Le mémo NIS 2

by CHIMERE

Qu'est ce que la directive NIS 2 ?

La directive NIS2 (Network and Information Security Directive) est un cadre législatif de l'Union européenne conçu pour renforcer les exigences en matière de cybersécurité pour les infrastructures critiques et les services essentiels en Europe. Face à des cybermenaces en constante évolution, elle élargit son champ d'application à un plus grand nombre de secteurs et impose des mesures de protection plus strictes :

- Mesures techniques robustes
- Gestion des accès
- Réponse rapide aux incidents de sécurité
- Contrôle accru des fournisseurs et sous-traitants

L'objectif est d'accroître la résilience face aux cybermenaces et de garantir une protection adéquate des réseaux et des services essentiels.

Suis-je concerné ?

Les entités des secteurs identifiés sont classées comme entités essentielles ou entités importantes en fonction de facteurs tels que la taille, le secteur et la criticité. Sont concernés :

Entités essentielles

- Secteurs de haute criticité – entreprises dépassant le seuil de taille moyenne.
- Fournisseurs de services de confiance qualifiés et registres de noms de domaine de premier niveau, quelle que soit leur taille.
- Fournisseurs de services DNS, quelle que soit leur taille.
- Fournisseurs de réseaux de communications électroniques (ECN) ou de services de communications électroniques (ECS) – entreprises de taille moyenne et grandes.

Entités importantes

- Secteurs de haute criticité – entreprises de petite ou moyenne taille
- Autres secteurs critiques – entreprises dépassant le seuil de taille moyenne
- Fournisseurs d'ECN ou d'ECS – petites entreprises

Pour en savoir plus, vous pouvez faire le test sur :

https://monespacenis2.cyber.gouv.fr

Secteurs de haute criticité :

Énergie, Infrastructures numériques, Transport, Espace, Santé, Administration publique, Eau potable, Banque, Eaux usées

Autres secteurs critiques :

Infrastructures des marchés financiers, Fabrication, production et distribution de produits chimiques, Industrie manufacturière, Recherche, Services TIC, Services postaux et de messagerie, Gestion des déchets (B2B), Production, transformation et distribution de produits alimentaires, Fournisseurs de services numériques.

Cf. Champ d'application et définition des entités concernées (Articles 1 à 7)

QORUM Secur'Num

Chimere est associé de Qorum Secur'Num, le guichet unique de la cybersécurité et de la conformité numérique. Avec plus de 450 experts cyber sur plus de 50 sites en France, Qorum Secur'Num peut vous accompagner sur tous les domaines dans votre démarche de mise en conformité avec la directive NIS 2.

Directive (UE) 2022/2555 sur EUR-Lex

La directive NIS 2 | ANSSI

Que contient la directive ?

Gestion des risques de cybersécurité (Article 18)

L'article exige des entités concernées qu'elles mettent en place une gestion des risques de cybersécurité intégrée, couvrant la prévention, la détection, et la réponse aux incidents de sécurité.

La directive insiste sur une approche proactive, recommandant l'évaluation régulière des risques de sécurité pour adapter les mesures de protection.

Politiques de gouvernance en cybersécurité (Article 20)

Cet article demande aux entités d'établir des politiques de gouvernance adaptées, incluant des plans de continuité et de reprise d'activité pour garantir la résilience en cas de cyberincident.

Il exige également la formation en cybersécurité pour le personnel et le développement d'une culture de la sécurité au sein de l'organisation.

Mesures de cybersécurité spécifiques (Article 21)

Parmis les plus important, cet article liste des mesures techniques obligatoires telles que le contrôle d'accès, la sécurisation des communications et l'authentification, la gestion des vulnérabilités, et la sécurisation des réseaux et systèmes d'information.

L'article est décliné en 10 sous-points :

- 21.2.a Les politiques relatives à l'analyse des risques et à la sécurité des systèmes d'information
- 21.2.b La gestion des incidents
- 21.2.c La continuité des activités, par exemple la gestion des sauvegardes et la reprise des activités, et la gestion des crises
- 21.2.d La sécurité de la chaîne d'approvisionnement, y compris les aspects liés à la sécurité concernant les relations entre chaque entité et ses fournisseurs ou prestataires de services directs
- 21.2.e La sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information, y compris le traitement et la divulgation des vulnérabilités
- 21.2.f Les politiques et des procédures pour évaluer l'efficacité des mesures de gestion des risques en matière de cybersécurité
- 21.2.g Les pratiques de base en matière de cyberhygiène et la formation à la cybersécurité
- 21.2.h Les politiques et des procédures relatives à l'utilisation de la cryptographie et, le cas échéant, du chiffrement
- 21.2.i La sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs
- 21.2.j L'utilisation de solutions d'authentification à plusieurs facteurs ou d'authentification continue, de communications vocales, vidéo et textuelles sécurisées et de systèmes sécurisés de communication d'urgence au sein de l'entité, selon les besoins

Surveillance et détection des incidents (Article 22)

L'article exige la mise en place de mécanismes de détection et de suivi des incidents, incluant l'analyse des logs et l'implémentation de systèmes de détection d'intrusion.

Il nécessite notament un système de surveillance continue pour identifier rapidement les cybermenaces.

Notification des incidents (Article 23)

L'article 23 impose une obligation de notification rapide des incidents ayant un impact significatif sur la continuité des services, dans un délai de 24 heures pour l'alerte initiale et un rapport final dans les 30 jours.

Audits de cybersécurité et évaluation de conformité (Article 24)

Finalement, les entités doivent se soumettre à des audits réguliers pour évaluer leur conformité aux exigences de sécurité.

Découvrez comment Chimere peut vous faciliter votre mise en conformité !

https://chimere.eu/fr/chimere-nis2/ contact@chimere.eu

A propos de Chimere.

Chimere est une solution de Zero Trust Network Access française et européenne. Entrez dans la nouvelle ère de l'accès distant sécurisé.