



CHECKLIST

Checklist cybersécurité PME — 15 actions essentielles

Hygiène de sécurité prioritaire, alignée sur les
recommandations ANSSI

Sedona Radar — audit de sécurité externe automatisé

Sedona AI Lecture ~10 min Édition 2026 sedona-ai.com

La sécurité d'une PME ne se joue pas sur un outil miracle, mais sur une poignée de mesures d'hygiène appliquées avec constance. Cette checklist réunit 15 actions concrètes, alignées sur le guide d'hygiène informatique de l'ANSSI et les bonnes pratiques de [Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr), classées par niveau d'effort. Commencez par les 6 actions « indispensables » : elles bloquent la majorité des attaques opportunistes. Chaque action indique pourquoi elle compte et par où démarrer — cochez au fur et à mesure.

À retenir

- Les fondamentaux d'abord : MFA, mots de passe + gestionnaire, correctifs, sauvegardes 3-2-1 testées, SPF/DKIM/DMARC et EDR bloquent la majorité des attaques opportunistes.
- Le MFA reste le maillon faible : seules 26 % des TPE-PME l'ont déployé, alors que le piratage de compte est la menace n°1 des professionnels en 2025 (+45 %).
- La sauvegarde déconnectée et testée est la vraie assurance anti-rançongiciel — 78 % des TPE-PME sauvegardent, mais peu vérifient la restauration.
- Réduire l'exposition externe (ports, services, sous-domaines, actifs oubliés) ferme des portes d'entrée fréquentes : on ne protège que ce que l'on a inventorié.
- Une action sans responsable ni échéance ne se fait pas : attribuez chaque ligne, puis réévaluez la checklist deux fois par an.

01 La menace, en chiffres, en France

Les attaques ne visent plus seulement les grands comptes. En 2025, les TPE-PME sont devenues la catégorie la plus ciblée par les rançongiciels signalés à l'ANSSI, et la demande d'assistance des professionnels a fortement progressé. Le point commun de la grande majorité des incidents : ils exploitent des failles d'hygiène de base — comptes non protégés, correctifs non appliqués, sauvegardes fragiles.

48 %

Part des PME/TPE/ETI parmi les victimes de rançongiciel signalées à l'ANSSI en 2025 (contre 37 % en 2024) — la catégorie la plus ciblée.

ANSSI/CERT-FR, Panorama de la cybermenace 2025 (CERTFR-2026-CTI-002)

504 000+

Victimes assistées par [Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr) en 2025 (+20 % vs 2024) ; la demande émanant de professionnels, surtout TPE-PME, progresse de +73 %.

[Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr), Rapport d'activité 2025

+45 %

Hausse du piratage de compte, devenu la menace n°1 pour les professionnels en 2025 — d'où la priorité absolue donnée au MFA.

Cybermalveillance.gouv.fr, Rapport d'activité 2025

Attaques moins nombreuses, mais plus lourdes

La part d'organisations attaquées mesurée par le CESIN est passée à 40 % en 2025 (contre 47 % en 2024). Ce recul apparent ne signale pas une menace qui faiblit : le baromètre décrit des attaques « moins nombreuses mais plus impactantes », 81 % des attaques réussies ayant un impact sur l'activité. Les trois premiers vecteurs restent le phishing (55 %), l'exploitation de vulnérabilités (41 %) et les attaques via un tiers (35 %).

Une note de méthode sur les chiffres

Le baromètre CESIN reflète surtout de grandes organisations (ses adhérents) : ses % de vecteurs valent d'abord pour les ETI/grands comptes. Pour les TPE-PME, la référence est le baromètre maturité cyber de Cybermalveillance (hameçonnage 43 %, failles de sécurité 18 % des incidents déclarés). Nous évitons volontairement les montants « coût moyen d'une attaque » qui circulent sans source primaire française vérifiable : pour une PME, une attaque peut être très lourde, parfois fatale.

02 Comment utiliser cette checklist

1. Traitez d'abord les 6 actions « Indispensables » : ce sont les fondations, celles qui arrêtent l'attaquant opportuniste.
2. Passez ensuite aux 5 « Recommandées », puis aux 4 « Avancées » à mesure que votre organisation gagne en maturité.
3. Pour chaque action, désignez un responsable et une échéance. Une mesure « à faire » sans propriétaire ni date ne se fait jamais.
4. Réévaluez la liste au moins deux fois par an : le SI évolue, les actifs exposés aussi.

Sur la hiérarchie « Indispensable / Recommandé / Avancé »

Cette priorisation en trois niveaux est une synthèse pédagogique de Sedona, cohérente avec l'esprit du guide d'hygiène ANSSI (qui distingue un niveau « standard » et un niveau « renforcé »). Ce n'est pas une nomenclature officielle de l'ANSSI. Le guide de référence compte 42 mesures d'hygiène, dont les fondamentaux sont repris par l'article 21 de la directive NIS2.

03 Indispensable — les 6 fondations

- ☐ 1. Authentification multifacteur (MFA) sur tous les accès sensibles — messagerie, VPN, comptes d'administration, accès distants, cloud. POURQUOI : le piratage de compte est la menace n°1 des professionnels en 2025 (+45 %) et seules 26 % des TPE-PME ont déployé le MFA. COMMENT DÉMARRER : activez la double authentification par application (TOTP) ou clé physique sur Microsoft 365 / Google Workspace, puis étendez au VPN et aux comptes admin.
- ☐ 2. Mots de passe robustes + gestionnaire — mots de passe longs et uniques par service, jamais réutilisés, stockés dans un gestionnaire ; politique de mots de passe formalisée. POURQUOI : 51 % des TPE-PME ont une politique de mots de passe, 46 % un gestionnaire. COMMENT DÉMARRER : déployez un gestionnaire d'entreprise, imposez la longueur et l'unicité, activez la surveillance des fuites. NB : l'ANSSI ne recommande plus le renouvellement périodique systématique — privilégiez longueur, unicité et MFA.
- ☐ 3. Mises à jour et correctifs — appliquer sans délai les correctifs de sécurité sur systèmes, logiciels et équipements exposés, en priorisant les vulnérabilités activement exploitées. POURQUOI : l'exploitation de failles est le 2e vecteur d'attaque (41 %, CESIN 2025). COMMENT DÉMARRER : activez les mises à jour automatiques, suivez les avis et alertes du CERT-FR, priorisez les équipements exposés sur Internet (VPN, pare-feu, serveurs de messagerie).
- ☐ 4. Sauvegardes 3-2-1, testées — 3 copies des données, sur 2 supports différents, dont 1 hors ligne / déconnectée (ou hors site), avec des tests de restauration réguliers. POURQUOI : la sauvegarde déconnectée est la contre-mesure clé face aux rançongiciels, qui chiffrent aussi les sauvegardes en ligne. 78 % des TPE-PME sauvegardent, mais la déconnexion et les tests de restauration restent rarement vérifiés. COMMENT DÉMARRER : ajoutez une copie déconnectée et planifiez un test de restauration réel ce trimestre.
- ☐ 5. Sécurité de la messagerie (SPF, DKIM, DMARC) — déployer et vérifier ces trois enregistrements sur vos domaines pour lutter contre l'usurpation d'identité, plus un filtrage anti-hameçonnage. POURQUOI : le phishing est le 1er vecteur d'attaque (55 % CESIN ; 43 % des incidents TPE-PME). COMMENT DÉMARRER : publiez SPF et DKIM, puis passez progressivement DMARC en politique « reject » pour bloquer l'usurpation de votre domaine.
- ☐ 6. Antivirus / EDR sur tous les postes et serveurs — protection contre les codes malveillants, idéalement un EDR pour la détection et la réponse, moteurs et signatures à jour. POURQUOI : 84 % des TPE-PME ont un antivirus mais seulement 16 % une solution de détection (EDR/XDR), laissant un angle mort sur les compromissions actives. COMMENT DÉMARRER : complétez l'antivirus par un EDR supervisé, avec alertes remontées et poste de réponse identifié.

04 Recommandé — les 5 mesures de consolidation

- ☐ 7. Moindre privilège & comptes d'administration dédiés — comptes utilisateurs sans droits admin, comptes d'administration dédiés et non nominatifs (jamais utilisés pour naviguer ou lire ses mails), revue régulière des comptes et privilèges. POURQUOI : mesures explicites du guide d'hygiène ANSSI ; le moindre privilège limite la propagation d'une compromission. COMMENT DÉMARRER : retirez les droits admin des comptes du quotidien et créez des comptes admin séparés.
- ☐ 8. Sensibilisation des collaborateurs au phishing — formations et exercices anti-phishing réguliers, procédure de signalement claire. POURQUOI : l'humain reste le premier point d'entrée. COMMENT DÉMARRER : utilisez les kits gratuits de Cybermalveillance (SensCyber, kits TPE-PME), organisez une campagne de faux phishing puis un débrief.
- ☐ 9. Inventaire des actifs — cartographier le SI : matériels, logiciels, comptes, domaines et services. POURQUOI : on ne protège que ce que l'on connaît ; l'ANSSI en fait un préalable (connaissance du SI). COMMENT DÉMARRER : tenez un inventaire à jour, identifiez vos actifs critiques et leurs responsables.
- ☐ 10. Réduction de l'exposition externe — connaître et réduire ce qui est exposé sur Internet : ports ouverts, services inutiles, sous-domaines, panneaux d'administration accessibles, actifs oubliés (shadow IT). POURQUOI : l'exposition externe non maîtrisée est une porte d'entrée fréquente ; c'est l'objet de l'EASM (gestion de surface d'attaque externe). COMMENT DÉMARRER : listez vos domaines et adresses IP publiques, fermez les services non nécessaires, restreignez les interfaces d'administration.
- ☐ 11. Plan de réponse à incident + contacts d'urgence — procédure de réaction (isolement, préservation des preuves, communication), exercices de crise, et réflexes en cas d'attaque. POURQUOI : réagir vite limite l'impact ; le dépôt de plainte est un préalable à toute indemnisation cyber. COMMENT DÉMARRER : rédigez une fiche réflexe, affichez les contacts (Cybermalveillance.gouv.fr pour la mise en relation avec un prestataire, dépôt de plainte), et notez, si vous êtes concerné par NIS2, les obligations de notification à l'ANSSI qu'elle prévoit (directive non transposée en droit français au 14/10/2026).

05 Avancé — les 4 mesures de renforcement

- ☐ 12. Chiffrement des postes — chiffrer les disques des ordinateurs, en priorité les postes nomades et portables. POURQUOI : en cas de vol ou de perte, le chiffrement protège les données de l'entreprise (mesure de nomadisme du guide ANSSI). COMMENT DÉMARRER : activez BitLocker (Windows) ou FileVault (macOS) sur l'ensemble du parc et centralisez les clés de récupération.

- ☐ 13. Cloisonnement réseau — segmenter le réseau pour isoler les zones sensibles (serveurs, postes utilisateurs, invités, OT/IoT). POURQUOI : la segmentation contient la propagation d'une attaque. COMMENT DÉMARRER : séparez les VLAN, filtrez les flux entre segments, isolez le réseau invité.
- ☐ 14. Journalisation et supervision — centraliser les journaux et surveiller les événements (idéalement un SIEM). POURQUOI : seules 16 % des TPE-PME disposent d'une capacité de détection ; sans journaux, une intrusion passe inaperçue. COMMENT DÉMARRER : activez la journalisation sur les équipements clés, centralisez les logs et définissez des alertes sur les événements critiques.
- ☐ 15. Gestion de la sécurité des prestataires — encadrer contractuellement la sécurité des tiers et maîtriser leurs accès. POURQUOI : les attaques via un tiers représentent 35 % des vecteurs (CESIN 2025) ; côté grandes organisations, 85 % intègrent des clauses de sécurité dans leurs contrats et 46 % utilisent le cyber-rating. COMMENT DÉMARRER : inventoriez vos prestataires disposant d'un accès, ajoutez des clauses de sécurité et limitez leurs droits au strict nécessaire.

06 Où en êtes-vous ? Auto-score

Faites le compte

Comptez 1 point par action réellement en place et testée (pas seulement « prévue »). 0–5 : socle à construire d'urgence, concentrez-vous sur les 6 indispensables. 6–10 : bonnes bases, consolidez avec les mesures recommandées. 11–15 : maturité solide, visez la supervision continue et l'audit régulier. Rappel : 80 % des dirigeants de TPE-PME s'estiment insuffisamment préparés à une cyberattaque — un score honnête vaut mieux qu'un score flatteur.

Pour situer votre équipement par rapport aux autres TPE-PME françaises (baromètre Cybermalveillance 2025) :

Mesure	Taux d'équipement des TPE-PME (2025)
Antivirus	84 %
Sauvegardes	78 %
Pare-feu	69 %
Politique de mots de passe	51 %
Gestionnaire de mots de passe	46 %
Double authentification (MFA)	26 %
Solution de détection (EDR/XDR)	16 %

Source : [Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr), 2e Baromètre de la maturité cyber des TPE-PME (2025).

L'IA générative non encadrée, nouveau facteur de fuite

L'usage de services d'IA générative non approuvés est jugé risqué par 75 % des répondants au baromètre CESIN 2025 : c'est un nouveau vecteur de fuite de données à intégrer dans votre politique d'hygiène. Encadrez-le par une charte d'usage de l'IA et une classification des données, plutôt que par une interdiction qui pousse à l'usage clandestin.

§ Sources

1. CESIN, 11e Baromètre de la cybersécurité des entreprises (données 2025) — <https://www.itforbusiness.fr/11e-barometre-cesin-2026-cyber-99603>
2. ANSSI/CERT-FR, Panorama de la cybermenace 2025 (CERTFR-2026-CTI-002) — <https://www.cert.ssi.gouv.fr/uploads/CERTFR-2026-CTI-002.pdf>
3. Cybermalveillance.gouv.fr, Rapport d'activité 2025 — <https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/rapport-activite-2025>
4. Cybermalveillance.gouv.fr, 2e Baromètre de la maturité cyber des TPE-PME (2025) — <https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/etude-maturite-cyber-tpe-pme-2025>
5. ANSSI, Guide d'hygiène informatique (42 mesures) — <https://cyber.gouv.fr/publications/guide-dhygiene-informatique>
6. ANSSI, Recommandations relatives à l'authentification multifacteur et aux mots de passe — <https://cyber.gouv.fr/publications/recommandations-relatives-lauthentification-multifacteur-et-aux-mots-de-passe>
7. ANSSI, Recommandations de sécurité pour la mise en œuvre d'un service de messagerie — <https://cyber.gouv.fr/publications/recommandations-de-securite-pour-la-mise-en-oeuvre-dun-service-de-messagerie>
8. ANSSI/CERT-FR, Avis et alertes de sécurité — <https://www.cert.ssi.gouv.fr/>
9. Cybermalveillance.gouv.fr, Bonnes pratiques — <https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques>
10. Cybermalveillance.gouv.fr, Fiche « Sauvegardes » — <https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/sauvegardes>

Mesurez régulièrement votre exposition externe

Les actions 9, 10 et 3 de cette checklist — inventaire, réduction de l'exposition externe et priorisation des correctifs — sont ce que Sedona Radar vous aide à suivre. Radar analyse ce que votre domaine expose sur Internet (domaines, ports, services, actifs oubliés) et classe les constats par gravité ; il ne réduit pas l'exposition à votre place. Il donne des indicateurs de maturité sur six référentiels dont NIS2, sans certifier : il n'existe aucune certification NIS2. Lancez un scan gratuit pour voir ce qu'un attaquant voit de vous.

Lancer mon scan gratuit

sedona-ai.com/scan-gratuit