Référentiels et normes en sécurité des systèmes d'information

Les **référentiels et normes en sécurité des systèmes d'information** désignent l'ensemble des standards, directives et bonnes pratiques établis pour assurer la protection, la confidentialité, et l'intégrité des informations au sein des systèmes informatiques. Ils fournissent un cadre structuré pour la gestion des risques liés à la sécurité des données, la conformité aux exigences légales, et l'amélioration continue des processus de sécurité. Ces normes sont utilisées par les organisations pour définir des politiques de sécurité, mettre en place des contrôles adaptés, et garantir la résilience face aux menaces et aux vulnérabilités informatiques.

- Directive Européenne NIS 2

Directive Européenne NIS 2

Publications Office (europa.eu)

La directive NIS2 (Network and Information Security) vise à renforcer la cybersécurité au sein de l’Union européenne. Publiée en décembre 2022, elle remplace la directive NIS1 et élargit son champ d’application pour inclure davantage d’entités critiques12.

Voici les principaux points de la directive NIS2 :

- Renforcement des mesures de sécurité : Les entités critiques doivent mettre en place des mesures de sécurité appropriées pour protéger leurs systèmes d’information2.
- Obligation de signalement : Les incidents de cybersécurité doivent être signalés aux autorités compétentes3.
- Coopération accrue : Les États membres doivent collaborer plus étroitement pour gérer les crises cybernétiques, notamment via le réseau CyCLONe1.
- Extension du périmètre : La directive s’applique désormais à un plus grand nombre de secteurs, y compris l’énergie, les transports, la santé, et les infrastructures numériques2.

Cette directive vise à améliorer la résilience des infrastructures critiques face aux cybermenaces croissantes.