EURO CYBER GROUP

RÉSILIENCE
CONFORMITÉ
CYBERSÉCURITÉ
COORDINATION

NIS 2
Directive européenne visant à renforcer la cybersécurité des secteurs critiques dans l'Union européenne.

DIRECTIVE NIS 2

Description de NIS 2

La directive (Directive (UE) 2022/2555) adoptée le 14 décembre 2022, vise à renforcer la cybersécurité dans l'Union européenne. Elle s'applique aux secteurs critiques tels que l'énergie, la santé, les infrastructures numériques et les télécommunications, afin de protéger leurs systèmes d'information contre les cyberattaques. Son objectif est de renforcer la résilience des infrastructures, en demandant aux entreprises d'améliorer la sécurité de leurs réseaux et de mieux se préparer face aux incidents. Elle harmonise également les normes de cybersécurité à travers l'UE, réduisant ainsi les disparités entre les États membres. Les entreprises doivent gérer les risques de manière proactive, en identifiant les vulnérabilités et en notifiant rapidement les incidents aux autorités. Des mécanismes de supervision plus stricts sont instaurés, avec des sanctions renforcées pour garantir la conformité. Cette directive est cruciale pour renforcer la sécurité numérique en Europe, assurer la continuité des services critiques et répondre aux défis croissants des cybermenaces.

Composition de NIS 2

Gestion des risques

La gestion des risques dans la directive NIS 2 exige que les entreprises identifient, évaluent et réduisent les vulnérabilités liées à leurs systèmes critiques, en mettant en place des mesures de protection adaptées. Elles doivent évaluer régulièrement leurs risques, déployer des solutions de cybersécurité efficaces, et prévoir des plans de réponse aux incidents pour réagir rapidement en cas de cyberattaque. Cette approche garantit une meilleure résilience face aux menaces tout en assurant la continuité des services essentiels.

Rapport d'incidents

Dans le cadre de la directive NIS 2, les entreprises sont tenues de signaler rapidement tout incident de cybersécurité majeur aux autorités compétentes. Ce rapport doit être fait dès la détection de l'incident pour permettre une réaction rapide et coordonnée. L'objectif est de minimiser les impacts, de limiter les perturbations des services essentiels et d'améliorer la résilience globale face aux cybermenaces à l'échelle nationale et européenne.

Coopération transfrontalière

La directive NIS 2 encourage une coopération renforcée entre les États membres et leurs autorités pour améliorer la cybersécurité au niveau national et européen. Les autorités nationales doivent collaborer étroitement en partageant informations et bonnes pratiques, et en coordonnant leurs actions face aux cybermenaces. Cette coopération permet une réponse harmonisée et efficace aux incidents transfrontaliers, renforçant ainsi la résilience collective de l'UE face aux cyberattaques.

Responsabilité des entreprises

La directive NIS 2 s'étend désormais aux prestataires tiers, comme les fournisseurs de services numériques et de cloud. Les entreprises doivent s'assurer que ces partenaires respectent les mêmes normes de cybersécurité, en évaluant les risques liés à leurs services. Cela renforce la sécurité de la chaîne d'approvisionnement et protège les infrastructures critiques contre les menaces cyber venant de tiers

Supervision renforcée

La directive NIS 2 instaure une supervision renforcée des entreprises critiques pour garantir leur conformité aux exigences de cybersécurité. Les autorités compétentes peuvent réaliser des audits réguliers, des inspections et imposer des mesures correctives en cas de non-conformité. Cette surveillance accrue permet d'assurer un haut niveau de sécurité et de réagir rapidement aux failles ou incidents potentiels.

EXPERTISE SUR DEMANDE EN CONFORMITÉ NIS 2
GESTION DES RISQUES, TECHNOLOGIES ET RÉSILIENCE OPÉRATIONNELLE

DES EXPERTS À VOTRE SERVICE POUR VOUS ACCOMPAGNER SUR LA DIRECTIVE NIS 2

Optimiser votre conformité à NIS 2 avec nos experts en gouvernance et conformité. Nous offrons une flexibilité totale en mettant à votre disposition des spécialistes qualifiés pour répondre à vos besoins en gestion des risques TIC, de résilience opérationnelle et de gouvernance.

Secteur concerné par NIS 2

- Énergie
- Transports
- Bancaire
- Infrastructures des marchés financiers
- Santé
- Eau potable
- Eaux usées
- Infrastructures numériques
- Gestion des services TIC
- Administration publique
- Espace
- Services postaux et d'expédition
- Gestion des déchets
- Fabrication, production et distribution de produits chimiques
- Production, transformation et distribution des denrées alimentaires
- Fabrication
- Fournisseurs numériques
- Recherche

Pourquoi est-ce important ?

La conformité à NIS 2 est obligatoire pour les secteurs critiques sous peine de sanctions. Avec la hausse de la cybercriminalité, cette directive est essentielle pour protéger les services vitaux contre les incidents.

Pourquoi nous choisir ?

1. Audit et diagnostic

- Identification des écarts : Nous analysons votre infrastructure et vos processus pour identifier les écarts par rapport aux exigences de NIS 2.
- Rapport d'audit détaillé : Vous recevrez un diagnostic complet, mettant en lumière les priorités de conformité.

2. Développement et mise en place d'un plan d'action

- Solutions sur mesure : Nos experts en cybersécurité élaborent des plans d'action ciblés pour combler les lacunes, incluant des solutions de gouvernance, de gestion des risques et d'amélioration des capacités techniques.
- Support continu : Nous accompagnons la mise en œuvre et assurons une supervision continue jusqu'à la conformité totale

3. Supervision

- Suivi des incidents : Nous mettons en place des mécanismes pour assurer la surveillance et la réponse aux incidents en temps réel, conformément aux obligations de NIS 2.
- Gestion proactive des risques : Notre approche vise à prévenir les cybermenaces avant qu'elles n'impactent votre activité.

4. Formation et sensibilisation

- Programmes de formation : Euro Cyber Group forme vos équipes aux meilleures pratiques de cybersécurité et aux procédures de gestion des incidents pour renforcer la cyber résilience de votre entreprise.
- Sensibilisation continue : Ateliers et campagnes de sensibilisation pour maintenir un haut niveau de vigilance.

CONTACTEZ NOUS

contact@eurocybergroup.fr - 01 46 94 62 00
Euro Cyber Group - 75 rue de Lourmel - 75015 Paris

www.eurocybergroup.fr