« Mon client me demande NIS2 » : guide pour les fournisseurs

Vous n'êtes pas soumis à NIS2, mais un client vous envoie un questionnaire de sécurité ou de nouvelles clauses contractuelles. Voici pourquoi, et comment répondre sereinement.

NIS2 Aware · nis2aware.eu · novembre 2026

Pourquoi votre client vous interroge

Les organisations soumises à NIS2 doivent gérer la sécurité de leur **chaîne d'approvisionnement**. Une grande partie des incidents commence chez un fournisseur : un prestataire informatique piraté, une mise à jour logicielle compromise, le mot de passe volé d'une société de maintenance. Votre client doit donc évaluer la sécurité des fournisseurs dont il dépend, et vous en faites partie.

Ce qu'il peut vous demander

- Un **questionnaire de sécurité** (souvent 20 à 100 questions) sur vos mesures.
- Des **clauses contractuelles** : mesures minimales, notification des incidents dans un délai court, droit d'audit, confidentialité.
- Des **preuves** : une auto-évaluation ou une vérification CyberFundamentals, un certificat ISO/IEC 27001, un résumé de votre politique de sécurité.
- Des mesures précises : **authentification multifacteur**, sauvegardes, mises à jour rapides, accès limité à ses systèmes.
- Un **contact sécurité** nommé, joignable en cas d'incident.

Comment répondre

1. **Ne paniquez pas et ne promettez pas trop.** Répondez honnêtement : « en place », « en cours (pour telle date) » ou « non applicable ». Un plan crédible vaut mieux qu'un oui sans fondement.
2. **Lisez attentivement les clauses** avant de signer : délais de notification, responsabilité, droit d'audit. Faites-les vérifier si nécessaire.
3. **Rassemblez vos réponses en un seul endroit**, pour pouvoir les réutiliser avec le prochain client.

4. **Faites-en un atout :** un fournisseur qui répond clairement et rapidement inspire confiance et remporte des contrats.

Votre plan d'action en 30 jours

Semaine	Actions
1	Désignez un contact sécurité. Activez l'authentification multifacteur sur la messagerie et l'accès à distance.
2	Vérifiez vos sauvegardes : au moins une copie hors ligne ou immuable, et testez une restauration. Activez les mises à jour automatiques.
3	Supprimez les droits administrateur inutiles. Vérifiez que chaque appareil dispose d'un anti-malware à jour.
4	Rédigez une procédure d'incident d'une page, y compris la manière d'informer vos clients. Sensibilisez votre personnel à l'hameçonnage.

Étape suivante : le montrer

Le cadre **CyberFundamentals** du CCB comprend un niveau **Basic** adapté à de nombreuses petites entreprises. Une auto-évaluation selon CyFun Basic vous donne une réponse structurée à la plupart des questionnaires. Les outils sont disponibles sur atwork.safeonweb.be.

> **Testez-vous d'abord :** notre check de maturité express montre vos lacunes en cinq minutes.

Information générale sur le cadre NIS2 belge en date de novembre 2026, pas un avis juridique. Consultez toujours les dernières informations du CCB (ccb.belgium.be et atwork.safeonweb.be).