MY TRUST PARTNER

Cybersecurite - Conformite - IA

Guide de conformite NIS2 pour les ETI

Perimetre, obligations, roadmap 18 mois et sanctions

LIVRE BLANC MTP 2026

www.mytrustpartner.fr - contact@mytrustpartner.fr - +33 1 84 16 05 27

Sommaire

1. Introduction : pourquoi NIS2 concerne les ETI

Un changement de paradigme reglementaire

La directive NIS2 (Network and Information Security 2) transposee en droit francais en octobre 2024 elargit considerablement le perimetre de la reglementation europeenne en matiere de cybersecurite. La precedente directive NIS concernait environ 500 entreprises francaises. NIS2 en concerne plus de 10 000, dont une grande majorite d'ETI jusque-la en dehors de tout cadre cyber contraignant.

De qui parle-t-on ?

Sont concernees les entreprises de plus de 50 salaries ou plus de 10 millions d'euros de chiffre d'affaires, des lors qu'elles operent dans l'un des 18 secteurs vises : energie, transport, sante, finance, infrastructures numeriques, services publics, espace, administration publique, eau, dechets, chimie, alimentaire, industrie manufacturiere critique, recherche, services postaux, services numeriques, fournisseurs de services geres. Deux categories : Entites Essentielles (EE) et Entites Importantes (EI), avec des obligations differenciees.

Les enjeux financiers

Les sanctions peuvent atteindre 10 millions d'euros ou 2 % du chiffre d'affaires mondial pour les EE, 7 millions d'euros ou 1,4 % pour les EI. Au-dela des amendes, la directive introduit la responsabilite personnelle des dirigeants en cas de manquement grave : suspension temporaire, interdiction d'exercer certaines fonctions de direction. L'ANSSI est l'autorite nationale competente.

2. Les 10 mesures de cyberhygiene obligatoires

Analyse des risques et politique de securite

Mettre en place une analyse des risques formalisee (methode EBIOS RM recommandee), avec revue annuelle minimum. Une politique de securite de l'information documentee, approuvee par la direction, communiquee a tous les collaborateurs et sous-traitants critiques.

Gestion des incidents

Plan de reponse aux incidents cyber (PRI) ecrit et teste annuellement. Obligation de notification a l'ANSSI dans un delai de 24 heures pour une alerte precoce, 72 heures pour un rapport detaille, 1 mois pour un rapport final. Pseudo-incidents (tentatives d'attaque detectees) egalement concernes.

Continuite d'activite

PCA/PRA documente, incluant les systemes critiques, les donnees sensibles, les interlocuteurs cles. Sauvegardes testees regulierement selon la regle 3-2-1 (3 copies, 2 supports differents, 1 hors site). Objectifs de RPO et RTO definis par activite.

Securite de la chaine d'approvisionnement

Cartographie des fournisseurs critiques, clauses contractuelles cyber (niveau de securite minimum, droit d'audit, notification d'incident), revue annuelle des risques tiers. Les fournisseurs de services cyber, cloud, maintenance IT sont particulierement cibles.

Securite du developpement et des acquisitions

Si developpement interne : SDLC securise (revues de code, SAST/DAST, gestion des vulnerabilites). Si achats : clauses de securite dans les cahiers des charges, tests d'intrusion a la livraison pour les solutions critiques.

Evaluation de l'efficacite

Indicateurs cles (KPI) de securite mesures regulierement : taux de patch, temps moyen de detection (MTTD), temps moyen de remediation (MTTR), resultats des phishing tests, couverture EDR, conformite des comptes privilegies.

Formation et sensibilisation

Formation cyber obligatoire pour les dirigeants. Sensibilisation annuelle de tous les collaborateurs. Programmes cibles pour les populations a risque (comptabilite, RH, DSI, direction). Les prestataires labellises SecNumEdu-FC par l'ANSSI sont recommandes.

Cryptographie

Politique de chiffrement documentee. Donnees sensibles chiffrees au repos (AES-256) et en transit (TLS 1.2+). Gestion des cles formalisee avec rotation reguliere, stockage dans HSM ou KMS pour les environnements critiques.

Controle d'acces et gestion des identites

Authentification multi-facteurs (MFA) obligatoire pour les acces administrateur et acces distants. Principe du moindre privilege. Revue trimestrielle des comptes actifs. Deprovisionning sous 24h apres depart. Journalisation des acces privilegies.

Securite des communications et reseaux

Segmentation reseau, pare-feu nouvelle generation avec IPS, DNS filtering, VPN pour les acces distants. EDR/XDR sur les endpoints. Solution anti-spam et DMARC/SPF/DKIM configures sur la messagerie.

3. Notification des incidents : les 3 delais a retenir

24 heures - Alerte precoce

Des lors qu'un incident est suspecte d'avoir un impact significatif, une alerte precoce doit etre envoyee a l'ANSSI sous 24 heures. Elle contient les informations preliminaires : nature presumee, systemes affectes, mesures prises. Pas besoin d'attendre d'avoir tous les details.

72 heures - Rapport d'incident

Rapport detaille avec evaluation initiale de l'impact, IOC (indicateurs de compromission), mesures de remediation engagees, communication prevue (clients, partenaires, grand public).

30 jours - Rapport final

Analyse complete : causes racines, impact definitif, actions correctives mises en place, lecons apprises. Ce rapport alimente la base de connaissances ANSSI pour le benefice collectif.

4. Gouvernance et responsabilite des dirigeants

Un sujet de direction generale

NIS2 impose la formation cyber des dirigeants. Le conseil d'administration doit valider la strategie cyber et suivre sa mise en oeuvre. Un comite cyber dedie ou inclus dans le comite des risques est recommande. Reporting trimestriel minimum.

Responsabilite personnelle

En cas de manquement grave, les dirigeants peuvent etre suspendus temporairement de leurs fonctions par l'autorite competente. L'excuse de l'ignorance n'est plus opposable : la directive presuppose que les dirigeants prennent leurs responsabilites.

Nomination d'un responsable cyber

Bien que NIS2 n'impose pas formellement un RSSI, la taille des ETI concernees rend cette nomination quasi-indispensable. Options : RSSI interne, RSSI externalise (CISO as a Service), DSI avec mandat cyber etendu.

Documentation attendue

Politique de securite, analyse des risques, cartographie des assets critiques, procedures de reponse a incident, PCA/PRA, registre des traitements, plan de formation, tableaux de bord. Cette documentation doit etre a jour et accessible en cas de controle.

5. Roadmap type sur 18 mois

Phase 1 - Diagnostic (mois 1 a 3)

Audit d'ecart NIS2 : identifier le positionnement (EE ou EI), cartographier les assets, analyser l'etat actuel vs les 10 mesures obligatoires, quantifier le gap. Livrables : rapport d'audit, plan d'action priorise, budget pluriannuel.

Phase 2 - Fondations (mois 4 a 9)

Mise en place des bases : politique de securite, PCA/PRA, MFA generalisee, EDR sur 100 % du parc, sauvegardes 3-2-1, formation dirigeants, programme de sensibilisation. Nomination du responsable cyber.

Phase 3 - Consolidation (mois 10 a 15)

Deploiement des mesures avancees : SOC managed ou interne, chiffrement generalise, segmentation reseau, SDLC securise, audit chaine approvisionnement, tests d'intrusion annuels. Premiere simulation d'incident.

Phase 4 - Maturite (mois 16 a 18)

Certification ISO 27001 ou HDS si pertinent, audit de conformite externe, integration dans le systeme de management qualite, preparation au controle ANSSI, amelioration continue.

6. Conclusion et accompagnement MTP

Un chantier structurant

NIS2 n'est pas qu'une obligation reglementaire, c'est l'occasion de structurer durablement la cybersecurite de l'ETI. Les entreprises qui s'y prennent tot beneficieront d'un avantage competitif (clients rassures, partenariats facilites, assurabilite cyber amelioree).

Notre accompagnement

My Trust Partner accompagne les ETI de bout en bout : diagnostic initial, plan de conformite, mise en oeuvre des 10 mesures, formation labellisee SecNumEdu-FC par l'ANSSI, SOC managed, CISO as a Service, reponse a incident. Contact : contact@mytrustpartner.fr, 01 84 16 05 27, www.mytrustpartner.fr

My Trust Partner

Cybersecurite - Conformite - IA

Labellise SecNumEdu-FC par l'ANSSI sur l'ensemble de notre catalogue formation.

Contact

www.mytrustpartner.fr
contact@mytrustpartner.fr
+33 1 84 16 05 27