10 questions que votre conseil d'administration devrait poser sur la cybersécurité

Avec NIS2, l'organe de direction approuve et supervise les mesures de cybersécurité, et il peut être tenu responsable. Ces dix questions aident les administrateurs à vérifier si la cybersécurité est vraiment maîtrisée.

NIS2 Aware · nis2aware.eu · novembre 2026

1. Sommes-nous concernés par NIS2, et sommes-nous une entité essentielle ou importante ?

Pourquoi c'est important : Vos obligations, la supervision et les amendes en dépendent, et personne ne vous le dira : c'est à vous de l'évaluer.

Une bonne réponse : Une analyse documentée du secteur et de la taille, revue quand l'organisation change (acquisition, nouvelle activité).

2. Sommes-nous enregistrés auprès du CCB, et nos données sont-elles à jour ?

Pourquoi c'est important : L'enregistrement sur Safeonweb@Work est obligatoire, et le CCB utilise ces contacts en cas de crise.

Une bonne réponse : Un enregistrement confirmé, avec des contacts nommés qui font toujours partie de l'entreprise.

3. Quels sont nos cinq principaux risques cyber, et combien nous coûteraient-ils ?

Pourquoi c'est important : Le conseil ne peut pas superviser ce qu'il ne voit pas. Des risques exprimés en termes métier permettent de décider.

Une bonne réponse : Un registre des risques succinct, avec l'impact sur les opérations, le chiffre d'affaires et la réputation, mis à jour au moins une fois par an.

4. Quelles mesures avons-nous approuvées, et comment savons-nous qu'elles fonctionnent ?

Pourquoi c'est important : La direction doit approuver les mesures et superviser leur mise en œuvre. Approuver sans suivre ne suffit pas.

Une bonne réponse : Un plan de mesures avec des responsables et des échéances, et un reporting régulier avec quelques indicateurs simples.

5. Si un rançongiciel nous frappait demain, combien de temps nous faudrait-il pour redémarrer ?

Pourquoi c'est important : Les sauvegardes et la reprise font la différence entre une mauvaise semaine et une faillite.

Une bonne réponse : Des sauvegardes hors ligne ou immuables, une restauration testée et un délai de reprise réaliste pour les systèmes critiques.

6. Qui décide, et qui notifie le CCB dans les 24 heures ?

Pourquoi c'est important : L'alerte précoce est due dans les 24 heures. En pleine crise, on n'a pas le temps de chercher qui fait quoi.

Une bonne réponse : Une procédure d'incident écrite avec des noms, des numéros de téléphone et des pouvoirs de décision, testée lors d'un exercice.

7. Quels fournisseurs pourraient nous mettre à l'arrêt, et qu'exigeons-nous d'eux ?

Pourquoi c'est important : Beaucoup d'incidents commencent chez un fournisseur. NIS2 impose de gérer la sécurité de la chaîne d'approvisionnement.

Une bonne réponse : Une liste des fournisseurs critiques avec des clauses de sécurité, des obligations de notification et des contrôles périodiques.

8. L'authentification multifacteur est-elle activée partout où c'est important ?

Pourquoi c'est important : Les mots de passe volés sont la porte d'entrée la plus courante. La MFA bloque la plupart de ces attaques.

Une bonne réponse : La MFA sur la messagerie, l'accès à distance, les services cloud et tous les comptes administrateurs, sans exception.

9. La direction et le personnel ont-ils été formés, et pouvons-nous le prouver ?

Pourquoi c'est important : La formation de l'organe de direction est une obligation légale, et le personnel est la première ligne de défense.

Une bonne réponse : Une formation de la direction réalisée, un programme annuel de sensibilisation du personnel et des listes de présence.

10. Quels sont notre budget et notre feuille de route pour les 12 prochains mois ?

Pourquoi c'est important : La cybersécurité est un effort continu. Sans budget ni objectifs, elle reste sur papier.

Une bonne réponse : Un objectif (par exemple un niveau CyberFundamentals), une feuille de route et un budget approuvés par le conseil.

Comment l'utiliser : inscrivez deux ou trois questions à l'ordre du jour de chaque réunion du conseil, et demandez les réponses par écrit.

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).