L'application de la directive NIS 2 et l'obligation de sécurisation des infrastructures

Avec la transposition en droit français de la directive européenne NIS 2 (prévue au plus tard en octobre 2024 et applicable dès 2025), la pression sur la sécurité des infrastructures d'entreprise change radicalement. Des sources spécialisées (LeMagIT, Solutions Numériques) et les communications de l'ANSSI insistent sur le changement d'échelle : la directive ne concerne plus seulement les "Opérateurs de Services Essentiels" (OSE) mais s'étend à des milliers de PME et ETI classées "Entités Essentielles" (EE) ou "Importantes" (EI). Cette nouvelle réglementation impose une gestion des risques basée sur des mesures techniques concrètes et non plus seulement sur des intentions.

L'Article 21 de la directive liste des exigences strictes : obligation de mettre en œuvre des solutions d'authentification multifacteur (MFA), sécurisation des réseaux, gestion rigoureuse des correctifs et, de manière critique, sécurisation de la chaîne d'approvisionnement. Cela signifie que l'entreprise devient responsable de la sécurité des logiciels et services tiers qu'elle intègre, forçant l'administrateur à auditer ses fournisseurs et à durcir les accès externes.

Le risque n'est plus seulement opérationnel, il devient légal et financier, avec des sanctions lourdes et une responsabilité accrue des dirigeants. De plus, NIS 2 impose des délais stricts de notification d'incident (une alerte sous 24h à l'ANSSI). Pour s'y préparer, la priorité est de renforcer la détection (via SIEM ou XDR), de généraliser le MFA sur les accès VPN et admin, et d'appliquer une segmentation réseau stricte pour limiter la propagation en cas d'intrusion.

https://cyber.gouv.fr/la-directive-nis-2

https://solutions.lesechos.fr/juridique/loi-conformite/nis2-ce-que-la-nouvelle-directive-europeenne-change-pour-votre-entreprise/