RAPPORT DE DIAGNOSTIC

Cybersécurité PME

product

14 mai 2026
Rapport confidentiel

SCORE DE MATURITÉ CYBERSÉCURITÉ

47

/100

Niveau moyen — des améliorations importantes sont nécessaires

Résumé pour la direction

Votre entreprise Product obtient un score de 47/100, ce qui révèle une protection numérique insuffisante face aux menaces actuelles. Trois domaines sont en situation critique : la gestion des accès (qui contrôle qui accède à quoi), la capacité à réagir en cas d'attaque, et l'anticipation des risques. Concrètement, si un pirate obtient un mot de passe d'un employé aujourd'hui, il pourrait accéder à l'ensemble de vos systèmes sans que vous le détectiez pendant plusieurs jours. La bonne nouvelle : les premières actions correctives sont simples à mettre en place et réduiront significativement votre exposition en quelques semaines seulement.

Points positifs identifiés

- Votre infrastructure technique de base est correctement sécurisée (pare-feu, antivirus) avec un score de 59/100
- La protection de vos données clients et la conformité aux règles européennes de protection des données personnelles sont à un niveau acceptable (58/100)

Résultats par domaine

Gouvernance	44/100
Accès & identités	38/100
Infrastructure	59/100
Données & RGPD	58/100
Sensibilisation	50/100
Incidents	38/100
Analyse risque	38/100

Analyse des risques identifiés

CRITIQUE **N'importe qui peut accéder à tout dans l'entreprise**

Vos employés ont probablement des accès trop larges aux fichiers et logiciels de l'entreprise. Si un pirate vole le mot de passe d'un seul collaborateur, il peut potentiellement accéder à toutes vos données sensibles (fichiers clients, comptabilité, contrats). Impact : vol de votre base clients par un concurrent, ou demande de rançon de 15 000 à 50 000€ pour récupérer vos données.

CRITIQUE **Aucun plan en cas d'attaque informatique**

Si vos ordinateurs sont bloqués demain matin par un virus, personne ne sait quoi faire ni qui appeler. Cette improvisation transforme un incident de quelques heures en paralysie de plusieurs jours. Impact : arrêt complet de l'activité pendant 3 à 7 jours, perte de chiffre d'affaires estimée entre 5 000 et 30 000€ selon votre activité, plus les frais de dépannage en urgence.

CRITIQUE **Vous ne savez pas ce qui menace vraiment votre entreprise**

Sans analyse des risques, vous investissez peut-être dans des protections inutiles tout en ignorant vos vraies failles. C'est comme installer une alarme sophistiquée en laissant la porte de derrière ouverte. Impact : dépenses de sécurité mal ciblées et vulnérabilité aux attaques ciblant spécifiquement votre secteur d'activité.

ÉLEVÉ **Les employés ne savent pas reconnaître une arnaque**

La moitié de vos collaborateurs pourraient cliquer sur un faux email imitant votre banque ou un fournisseur. Ces emails piégés sont la porte d'entrée de 80% des attaques contre les PME. Impact : un seul clic peut déclencher un virement frauduleux de 10 000€ ou infecter tout le réseau.

Plan d'action priorisé

Priorité	Action	Comment faire	Effort
🔴 Immédiat	**Activer la double vérification sur tous les comptes sensibles**	Activez la validation en deux étapes (code SMS ou application) sur les emails, la banque en ligne et vos logiciels métier. Commencez par vous-même et les personnes ayant accès aux finances. Tutoriels disponibles sur chaque service dans 'Paramètres > Sécurité'.	quelques heures
🔴 Immédiat	**Créer une fiche réflexe 'En cas d'attaque informatique'**	Rédigez un document A4 avec : 1) Qui appeler en premier (prestataire informatique + numéro), 2) Comment éteindre les ordinateurs et couper le wifi, 3) Où sont les sauvegardes. Affichez-le près de chaque poste et envoyez-le par email à tous.	quelques heures
🟡 Court terme (1 mois)	**Vérifier et limiter les accès de chaque employé**	Faites la liste de qui accède à quoi (dossiers partagés, logiciels, comptes). Supprimez les accès inutiles : un commercial n'a pas besoin d'accéder à la comptabilité. Dans vos dossiers partagés, créez des sous-dossiers par service avec des droits limités.	1-2 jours

Priorité	Action	Comment faire	Effort
🟡 Court terme (1 mois)	**Organiser une session de sensibilisation aux emails frauduleux**	Réunissez votre équipe 30 minutes pour montrer des exemples réels de faux emails (cherchez 'exemples phishing' sur Google Images). Donnez la règle d'or : en cas de doute sur un email demandant de l'argent ou un mot de passe, appeler directement l'expéditeur par téléphone.	quelques heures
🟡 Court terme (1 mois)	**Lister vos 5 pires scénarios de catastrophe numérique**	Prenez 1 heure pour noter : qu'est-ce qui vous ferait perdre le plus d'argent ou de clients si ça arrivait ? (vol de fichiers clients, blocage des ordinateurs, piratage du compte bancaire...). Ce sera votre base pour décider où investir en priorité.	quelques heures
🟢 Moyen terme (3 mois)	**Désigner un responsable sécurité, même à temps partiel**	Nommez une personne de confiance comme référent sécurité (même sans compétence technique). Son rôle : être le contact en cas de doute, vérifier que les sauvegardes fonctionnent chaque mois, et suivre ce plan d'action. Formalisez cette mission par un simple email.	30 minutes

Votre action prioritaire cette semaine

Dès demain, activez la double vérification sur votre propre boîte email professionnelle et sur l'accès à votre banque en ligne - cela prend 10 minutes par compte et bloque 99% des tentatives de piratage de mot de passe.