Kiteworks

# Liste de vérification des meilleures pratiques pour la conformité NIS 2 pour les petites entreprises

Contrairement à la première directive NIS, le champ d›application de la directive NIS2 inclut désormais les petites et moyennes entreprises (PME) car elles jouent un rôle crucial dans la chaîne d›approvisionnement des services essentiels. Pour aider les PME à atteindre la conformité NIS2, voici quelques meilleures pratiques clés adaptées à leurs ressources et capacités :

- **1. Réaliser une évaluation des risques:** Identifiez les principaux actifs, les menaces potentielles et les vulnérabilités. Priorisez les risques en fonction de la probabilité et de l›impact potentiel, en utilisant des méthodologies telles que l›ISO/IEC 27005 ou les directives de l›ENISA.
- **2. Mettre en place un cadre de gouvernance de la cybersécurité:** Adoptez une version simplifiée des cadres existants (ISO/IEC 27001, NIST CSF) pour établir les rôles, responsabilités et politiques autour de la cybersécurité.
- **3. Former le personnel à la sensibilisation à la cybersécurité:** Éduquer régulièrement les employés sur les attaques par phishing, l›ingénierie sociale, la gestion des mots de passe et les pratiques sécurisées en ligne.
- **4. Assurez un contrôle d›accès et une authentification robustes:** Appliquez l›authentification multifactorielle (MFA) sur les systèmes clés. Limitez les privilèges des utilisateurs grâce à un modèle de moindre privilège pour réduire les menaces internes.
- **5. Développer un plan de réponse aux incidents:** Créez un plan de réponse aux incidents qui décrit les procédures de détection, de signalement et de réponse aux incidents de cybersécurité. Testez le plan à travers des exercices de simulation pour identifier les lacunes et les faiblesses.
- **6. Pratiquez la mise à jour régulière et la gestion des vulnérabilités:** Mettez en place des processus automatisés de gestion des mises à jour pour garantir que les systèmes et logiciels sont régulièrement actualisés. Utilisez des outils de scan de vulnérabilités pour identifier les faiblesses de sécurité.
- **7. Planifier la Continuité d›Activité et la Reprise après Sinistre (BC/DR):** Élaborez des plans BC/DR couvrant les systèmes clés et la récupération des données après un incident de sécurité. Testez régulièrement les processus de sauvegarde pour garantir que les données critiques peuvent être restaurées efficacement.
- **8. Surveillez et consignez l›activité réseau:** Mettez en place des outils de surveillance réseau pour détecter les activités inhabituelles. Conservez des journaux pour faciliter la détection des incidents et la conformité avec les exigences de déclaration sous NIS2.