Cyleme

Checklist cybersécurité PME

20 points de contrôle essentiels

Cochez chaque case à laquelle vous répondez « oui ». Chaque case non cochée est une porte d'entrée potentielle pour une attaque. Ces questions reprennent les contrôles que nous vérifions lors de notre audit gratuit d'une heure.

Identités et accès

- ☐ La double authentification (MFA) est-elle active sur tous les comptes (e-mail, outils métier, accès distants) ?
- ☐ Les comptes administrateurs sont-ils nominatifs, en nombre limité et distincts des comptes du quotidien ?
- ☐ Les mots de passe sont-ils gérés dans un coffre-fort dédié (ni fichier Excel, ni post-it, ni mot de passe réutilisé) ?
- ☐ Les accès d'un collaborateur qui part sont-ils coupés le jour même de son départ ?

Postes de travail

- ☐ Chaque poste dispose-t-il d'un antivirus nouvelle génération (détection comportementale), au-delà de l'antivirus classique ?
- ☐ Les mises à jour Windows / macOS et logicielles sont-elles appliquées automatiquement et suivies ?
- ☐ Le disque de chaque ordinateur est-il chiffré (BitLocker / FileVault), pour qu'un PC volé reste illisible ?
- ☐ Un pare-feu est-il actif sur chaque poste ?

Messagerie et navigation

- ☐ Un filtrage anti-phishing analyse-t-il les e-mails entrants (liens et pièces jointes) ?
- ☐ Les protections anti-usurpation (SPF, DKIM, DMARC) empêchent-elles l'envoi d'e-mails au nom de votre domaine ?
- ☐ Vos collaborateurs savent-ils signaler un e-mail suspect en un clic ?
- ☐ La navigation web est-elle filtrée pour bloquer les sites malveillants connus (filtrage DNS) ?

Sauvegardes

- ☐ Vos données Microsoft 365 / Google Workspace (e-mails, fichiers) sont-elles sauvegardées ? (elles ne le sont pas par défaut)
- ☐ Vos serveurs et données métier suivent-ils la règle 3-2-1 (3 copies, 2 supports, 1 hors site) ?
- ☐ Une restauration a-t-elle été testée dans les 12 derniers mois ? (une sauvegarde jamais testée n'en est pas une)

Sensibilisation et réaction

- ☐ Vos collaborateurs sont-ils sensibilisés régulièrement au phishing (simulations, formations courtes) ?
- ☐ Disposez-vous d'une procédure écrite en cas d'incident (qui appeler, quoi faire dans la première heure) ?

Conformité et gouvernance

- ☐ Tenez-vous un registre des traitements de données personnelles (RGPD) ?
- ☐ Savez-vous si votre entreprise est concernée par la directive NIS2, et quelles obligations en découlent ?
- ☐ Avez-vous un inventaire à jour du matériel et des logiciels, et un interlocuteur identifié pour l'informatique ?

Comment lire votre résultat

- 0 à 3 cases non cochées : bon niveau, quelques ajustements à prévoir.
- 4 à 8 cases non cochées : des angles morts à traiter sans tarder.
- Plus de 8 cases non cochées : exposition élevée, un plan d'action s'impose.

Plusieurs cases non cochées ?

Notre audit gratuit d'une heure fait le point précisément sur vos identités, votre messagerie, vos sauvegardes et votre conformité — sur site ou en visio, sans engagement.

Réservez votre audit → cyleme.fr/audit-gratuit