AMENDES NSI2 : APERÇU DES POTENTIELLES SANCTIONS EN CAS DE NON-CONFORMITÉ AVEC LA DIRECTIVE NIS2

Présentation de la directive NIS2

La directive NIS2 s'appuie sur les exigences de la directive originale : elle a toujours pour objectif de protéger les infrastructures et les organisations critiques au sein de l'UE contre les cybermenaces et d'atteindre un même niveau élevé de sécurité dans toute l'UE.

Pour atteindre cet objectif, la directive NIS2 exige que les États membres prennent un certain nombre de mesures supplémentaires, notamment :

- Établir un plan de réponse aux incidents coordonné avec les plans des autres États membres.
- Créer un CERT (Computer Emergency Response Team) national.
- Renforcer la coopération entre les entités des secteurs public et privé.
- Améliorer le partage d'informations entre les États membres.

En travaillant avec les États membres pour les aider à améliorer leurs défenses contre les cyberattaques et en fournissant un soutien et des conseils aux entreprises et aux particuliers, l'UE veille à ce que ses citoyens soient protégés contre le risque croissant de menaces en ligne.

Conséquences de la non-conformité avec la directive NIS2

La directive NIS2 définit clairement les conséquences en cas de violation, notamment :

- Des recours n'impliquant pas l'aspect financier.
- Des sanctions financières.
- Des répercussions juridiques.

Les entités essentielles et importantes peuvent être confrontées à ces conséquences en cas de manquements tels que le non-respect des protocoles de sécurité ou la négligence au niveau du reporting de certains incidents.

Conséquences non financières

La directive NIS2 offre aux organismes de contrôle nationaux la possibilité d'imposer des sanctions non financières, notamment :

- Des obligations de mise en conformité.
- Des directives strictes pour une mise en œuvre immédiate.
- Des exigences en matière d'audit de sécurité.
- Des alertes envoyées aux clients d'une entité concernant les risques potentiels.

Aperçu des sanctions financières

La directive NIS2 différencie clairement les sanctions financières pour les entités essentielles et importantes :

- Entités Essentielles (EE) : les États membres sont invités à infliger des amendes pouvant aller jusqu'à 10 000 000 € ou 2 % du chiffre d'affaires annuel global, le montant le plus élevé étant retenu.

- Entités Importantes (IE) : dans le cadre de la directive NIS2, les amendes peuvent atteindre 7 000 000 € ou 1,4 % du chiffre d'affaires annuel global, le montant le plus élevé étant retenu.

AMENDES NSI2 : APERÇU DES POTENTIELLES SANCTIONS EN CAS DE NON-CONFORMITÉ AVEC LA DIRECTIVE NIS2

ENTITÉS ESSENTIELLES (EE)

- Cette catégorie englobe les organisations des secteurs public et privé opérant dans des domaines tels que les transports, la finance, l'énergie, l'eau, l'aérospatiale, la santé, la gouvernance publique et l'infrastructure numérique.
- Amende potentielle : le montant le plus élevé entre 10 millions d'euros ou 2 % du chiffre d'affaires global annuel.

ENTITÉS IMPORTANTES (IE)

- Ce groupe couvre à la fois les entreprises publiques et privées dans des secteurs tels que la production alimentaire, les services numériques, la chimie, les services postaux, la gestion des déchets, la recherche et les secteurs manufacturiers.
- Seuil des sanctions : 7 millions d'euros ou 1,4 % du chiffre d'affaires global annuel, selon le montant le plus élevé.

Responsabilité managériale en cas de cyberincidents

Afin de réduire la responsabilité écrasante traditionnellement confiée aux services informatiques concernant la sécurité organisationnelle et pour modifier la perception de la notion de responsabilité en matière de cybersécurité, la directive NIS2 introduit des réglementations visant à tenir l'équipe dirigeante directement responsable de toute négligence importante lors de violations de sécurité.

Dans le cadre de NIS2, si une négligence grave est établie à la suite d'un incident lié à la cybersécurité, les autorités des États membres peuvent :

- Exiger que les organisations divulguent publiquement les violations de conformité.
- Publier des annonces publiques mettant en lumière à la fois la ou les personnes physiques et morales responsables de la violation, en fournissant les détails.
- Pour les organisations classées comme entités essentielles, imposer une interdiction temporaire à certaines personnes d'assumer des rôles de direction si de telles violations devaient se reproduire.

Ces dispositions visent à garantir l'engagement et la responsabilité de l'équipe dirigeante concernant la lutte contre les risques de cybersécurité.