



Constats types par segment

Vulnérabilités les plus fréquemment observées dans chaque segment cible — TPE-PME, collectivités territoriales et associations.

Sources : ANSSI — Panorama de la cybermenace 2023 · ANSSI — Guide cybersécurité TPE/PME · CNIL — Rapport d'activité 2023 · ENISA — Threat Landscape 2023 · Cybermalveillance.gouv.fr — Rapport 2023.

SEGMENT 1 — TPE-PME

Profil type

- 0 à 250 salariés
- Pas de RSSI ni d'équipe IT dédiée
- Prestataire informatique externe (souvent unique)
- Budget IT < 5 000 €/an

Vulnérabilités les plus fréquentes

1. Mots de passe faibles et comptes partagés

85 % des incidents en entreprise impliquent un mot de passe compromis (source : Verizon DBIR 2023). Comptes admin partagés entre collaborateurs, mots de passe notés sur post-it, absence de MFA sur la messagerie.

■ **Risque :** Prise de contrôle du SI, exfiltration de données, usurpation d'identité.

2. Sauvegardes insuffisantes ou inexistantes

Absence de sauvegarde hors site ou cloud. Fréquence insuffisante (hebdomadaire au lieu de quotidienne). Sauvegardes non testées depuis des mois.

■ **Risque :** Perte totale de données en cas de ransomware ou sinistre physique.

3. Logiciels non mis à jour

Windows/macOS en version obsolète. Logiciels métier non patchés. Antivirus expiré ou absent. Plugins WordPress/CMS jamais mis à jour.

■ **Risque :** Exploitation de vulnérabilités connues et corrigées — vecteur principal des ransomwares.

4. RGPD non appliqué

Registre des traitements inexistant. Pas de politique de confidentialité sur le site. Consentement cookies absent. Données clients dans des fichiers Excel partagés non sécurisés.

■ **Risque :** Sanction CNIL — amendes jusqu'à 4 % du CA mondial. Perte de confiance clients.



5. Absence de sensibilisation au phishing

Employés non formés à la détection d'emails frauduleux. Pas de filtre anti-spam efficace. Aucune procédure de signalement interne.

■ **Risque** : Le phishing est le premier vecteur d'attaque — 91 % des cyberattaques débutent par un email malveillant.

SEGMENT 2 — COLLECTIVITÉS TERRITORIALES

Profil type

- Communes, EPCI, départements, régions
- DSI mutualisée ou prestataire unique
- Données sensibles : état civil, urbanisme, données des administrés
- Soumises à NIS2 depuis 2024 — obligations de notification sous 24h

Vulnérabilités les plus fréquentes

1. Dépendance à un prestataire unique

Un seul prestataire IT gère l'intégralité du SI. Pas de SLA formalisé. Pas de plan de continuité si le prestataire est défaillant.

■ **Risque** : Paralysie totale de la collectivité en cas de défaillance du prestataire.

2. Ransomware — premier vecteur (80 % des incidents ANSSI 2023)

Sauvegardes sur le même réseau que la production (chiffrées simultanément). Absence de segmentation réseau. Pas de plan de réponse aux incidents.

■ **Risque** : Paralysie des services publics, coûts de reconstruction estimés entre 500 K€ et plusieurs M€.

3. Non-conformité NIS2

Absence de cartographie du SI. Pas de processus de gestion des incidents. Sécurité de la chaîne d'approvisionnement non évaluée. Délais de notification inconnus.

■ **Risque** : Sanctions administratives, mise en demeure ANSSI, responsabilité des élus.

4. Données sensibles non protégées

Données d'état civil, données sociales, données des administrés stockées sans chiffrement. Accès non contrôlé aux bases de données.

■ **Risque** : Violation massive de données — obligation de notification CNIL + personnes concernées.

5. Formation insuffisante des agents

Taux de sensibilisation cyber < 20 % dans la plupart des communes. Aucune simulation de phishing. Pas de procédure d'escalade en cas d'incident.

■ **Risque** : Facteur humain responsable de 82 % des incidents (source : Verizon DBIR).



SEGMENT 3 — ASSOCIATIONS

Profil type

- Associations loi 1901 — employeuses ou non
- Données adhérents, bénévoles, bénéficiaires
- Budget IT quasi inexistant
- Fort turnover bénévoles → gestion des droits d'accès difficile

Vulnérabilités les plus fréquentes

1. Comptes partagés et accès non révoqués

Identifiants partagés entre bénévoles. Anciens membres conservant des accès après départ. Mot de passe unique pour toute l'association.

■ **Risque** : Accès non autorisé aux données — violation du RGPD.

2. Données adhérents non sécurisées

Fichiers Excel d'adhérents sur Google Drive partagé publiquement. Données de santé (associations médico-sociales) sans protection particulière.

■ **Risque** : Violation RGPD — données sensibles (art. 9) soumises à des obligations renforcées.

3. Absence de contrats de sous-traitance RGPD

Logiciels de gestion des adhérents, outils de communication, hébergeur web sans DPA (Data Processing Agreement) signé.

■ **Risque** : Responsabilité du responsable de traitement engagée — sanction CNIL possible.

4. Pas de politique de sauvegarde

Données associatives (comptabilité, adhérents, PV de CA) stockées uniquement sur l'ordinateur du trésorier ou du président. Aucune copie externalisée.

■ **Risque** : Perte irréversible des données en cas de panne ou sinistre.

5. Méconnaissance des obligations RGPD

73 % des associations ignorent qu'elles sont soumises au RGPD dès qu'elles gèrent des données de leurs adhérents ou bénéficiaires (source : enquête Wilizé 2026).

■ **Risque** : Amende CNIL, perte de confiance des adhérents et des financeurs institutionnels.

Ce document est mis à jour annuellement en fonction des données ANSSI, CNIL et ENISA. Pour un diagnostic personnalisé de votre structure : infos.wilize@gmail.com · wilize.com