

Directives NIS2

Résumé des objectifs de sécurité

February 11, 2025

1 Introduction

Ce document recense les vingt (20) objectifs de sécurité issus de la directive NIS2 tels que présentés par l'ANSSI. Chaque objectif inclut une brève description et souligne pourquoi il est important pour la protection globale des systèmes d'information.

2 Objectifs de sécurité NIS2

2.1 Objectif de sécurité 1 : Recensement des systèmes d'information

Brève description :

L'entité doit inventorier l'ensemble de ses systèmes d'information afin d'avoir une vision exhaustive de ses actifs numériques.

Pourquoi c'est important ?

Cela permet de connaître précisément les ressources à protéger et d'identifier les vulnérabilités potentielles.

2.2 Objectif de sécurité 2 : Cadre de gouvernance de la sécurité numérique

Brève description :

Mettre en place un cadre de gouvernance structuré qui définit les responsabilités, les politiques et les procédures en matière de cybersécurité.

Pourquoi c'est important ?

Cela garantit une organisation claire, un pilotage unifié et une responsabilisation effective de chaque acteur.

2.3 Objectif de sécurité 3 : Approche par les risques

Brève description :

Adopter une démarche basée sur l'identification, l'analyse et la gestion des risques afin de prioriser les actions de sécurité.

Pourquoi c'est important ?

Une bonne évaluation des risques aide à concentrer les ressources sur les menaces les plus critiques, optimisant ainsi la posture de sécurité.

2.4 Objectif de sécurité 4 : Maîtrise de l'écosystème

Brève description :

Comprendre et contrôler l'ensemble des interactions et dépendances entre les systèmes internes et l'environnement externe (fournisseurs, partenaires, etc.).

Pourquoi c'est important ?

Une faille peut provenir d'un partenaire ou d'un sous-traitant. Cartographier l'écosystème permet de limiter les risques de supply chain.

2.5 Objectif de sécurité 5 : Audit de la sécurité des systèmes d'information réglementés

Brève description :

Réaliser des audits réguliers pour vérifier la conformité des dispositifs de sécurité et identifier d'éventuelles vulnérabilités.

Pourquoi c'est important ?

Les audits permettent de mesurer l'efficacité des contrôles en place et de mettre en évidence des failles à corriger rapidement.

2.6 Objectif de sécurité 6 : Sécurité numérique dans la gestion des ressources humaines

Brève description :

Intégrer la cybersécurité dans la gestion des RH via la formation, la sensibilisation et des procédures adaptées pour les personnels.

Pourquoi c'est important ?

Le facteur humain est crucial : des collaborateurs formés et sensibilisés réduisent drastiquement les risques d'erreurs ou d'attaques réussies (phishing, etc.).

2.7 Objectif de sécurité 7 : Maîtrise des systèmes d'information réglementés

Brève description :

Exercer un contrôle strict et continu sur les systèmes soumis aux obligations réglementaires pour garantir leur sécurité.

Pourquoi c'est important ?

Les systèmes critiques doivent être surveillés de façon rapprochée pour éviter toute compromission pouvant impacter le cœur de l'activité.

2.8 Objectif de sécurité 8 : Maîtrise des accès physiques aux locaux

Brève description :

Mettre en place des mesures de sécurité physique (badges, surveillance, contrôles) pour restreindre l'accès aux infrastructures critiques.

Pourquoi c'est important ?

Une intrusion physique peut contourner la majorité des protections logicielles, rendant indispensable le verrouillage des locaux sensibles.

2.9 Objectif de sécurité 9 : Sécurisation de l'architecture des systèmes d'information réglementés

Brève description :

Concevoir une architecture sécurisée garantissant l'intégrité, la disponibilité et la confidentialité des données et des systèmes.

Pourquoi c'est important ?

Une architecture cloisonnée et robuste limite la propagation d'incidents et prévient les accès non autorisés.

2.10 Objectif de sécurité 10 : Sécurisation des accès distants aux systèmes d'information réglementés

Brève description :

Mettre en place des dispositifs (MFA, VPN, etc.) pour sécuriser les accès à distance, notamment en situation de télétravail.

Pourquoi c'est important ?

Les accès distants sont une cible de choix pour les attaquants. Les renforcer limite considérablement les risques d'intrusion externe.

2.11 Objectif de sécurité 11 : Protection contre les codes malveillants

Brève description :

Déployer des solutions de détection et de prévention pour se prémunir contre virus, ransomwares et autres malwares.

Pourquoi c'est important ?

Les codes malveillants sont à l'origine d'une large part des incidents de sécurité. Les prévenir est donc fondamental.

2.12 Objectif de sécurité 12 : Sécurisation de la configuration des ressources

Brève description :

Configurer de manière sécurisée les ressources (serveurs, applications, équipements) afin de limiter les vulnérabilités potentielles.

Pourquoi c'est important ?

Les configurations par défaut ou non maîtrisées laissent des failles qui peuvent être exploitées aisément par des attaquants.

2.13 Objectif de sécurité 13 : Gestion des identités et des accès

Brève description :

Mettre en place une gestion rigoureuse des identités et des droits d'accès pour s'assurer que seuls les utilisateurs autorisés accèdent aux systèmes critiques.

Pourquoi c'est important ?

Le contrôle d'accès est un pilier de la sécurité : un accès non autorisé permettrait à un intrus d'exfiltrer des données ou de saboter le système.

2.14 Objectif de sécurité 14 : Maîtrise de l'administration des systèmes d'information réglementés

Brève description :

Encadrer strictement l'administration des systèmes (accès, droits, journalisation) pour éviter tout usage malveillant ou abusif.

Pourquoi c'est important ?

Les comptes administrateurs disposent de droits étendus. Leur compromis entraînerait des conséquences majeures sur l'ensemble des SI.

2.15 Objectif de sécurité 15 : Réalisation des actions d'administration depuis des ressources dédiées

Brève description :

Effectuer les tâches d'administration à partir de postes ou environnements isolés des usages courants (navigation, mails, etc.).

Pourquoi c'est important ?

Un poste dédié réduit la surface d'attaque et empêche qu'un malware courant sur un poste utilisateur n'accède à des fonctions critiques.

2.16 Objectif de sécurité 16 : Supervision de la sécurité des systèmes d'information réglementés

Brève description :

Assurer une surveillance continue (journaux, alertes, corrélations d'événements) pour détecter rapidement toute anomalie.

Pourquoi c'est important ?

La détection précoce est essentielle pour réagir à un incident avant qu'il ne prenne de l'ampleur.

2.17 Objectif de sécurité 17 : Réaction aux incidents de sécurité

Brève description :

Être capable de détecter, analyser et réagir promptement aux incidents pour limiter leur impact et restaurer la sécurité.

Pourquoi c'est important ?

Un incident mal géré peut se transformer en crise et provoquer des dommages majeurs (pertes financières, atteinte à la réputation, etc.).

2.18 Objectif de sécurité 18 : Capacité de continuité et de reprise d'activité

Brève description :

Mettre en place des mécanismes et procédures de continuité (PCA/PRA) pour assurer la résilience en cas d'incident majeur.

Pourquoi c'est important ?

La possibilité de reprendre rapidement l'activité réduit l'impact opérationnel, financier et légal en cas de sinistre.

2.19 Objectif de sécurité 19 : Réaction aux crises d'origine cyber

Brève description :

Prévoir des procédures spécifiques pour gérer et résoudre les crises engendrées par des cyberattaques de grande ampleur.

Pourquoi c'est important ?

Une crise majeure nécessite une réponse coordonnée au niveau stratégique, opérationnel et de communication (interne/externe).

2.20 Objectif de sécurité 20 : Vérification des capacités opérationnelles

Brève description :

Tester régulièrement le fonctionnement des dispositifs de sécurité (exercices, simulations, pentests) afin de s'assurer de leur efficacité en situation réelle.

Pourquoi c'est important ?

Des mécanismes non testés risquent d'être inopérants le jour où un incident se produit, laissant l'organisation vulnérable.