français d'ici à octobre 2024. Le texte vise à mieux protéger les systèmes d'information face aux menaces cybernétiques, mais génère également de nouvelles obligations pour les entreprises et les collectivités.

Périmètre de la réglementation et nouvelles obligations pour les acteurs concernés

Bien que le périmètre exact et la nature de la réglementation restent flous, plusieurs secteurs devront se conformer à la directive NIS 2. Parmi eux :

- Les fournisseurs de services essentiels (FSE) dans des secteurs tels que l'énergie, les transports et les communications.
- Les prestataires de services numériques (PSD), incluant notamment les plateformes d'intermédiation, les moteurs de recherche et les centres de traitement de données.
- Les collectivités locales et intercommunales.

Ces entités devront mettre en place des mesures techniques et organisationnelles pour assurer la sécurité des réseaux et des systèmes d'information. Elles devront également signaler les incidents de sécurité importants à l'autorité compétente.

Un renforcement nécessaire face à une multiplication des cyberattaques

La directive NIS 2 intervient dans un contexte de hausse des cyberattaques en Europe. Il est crucial pour l'Union européenne de mettre en place des mécanismes solides pour protéger ses infrastructures critiques et ses citoyens. En 2023, l'Europe était le continent le plus ciblé par des attaques en ligne avec près de 304 millions de tentatives d'intrusion, ce qui justifie l'importanceque l'UE accorde à la cybersécurité et son souhait de s'appuyer sur ses états membres pourpouvoir réagir rapidement et efficacement.

Préparation et mise en conformité des entreprises françaises

Selon certaines estimations, seulement 7% des entreprises françaises seraient prêtes à incorporer la directive NIS 2. Dans ce contexte, les acteurs concernés doivent se préparer à cette échéance cruciale et mettre en œuvre les dispositifs nécessaires pour être en conformité avec les nouvelles exigences. La coopération entre les différents acteurs, privés et publics, est essentielle pour garantir la mise en place de mesures adéquates et efficientes.

Les collectivités demandent une application proportionnée de la directive NIS 2

Plusieurs associations d'élus représentant les collectivités locales et intercommunales appellent le législateur à une mise en œuvre progressive de la directive NIS 2, afin que le coût financier et technique pour les collectivités concernées soit proportionné. Les Interconnectés, France urbaine et Intercommunalités de France soulignent l'importance d'une cybersécurité renforcée pour protéger les institutions démocratiques, mais demandent également de prendre en compte la réalité budgétaire des collectivités et la capacité des entreprises à mettre en place des mesures efficaces dans un délai aussi court.

La nécessité d'un accompagnement et d'un soutien aux acteurs concernés

Pour aider les acteurs publics et privés à se conformer à la directive NIS 2, il est important d'établir un dialogue entre les différentes parties prenantes et de proposer des formations en cybersécurité. Les pouvoirs publics ont également un rôle à jouer dans le soutien financier et l'accompagnement technique pour faciliter la transition vers des infrastructures plus sécurisées.

Une opportunité pour renforcer la coopération européenne en matière de cybersécurité

L'implémentation de la directive NIS 2 représente une opportunité pour l'Union européenne de consolider son action commune contre les menaces cybernétiques. La réalisation d’une cyberprotection harmonisée au sein des États membres permettrait de développer davantage de synergies et de favoriser la collaboration en cas d'incidents de sécurité transfrontaliers.

En définitive, la directive NIS 2 constitue un défi majeur pour les acteurs concernés, mais également une chance d'améliorer significativement la résilience des infrastructures critiques et des entreprises face aux cyberattaques.