TAVITA CYBERSECURITY
GARDIEN CYBER DES TERRITOIRES

TPE · ARTISANS · PROFESSIONS LIBÉRALES

ACCOMPAGNEMENT CYBER SUR MESURE DES TPE

L'essentiel, bien dimensionné : protéger votre activité, vos clients et votre trésorerie sans usine à gaz, avec un accompagnement proportionné à la taille de votre entreprise.

LES TPE, CIBLES FACILES ET PREMIÈRES VICTIMES

Une messagerie, un logiciel de facturation, un compte bancaire en ligne, un fichier clients : c'est tout ce qu'il faut à un attaquant. Les TPE n'ont ni service informatique ni temps à y consacrer, et les cybercriminels le savent : les bilans 2025 de Cybermalveillance.gouv.fr, de l'ANSSI et de la CNIL le confirment.

+73 % [1]
de demandes d'assistance d'entreprises et d'associations sur le 17Cyber en 2025

48 % [2]
des 128 victimes de rançongiciel signalées à l'ANSSI en 2025 sont des TPE, PME et ETI, catégorie la plus touchée

+93 % [1]
de fraudes au virement visant les entreprises en 2025 : un faux RIB, un faux fournisseur, et la trésorerie part

+45 % [1]
de piratages de comptes chez les professionnels en 2025, première menace : messagerie, Microsoft 365, réseaux sociaux, banque en ligne

Concrètement, pour une TPE : un compte de messagerie piraté sert à détourner vos virements et ceux de vos clients ; un rançongiciel chiffre le poste qui contient la compta et les devis ; sans sauvegarde testée, l'activité s'arrête plusieurs jours. Aux Antilles, opérateurs télécoms, cabinets d'avocats et collectivités ont déjà été touchés (2023) [4]. TAVITA CYBERSECURITY est intervenue 11 fois après une cyberattaque auprès de TPE, PME et groupes.

Sources — [1] Cybermalveillance.gouv.fr, *Rapport d'activité et état de la menace 2025* (cybermalveillance.gouv.fr) · [2] ANSSI, *Panorama de la cybermenace 2025*, CERTFR-2026-CTI-002 (cyber.gouv.fr) · [4] Presse locale : Le Pélican, Journal de Saint-Barth, Bondamanjak, RCI.

SE METTRE EN CONFORMITÉ N'EST PLUS UNE OPTION

RGPD Il s'applique dès le premier fichier client ou salarié : mesures de sécurité adaptées (art. 32), registre simplifié, notification d'une violation à la CNIL sous **72 h**.

ASSURANCE Pour être indemnisé d'une cyberattaque, la loi impose un dépôt de plainte sous **72 h** ; les assureurs exigent MFA, sauvegardes et procédures écrites.

CLIENTS Vos donneurs d'ordre soumis à NIS 2 répercutent leurs exigences sur leurs fournisseurs : questionnaires, attestations, clauses cyber dans les contrats et appels d'offres.

E-FACTURE Facturation électronique obligatoire : réception pour toutes les entreprises dès septembre 2026, émission pour les TPE en 2027 — des flux dématérialisés à sécuriser contre la fraude.

SANCTIONS
Amendes CNIL même pour les petites structures ; responsabilité personnelle du dirigeant en cas de négligence.

TRÉSORERIE
Un virement détourné ou une semaine d'arrêt suffisent à mettre une TPE en difficulté ; une fuite de données fait fuir les clients.

ASSURANCE & AIDES
Refus ou résiliation d'assurance cyber faute de mesures de base ; des dispositifs publics gratuits existent (17Cyber, MonAideCyber de l'ANSSI).

Choisir TAVITA CYBERSECURITY, c'est faire le choix d'un partenaire de confiance, expert, réactif et engagé pour la protection durable de votre système d'information.

NOTRE RÉPONSE AU VERSO →

UN ACCOMPAGNEMENT SUR MESURE, DIMENSIONNÉ POUR UNE TPE

Une TPE n'a pas besoin d'un SOC 24/7 ni d'une certification ISO 27001 : elle a besoin que les quelques mesures qui comptent vraiment soient en place, sans mobiliser son dirigeant pendant des semaines. Trois paliers progressifs, activables un par un, chacun chiffré sur devis.

TROIS PALIERS, À VOTRE RYTHME

1 · Diagnostic flash

1 journée, sur site ou à distance

Tour d'horizon de votre exposition : messagerie, comptes et mots de passe, sauvegardes, postes, box et Wi-Fi, site web. Restitution au dirigeant et plan d'action en 10 points, priorisé et chiffré.

2 · Socle de sécurité

2 à 5 jours selon la taille

Mise en œuvre des priorités : MFA partout, sauvegarde 3-2-1 testée, antivirus/EDR géré, durcissement Microsoft 365 ou Google Workspace, pare-feu et Wi-Fi, procédure anti-fraude au virement, charte informatique.

3 · Suivi sérénité

Forfait léger, trimestriel ou mensuel

Supervision EDR et alertes, point trimestriel, mises à jour et vérification des sauvegardes, exercice de phishing annuel, dossier pour votre assureur, ligne directe en cas d'incident.

CE QUE CONTIENT UN ACCOMPAGNEMENT TPE BIEN DIMENSIONNÉ

1 — Les 5 mesures essentielles
MFA, sauvegardes testées, mises à jour, antivirus/EDR géré, comptes et droits maîtrisés — installées, vérifiées, documentées.

2 — Anti-fraude au virement
Procédure de double vérification des RIB et des demandes urgentes, sécurisation de la banque en ligne, sensibilisation de la personne qui paie.

3 — Sensibilisation courte et concrète
2 heures avec toute l'équipe, sur vos propres outils : reconnaître un hameçonnage, réagir, à qui le dire. Rappel annuel avec un test de phishing.

4 — Conformité au bon niveau
Registre RGPD simplifié, charte informatique, mentions et contrats prestataires, réponses aux questionnaires cyber de vos clients et assureurs.

5 — Plan « et si ça arrive »
Une page : qui appeler, quoi débrancher, comment restaurer, quoi déclarer (plainte sous 72 h, CNIL, assureur). Assistance de TCS en cas d'incident.

6 — Prestataires et outils cloud
Revue de vos accès et contrats (hébergeur web, logiciel métier, expert-comptable, infogérant) pour que la sécurité ne s'arrête pas à votre porte.

TROIS FAÇONS DE TRAVAILLER ENSEMBLE

Intervention ponctuelle

Diagnostic flash puis socle de sécurité, à la journée, avec un livrable clair à chaque étape. Vous gardez la main.

Forfait de suivi

Quelques heures par mois ou par trimestre : supervision, vérifications, conseils, et un interlocuteur qui connaît votre entreprise.

Réponse à incident

Compte piraté, virement détourné, poste chiffré : contenir, restaurer, déclarer, et renforcer pour que ça ne se reproduise pas.

VOTRE INTERLOCUTEUR

David TOUCHE — Gérant et consultant en cybersécurité

Architecte système, réseau et sécurité, ancien des forces armées : 23 ans au Ministère des Armées, 28 ans d'expérience en SI dont 17 en cybersécurité. Master 2, certifié ISO/IEC 27005 Risk Manager, membre de la Cybersecurity Flying Squad Paris 2024 à Teahupo'o. Il intervient personnellement sur chaque mission, en présentiel et à distance.

Références : 57 projets d'audit et de sécurisation · 11 interventions après cyberattaque (TPE, PME, ETI, groupes) · 5 entreprises supervisées · 234 personnes formées, en Polynésie française et en Martinique.

SUR MESURE, SUR DEVIS

Un échange de 30 minutes suffit pour cadrer le diagnostic flash. Chaque palier est chiffré séparément, sans engagement sur le suivant.

contact@tavita-cybersecurity.com
+33 6 99 63 17 11 · +689 87 30 41 25
www.tavita-cybersecurity.com
Nous suivre : linktr.ee/TAVITACYBERSECURITY