Conformité, Sécurité

# NIS2 et cybersécurité Ce que les PME doivent anticiper

La directive NIS2 renforce les exigences de cybersécurité pour de nombreuses organisations publiques et privées. Toutes les PME ne seront pas directement concernées, mais beaucoup devront progresser rapidement : identification des risques, sauvegardes, mises à jour, gestion des accès, prestataires critiques, plan de réponse aux incidents.

Publié le 11 mai 2026

Ce qu’il faut retenir de ce dossier

La directive NIS2 est un texte européen destiné à élever le niveau de cybersécurité dans l’Union européenne. Elle remplace la première directive NIS et élargit fortement le périmètre des organisations concernées. L’ANSSI indique que cette extension est « sans précédent » en matière de réglementation cyber et invite les futures entités essentielles et importantes à engager dès maintenant une démarche de sécurisation cohérente avec NIS2.

Pour les PME, le premier repère est important : toutes les PME ne sont pas automatiquement soumises à NIS2. Le texte vise des entités appartenant à des secteurs critiques ou importants. La règle générale s’apprécie notamment à partir du seuil de moyenne entreprise, en pratique autour de 50 salariés ou de 10 millions d’euros de chiffre d’affaires ou de bilan annuel, avec des exceptions selon certains services et secteurs.

Le contexte français doit être lu avec prudence : la directive européenne prévoyait une transposition par les États membres au 17 octobre 2024, mais la transposition française a pris du retard. Cela ne doit pas conduire à attendre : l’ANSSI invite déjà les futures entités essentielles et importantes à engager une démarche cohérente avec NIS2.

Même lorsqu’une PME n’est pas directement assujettie, NIS2 peut avoir un effet indirect. Un prestataire, un sous-traitant, un hébergeur, un infogérant, un éditeur logiciel ou un fournisseur de services numériques peut se voir demander des garanties plus formalisées par ses clients.

Les mesures à anticiper sont concrètes : cartographier les actifs numériques, mieux gérer les accès, appliquer les mises à jour, sauvegarder et tester les restaurations, documenter les prestataires critiques, préparer la réponse à incident et sensibiliser les utilisateurs. Pour les entités concernées, les incidents importants s’inscrivent aussi dans une logique de notification rapide : alerte précoce sous 24 heures, notification sous 72 heures et rapport final sous un mois.

## Un sujet réglementaire, mais surtout un sujet de continuité d’activité

NIS2 est souvent présentée comme une contrainte réglementaire. Pour un dirigeant de PME, il est plus utile de la lire comme un signal : les autorités européennes considèrent désormais que la cybersécurité est une condition normale de fonctionnement des entreprises et des services essentiels.

L’ANSSI rappelle que la menace cyber augmente et que les systèmes d’information restent pour partie vulnérables. La directive NIS2 vise à permettre à des milliers d’entités de mieux se protéger, en élargissant les objectifs et le périmètre de la première directive NIS.

Un sujet de direction autant qu’un sujet techniqueLa sécurité numérique ne peut plus être traitée uniquement comme une affaire d’outils. Elle engage les accès, les prestataires, les sauvegardes, les délais de reprise, la communication en cas d’incident et la capacité de l’entreprise à poursuivre son activité.

Trois questions pour commencer

- Quels services numériques sont indispensables à l’activité quotidienne ?

- Quels prestataires disposent d’un accès technique au site, aux serveurs ou aux outils métier ?
- Combien de temps l’entreprise peut-elle fonctionner sans site, sans messagerie ou sans application métier ?

## NIS2 : de quoi parle-t-on exactement ?

La directive NIS2, ou Network and Information Security 2, a été publiée au Journal officiel de l’Union européenne en décembre 2022. Elle remplace la directive NIS1 et vise à renforcer le niveau commun de cybersécurité dans l’Union européenne.

Son principe général est de demander aux organisations concernées de mieux gérer leurs risques numériques, de renforcer leurs mesures de sécurité, de notifier certains incidents et de s’inscrire dans un cadre de supervision plus structuré.

Contexte français

La directive imposait aux États membres d’adopter et publier les dispositions de transposition au plus tard le 17 octobre 2024, pour une application à partir du 18 octobre 2024. En France, le texte national de transposition a pris du retard ; les entreprises doivent donc suivre les publications de l’ANSSI et raisonner en trajectoire de préparation plutôt qu’en conformité déclarative improvisée.

1Gérer les risques

Identifier les actifs, les dépendances, les menaces et les mesures de protection prioritaires.

2Renforcer la sécurité

Mettre en place des mesures techniques et organisationnelles adaptées au niveau d’exposition.

3Savoir réagir

Préparer la détection, la qualification, la notification et la gestion des incidents significatifs.

Repère simple : NIS2 ne consiste pas à acheter un outil unique. Le texte pousse les organisations concernées à démontrer qu’elles connaissent leurs risques, qu’elles appliquent des mesures adaptées et qu’elles savent réagir en cas d’incident.

## Toutes les PME sont-elles concernées ?

Non. Il faut éviter deux erreurs : penser que NIS2 ne concerne que les très grandes organisations, ou penser à l’inverse que toutes les PME seront automatiquement soumises au texte.

L’ANSSI parle de futures entités essentielles et entités importantes. Elle met à disposition MonEspaceNIS2 pour aider les organisations à évaluer si elles sont concernées.

Les seuils ne suffisent pas, mais ils donnent un premier repèreLa directive s’appuie en règle générale sur les catégories d’entreprises européennes. Une organisation peut entrer dans le périmètre à partir du seuil de moyenne entreprise, souvent résumé à 50 salariés ou 10 millions d’euros de chiffre d’affaires ou de bilan annuel, sous réserve d’appartenir à un secteur visé. Certaines entités peuvent toutefois être concernées indépendamment de leur taille, notamment selon la nature du service rendu.

| Situation | Ce que cela signifie | Action prioritaire |
| --- | --- | --- |
| Entreprise directement concernée | L’entreprise entre dans le périmètre des entités essentielles ou importantes, selon son activité, sa taille, son rôle ou une règle spécifique applicable à certains services. | Utiliser MonEspaceNIS2, vérifier les seuils et exceptions, puis préparer une trajectoire de sécurisation. |
| Entreprise concernée indirectement | L’entreprise est prestataire, sous-traitante ou fournisseur d’une organisation qui devra renforcer ses exigences cyber. | Préparer une documentation simple : accès, sauvegardes, sécurité, continuité, contacts d’urgence. |
| Entreprise non assujettie | L’entreprise n’entre pas dans le périmètre identifié, mais reste exposée aux risques numériques ordinaires. | Appliquer les bonnes pratiques de sécurité et traiter les risques les plus probables. |

Point de vigilance

La question n’est pas seulement “sommes-nous concernés par le texte ?”. Elle est aussi “nos clients, donneurs d’ordre ou partenaires vont-ils nous demander de prouver notre niveau de sécurité ?”.

## Ce que NIS2 change dans la relation avec les prestataires

Pour une PME, l’un des effets les plus visibles de NIS2 sera probablement la montée des exigences envers les prestataires numériques. Les organisations concernées devront mieux maîtriser leurs dépendances et vérifier davantage leurs fournisseurs.

Cette logique peut concerner les hébergeurs, infogérants, agences web, éditeurs logiciels, prestataires cloud, plateformes e-commerce, services de messagerie, sauvegarde ou supervision.

?Accès techniques

Les accès prestataires doivent être connus, nominatifs lorsque c’est possible, limités et supprimés lorsqu’ils ne sont plus nécessaires.

?Responsabilités

Chaque acteur doit savoir ce qu’il prend en charge : hébergement, maintenance, supervision, sauvegardes, restauration ou support.

?Documentation

Un socle documentaire simple facilite les échanges avec les clients : périmètre, mesures de sécurité, sauvegardes, contacts d’urgence.

?Incident

Les délais d’alerte, d’intervention, de restauration et de communication doivent être clarifiés avant la crise.

## Délais de notification et sanctions : les repères à connaître

Pour les entités essentielles ou importantes, NIS2 ne se limite pas à la prévention. Le texte européen organise aussi la manière de signaler un incident important et fixe un cadre de sanctions en cas de manquement aux obligations de gestion des risques ou de notification.

| Repère | Ce que prévoit la directive européenne | Lecture PME |
|---|---|---|
| Alerte précoce | Sans retard injustifié et, en tout état de cause, dans les 24 heures après connaissance d’un incident important. | Il faut savoir qui qualifie l’incident et qui déclenche l’alerte. |
| Notification d’incident | Sans retard injustifié et, en tout état de cause, dans les 72 heures, avec une première évaluation de la gravité et de l’impact. | Les journaux, contacts et informations techniques doivent être disponibles rapidement. |
| Rapport final | Au plus tard un mois après la notification, ou après le traitement de l’incident s’il est encore en cours. | La gestion de crise doit laisser des traces exploitables. |
| Sanctions maximales | Jusqu’à 10 millions d’euros ou 2 % du chiffre d’affaires mondial pour les entités essentielles ; jusqu’à 7 millions d’euros ou 1,4 % pour les entités importantes. | Les montants exacts et modalités relèvent du cadre national, mais la directive rend le sujet stratégique pour la direction. |

Repère neutre

Ces chiffres ne signifient pas qu’une PME non assujettie serait automatiquement exposée à ces sanctions. Ils montrent en revanche que les organisations concernées devront traiter la cybersécurité comme un sujet de gouvernance, pas seulement comme une maintenance technique.

## Les 8 chantiers de cybersécurité à anticiper

Les recommandations générales de l’ANSSI convergent avec les mesures de base attendues dans une démarche de sécurisation : mises à jour, authentification forte, sauvegardes, protection de la messagerie, principe du moindre privilège et bonnes pratiques utilisateurs.

1. 01Cartographier les actifs numériquesIdentifier les noms de domaine, hébergements, sites, messageries, comptes administrateurs, outils métier, sauvegardes et prestataires ayant accès aux systèmes.
2. 02Sécuriser les accèsSupprimer les comptes inutilisés, éviter les comptes partagés, activer la double authentification lorsque c’est possible et limiter les privilèges.
3. 03Maintenir les outils à jourSuivre les mises à jour du CMS, des extensions, du thème, du serveur, de PHP et des composants techniques utilisés.
4. 04Sauvegarder et tester la restaurationVérifier la fréquence, la conservation, l’emplacement, la protection et la capacité réelle à restaurer les fichiers et la base de données.
5. 05Protéger la messagerieRenforcer la vigilance face au phishing, activer la double authentification et vérifier les réglages de domaine utiles à la délivrabilité et à l’anti-usurpation.

6. 06Préparer la réponse à incidentDéfinir qui alerte, qui coupe les accès, qui restaure, qui communique, qui conserve les traces et qui décide de la remise en ligne.

7. 07Maîtriser les prestatairesClarifier les responsabilités, les contacts, les délais d'intervention, les accès conservés et les conditions de réversibilité.

8. 08Sensibiliser les utilisateursFormer les équipes aux risques courants : phishing, mots de passe, pièces jointes, séparation des usages et signalement rapide d'un incident.

## Ce que cela signifie pour un site WordPress, WooCommerce ou un site métier

Le CMS utilisé n'est pas le critère principal. Ce qui compte est le rôle du site dans l'activité : visibilité commerciale, collecte de formulaires, e-commerce, espace client, outil métier ou dépendance à des connecteurs externes.

| Type de site | Risques principaux | Points à vérifier |
|---|---|---|
| Site vitrine | Défiguration, spam, injection de contenu, fuite de données de formulaires, indisponibilité. | Mises à jour, accès, sauvegardes, anti-spam, supervision, propriété du domaine. |
| Site e-commerce | Interruption de commandes, comptes clients exposés, emails transactionnels bloqués, connecteurs sensibles. | Maintenance WooCommerce, sauvegardes fréquentes, paiement, journaux, délivrabilité email, capacité de restauration. |
| Application métier ou portail client | Accès non autorisé, perte de données opérationnelles, indisponibilité d'un processus critique. | Droits utilisateurs, sauvegardes, journalisation, cloisonnement, procédure d'incident, tests de reprise. |
| Hébergement et infogérance | Serveur non maintenu, absence de supervision, sauvegardes insuffisantes, dépendance mal documentée. | Monitoring, correctifs serveur, sauvegardes hors production, délai d'intervention, restauration testée. |

Repère pour dirigeants

Un site web professionnel doit être regardé comme un actif de l'entreprise. Plus il intervient dans les ventes, les données ou les échanges clients, plus il doit être intégré au plan de sécurité et de continuité.

## Les erreurs à éviter

- ?Attendre pour commencerLes mesures de base sont déjà connues : accès, sauvegardes, mises à jour, prestataires, réponse à incident. Elles sont utiles même hors obligation directe.
- ?Chercher une réponse uniquement juridiqueNIS2 est un texte réglementaire, mais sa mise en œuvre repose sur des réalités techniques, organisationnelles et contractuelles.
- ?Acheter un outil avant d'avoir fait l'inventaireAvant de choisir une solution, il faut savoir ce que l'on protège, qui y accède, où sont les données et quels scénarios sont les plus critiques.
- ?Oublier les prestatairesUn prestataire qui conserve un accès administrateur, une ancienne agence qui détient un compte ou une sauvegarde mal localisée peuvent devenir des points faibles.

- ?Confondre sauvegarde et continuité d’activitéAvoir une sauvegarde ne suffit pas. Il faut connaître le délai de restauration, la qualité de la sauvegarde et la date du dernier test.
- ?Découvrir les délais d’alerte le jour de l’incidentPour les entités concernées, la logique 24 h / 72 h impose de préparer les rôles, les contacts et les informations utiles avant la crise.

## Checklist pratique pour une PME

1Vérifier l’exposition NIS2

Utiliser les ressources officielles de l’ANSSI, notamment MonEspaceNIS2, pour évaluer l’exposition de l’entreprise.

2Identifier les services critiques

Site, messagerie, boutique, CRM, facturation, stockage documentaire, sauvegardes, accès cloud.

3Contrôler les accès

Comptes administrateurs, anciens utilisateurs, MFA, droits minimaux, accès prestataires.

4Vérifier les mises à jour

CMS, extensions, thèmes, version PHP, composants serveur et bibliothèques utilisées.

5Auditer les sauvegardes

Fréquence, stockage, conservation, sécurité, restauration réelle des fichiers et de la base.

6Documenter les prestataires

Rôles, responsabilités, contacts d’urgence, délais d’intervention, réversibilité.

7Préparer l’incident

Décision, intervention, communication, restauration, conservation des traces et, si l’entreprise est concernée, capacité à respecter les jalons 24 h / 72 h.

8Sensibiliser les équipes

Phishing, mots de passe, pièces jointes, usages personnels/professionnels, signalement.

## Ce que les lecteurs demandent souvent

### NIS2 concerne-t-elle toutes les PME ?

### Faut-il attendre avant d’agir ?

### Une certification est-elle obligatoire ?

### Un site WordPress est-il concerné ?

### Que demander à son prestataire web ?

### Une sauvegarde quotidienne suffit-elle ?

### Quels délais de notification faut-il retenir ?

### Les sanctions s’appliquent-elles immédiatement à toutes les PME ?

## Conclusion

Pour une PME, NIS2 ne doit pas être abordée comme une contrainte isolée ou comme un sujet réservé aux grandes organisations. C’est un cadre qui confirme une évolution déjà engagée : les entreprises doivent mieux connaître leurs dépendances numériques, protéger leurs accès, documenter leurs prestataires, tester leurs sauvegardes et préparer leur réaction en cas d’incident.

Le bon point de départ n’est pas de tout sécuriser en une fois. Il consiste à identifier les risques les plus concrets : un site non maintenu, une messagerie exposée, des comptes administrateurs partagés, des sauvegardes jamais testées, un prestataire qui conserve des accès anciens, une absence de procédure en cas de compromission.

Un diagnostic court peut suffire à classer les priorités : ce qui doit être corrigé immédiatement, ce qui peut être planifié, ce qui relève du prestataire web, ce qui relève de l’informatique interne et ce qui doit être arbitré par la direction.

## Sources


- ANSSI, La directive NIS 2 : présentation de la directive, du changement de périmètre, de MonEspaceNIS2 et du Référentiel Cyber France.
- ANSSI, 10 règles d’or en matière de sécurité numérique : bonnes pratiques sur les mises à jour, l’authentification, la messagerie, les sauvegardes et les privilèges.
- MesServicesCyber, NIS2 : accès aux services et ressources de l’ANSSI et de ses partenaires.
- EUR-Lex, Directive (UE) 2022/2555 : texte européen de référence, notamment seuils, transposition, notification des incidents et sanctions.