NIS2 et résilience télécom : quelles exigences pour les OIV et collectivités après le cuivre ?

La migration hors du cuivre coïncide avec une autre transformation majeure : le renforcement des obligations de cybersécurité porté par la directive européenne NIS2. Pour les opérateurs d'importance vitale et, plus largement, pour un grand nombre d'organisations, ces deux mouvements se rejoignent sur un même terrain, celui de la résilience des communications. Basculer la voix et les données sur des réseaux IP, tout en devenant assujetti à des exigences de sécurité renforcées, impose de penser la migration non seulement sous l'angle de la continuité de service, mais aussi sous celui de la sécurité. Cet article éclaire cette articulation, en restant sur les principes et en renvoyant à une expertise dédiée pour la conformité.

Ce qu'est la directive NIS2

La directive NIS2, adoptée fin 2022, vise à assurer un niveau élevé et commun de cybersécurité dans l'Union européenne. Elle élargit considérablement le périmètre de la première directive NIS : là où celle-ci ne concernait qu'environ cinq cents entités en France, NIS2 devrait s'appliquer à plusieurs milliers d'organisations, réparties dans dix-huit secteurs d'activité. Elle distingue deux catégories d'assujettis, les entités essentielles et les entités importantes, selon la criticité du secteur et la taille de l'organisation, avec des exigences graduées. En France, la transposition s'opère via un projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité, dont le processus législatif s'est poursuivi en 2025 et 2026, l'ANSSI étant désignée comme autorité nationale de supervision.

Qui est concerné, et pourquoi les télécoms au premier chef

Le secteur des infrastructures numériques figure parmi les secteurs hautement critiques visés. Certaines entités sont concernées quelle que soit leur taille, et les opérateurs de communications électroniques en font partie. Les anciens opérateurs d'importance vitale et opérateurs de services essentiels basculent par ailleurs mécaniquement dans le nouveau dispositif. Point notable pour le secteur public, la transposition française inclut les collectivités

territoriales d'une certaine taille, communes importantes, départements, régions et leurs groupements, dans le périmètre. Ainsi, la migration télécom d'un opérateur critique, d'un grand établissement ou d'une collectivité s'inscrit désormais dans un cadre où la sécurité des systèmes de communication n'est plus une option mais une obligation réglementaire.

Le lien entre fin du cuivre et résilience

La bascule vers l'IP change la nature des risques. Le réseau cuivre analogique, techniquement rudimentaire, présentait une forme de robustesse propre : autonomie électrique par télé-alimentation, faible surface d'exposition numérique. En passant à des communications transportées sur IP, sur des réseaux mutualisés et interconnectés, l'organisation gagne en fonctionnalités mais s'expose à des risques nouveaux, indisponibilité en cas de panne réseau ou électrique, attaques informatiques, fraude téléphonique. La résilience, entendue comme la capacité à maintenir le service face aux incidents, devient un objet de conception à part entière. C'est précisément ce que la logique NIS2 impose de prendre en compte : anticiper les défaillances, sécuriser les accès, garantir la continuité.

Les grands types d'exigences

Sans entrer dans le détail technique, qui relève de référentiels spécialisés, les obligations issues de NIS2 s'organisent autour de quelques axes. La gouvernance de la sécurité, avec une politique formalisée et une implication de la direction, dont la responsabilité peut être engagée. La gestion des risques, incluant la sécurisation des accès, le chiffrement des communications, la maîtrise de la chaîne d'approvisionnement. La détection et le traitement des incidents, avec une obligation de notification à l'autorité selon des délais encadrés. La résilience et la continuité, à travers des plans de reprise et de continuité d'activité. En France, l'ANSSI a diffusé un référentiel définissant des objectifs de sécurité assortis de moyens de conformité, avec un principe de proportionnalité selon la catégorie d'entité.

Concevoir sa migration à l'aune de la résilience

Pour une organisation concernée, la conséquence pratique est de traiter la migration télécom et la conformité cybersécurité comme deux faces d'un même projet. Cela signifie intégrer, dès la conception de la nouvelle architecture, les exigences de continuité : secours électrique des équipements critiques, redondance des accès pour les sites sensibles, solution de secours mobile, sécurisation de la téléphonie IP contre la fraude. Cela signifie aussi documenter et gouverner ces choix, plutôt que de les traiter comme de simples paramètres techniques. La fin du cuivre offre une opportunité : plutôt que de reconstruire à l'identique, elle permet de bâtir

une infrastructure pensée d'emblée pour la résilience, en cohérence avec les attentes réglementaires.

Une réserve importante

La conformité NIS2 est un sujet complexe, en cours de stabilisation réglementaire, et dont le périmètre exact dépend du secteur et de la taille de chaque organisation. Le calendrier de transposition et les référentiels techniques ont continué d'évoluer, et l'assujettissement précis d'une entité donnée doit être vérifié au regard des textes en vigueur. Cet article se limite à éclairer l'articulation entre fin du cuivre et résilience ; il ne constitue pas un guide de conformité. Toute organisation susceptible d'être concernée gagne à faire évaluer sa situation par un spécialiste de la cybersécurité et à s'appuyer sur les ressources officielles de l'ANSSI, sans attendre la finalisation complète du cadre.

En synthèse

La fin du cuivre et la directive NIS2 convergent sur la résilience des communications. En basculant vers l'IP, les organisations, et notamment les opérateurs critiques et les collectivités, s'exposent à de nouveaux risques que NIS2 impose précisément d'anticiper. La bonne approche consiste à concevoir la migration en intégrant d'emblée continuité électrique, redondance, secours et sécurité, plutôt que de reconstruire à l'identique. Compte tenu de la complexité et de l'évolution du cadre, l'appui d'une expertise en cybersécurité et le recours aux ressources de l'ANSSI sont vivement recommandés pour les entités concernées.

Cet article présente un cadre général à visée d'information et ne constitue pas un avis juridique ni un guide de conformité. Le cadre NIS2 est en cours de stabilisation ; l'assujettissement et les obligations doivent être vérifiés au regard des textes en vigueur avec l'appui d'un spécialiste. Sources : directive (UE) 2022/2555 ; ANSSI (dont le Référentiel Cyber France) ; travaux parlementaires sur le projet de loi résilience ; analyses de la filière cybersécurité.

Pour aller plus loin

- Résilience de la voix sur IP : que se passe-t-il en cas de coupure ?
- Fibre, 4G ou satellite : choisir le bon accès pour chaque site
- Rétroplanning type d'un projet de migration télécom sur 18 mois

Concerné par la fin du cuivre sur vos sites ?

AILERYS Conseil vous accompagne de bout en bout : audit de votre parc, choix des accès et des opérateurs, pilotage de la migration.

Échanger avec un expert : https://finducuivre.info/contact/

À lire aussi dans ce dossier

- Sécuriser sa téléphonie IP : fraude téléphonique (toll fraud) et parades
- RGPD et téléphonie IP : les obligations liées à la voix sur IP
- Le RIO comme outil de diagnostic : identifier une ligne analogique par la commande 3179
- La fin du cuivre en outre-mer : échéances et particularités pour les DROM

Article révisé le 19 août 2026 par FinDuCuivre.info
https://finducuivre.info/nis2-resilience-telecom-oiv-collectivites-fin-cuivre-cybersecurite/