

Cyber-résilience des PME 2026-2027

Note stratégique gratuite • Première édition • Europe, Norvège et marchés internationaux

Résumé exécutif

La cybersécurité des PME ne doit plus être évaluée exclusivement par l’acquisition d’un antivirus. Les dépendances aux prestataires, la gestion des identités, les sauvegardes et la capacité de reprise sont des décisions de direction.

En septembre 2026, ENISA souligne la persistance des ransomwares, du phishing et des vulnérabilités exploitées, ainsi que le risque créé par les dépendances numériques. Cette note propose un cadre de priorisation et non un audit de sécurité d’une entreprise précise.

Signal externe	Lecture pour décideurs
ENISA 2026 : ransomware à fort impact	Tester la capacité de restaurer les fonctions essentielles
Verizon DBIR 2025 : 30 % des violations avec tiers impliqués	Cartographier fournisseurs et accès externes
Verizon DBIR 2025 : exploitation de vulnérabilités en hausse de 34 %	Prioriser inventaire, correctifs et exposition Internet

Les cinq décisions prioritaires

1. Identités : authentification multifactorielle sur e-mail, cloud et comptes privilégiés ; revue mensuelle des départs et accès.
2. Sauvegardes : copie protégée et exercice réel de restauration, avec objectifs RPO/RTO adaptés.
3. Exposition : inventaire des systèmes accessibles sur Internet, responsables désignés et délais de correction.
4. Fournisseurs : registre de dépendances, preuves de contrôle et procédures de rupture de service.
5. Réponse : responsabilités, contacts d’urgence, exercices simples et messages préparés pour les clients.

Tableau de pilotage proposé

Le comité de direction peut suivre six indicateurs : couverture MFA des comptes critiques ; proportion d’actifs inventoriés ; correctifs critiques hors délai ; restaurations testées ; fournisseurs à risque

réévalués ; temps de simulation de reprise. Chaque indicateur doit avoir une définition stable et un propriétaire.

Scénarios de décision sur 90 jours

Scénario A — minimum défensif : inventaire, MFA, sauvegarde, formation ; coût opérationnel faible mais profondeur limitée.

Scénario B — résilience structurée : A + gestion fournisseurs, test de reprise, revue sécurité trimestrielle ; convient aux PME en croissance.

Scénario C — exigences sectorielles : B + évaluation externe, gestion avancée des risques et exigences contractuelles ; nécessaire uniquement selon exposition et obligations.

Plan 30 / 60 / 90 jours

Jours 1-30 : définir les services critiques, les accès et les dépendances ; établir un niveau initial.

Jours 31-60 : déployer les protections priorisées ; réaliser un test de restauration.

Jours 61-90 : exercer un incident fictif, réévaluer les fournisseurs et présenter les indicateurs à la direction.

Ce que MSI peut proposer

MSI peut préparer un diagnostic de maturité non intrusif, un atelier de priorisation et un tableau de bord de gouvernance. Les vérifications techniques nécessitent mandat écrit et intervenants qualifiés ; aucun niveau de conformité ou d'absence de risque n'est garanti.

Sources vérifiables

ENISA, Threat Landscape 2026, 22 septembre 2026 : <https://www.enisa.europa.eu/news/exploring-the-evolution-of-the-cyber-threat-landscape-how-dependencies-weaken-our-digital-resilience>

Verizon, 2025 Data Breach Investigations Report :
<https://www.verizon.com/about/news/2025-data-breach-investigations-report>

Limites : synthèse documentaire ; aucune collecte originale d'incidents auprès d'entreprises ni audit terrain.