RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

COMMUNIQUE DE PRESSE

Maturité cyber des TPE-PME : encore un cap à franchir

Paris, le 7 octobre 2025 – À l'occasion du salon des Assises de la cybersécurité, Cybermalveillance.gouv.fr publie les résultats de la 2ème édition du baromètre national de la maturité cyber des TPE-PME, réalisée en partenariat avec la CPME, le MEDEF et l'U2P. L'étude passe en revue l'évolution des entreprises en termes d'équipement, de procédure, d'investissement budgétaire et de façon générale, de capacité à faire face aux attaques. En dépit d'une meilleure conscience des enjeux et de tendances encourageantes, les TPE-PME ont encore des efforts à accomplir.

Une amélioration de la perception des enjeux et des usages cyber

Alors que **16 % des entreprises interrogées déclarent avoir été victimes** d'un ou plusieurs incidents au cours des 12 derniers mois, les résultats 2025 du baromètre national cyber des TPE-PME paraissent refléter une évolution positive de leur rapport à la cybersécurité.
En effet, la tendance pour cette 2ème édition démontre que **les entreprises interrogées cette année sont plus nombreuses à penser qu'elles sont fortement exposées, 44 %** (38 % en 2024).
La perception de leur protection est également meilleure en 2025 avec **58 % des TPE-PME qui pensent bénéficier d'un bon ou très bon niveau de protection** (39 % l'an passé).

Ces constats coïncident d'ailleurs avec les dispositifs de sécurité mis en place…
Ainsi, si le trio de tête reste stable (84 % antivirus, 78 % sauvegardes, 69 % pare-feu), **le nombre moyen de dispositifs de sécurité installés augmente** (de 3,62 en 2024 à 4,06). Les entreprises indiquent être davantage dotées d'une politique de mots de passe (51 %, +11 points), de gestionnaires de mots de passe (46 %, +8 points), de solutions de double authentification pour 26 % d'entre elles (+6 points) et de solutions de détection d'attaque (16 %, +4 points). Même tendance concernant les procédures de réaction aux cyberattaques avec 24 % de TPE affirmant en disposer, soit 5 points de plus en 1 an.

…avec l'analyse que les TPE-PME font des cyberattaques,
La mise en place de ces dispositifs de sécurité semble permettre aux TPE-PME de mieux comprendre les incidents avec 7 entreprises victimes sur 10 en capacité d'en identifier les causes.
Ainsi, 43 % ont déclaré que ces attaques étaient liées à l'hameçonnage contre 24 % l'an dernier, 18 % à des failles de sécurité (14 % en 2024) et 11 % à des consultations de sites Internet vérolés (5 % en 2024).

…et avec leur meilleure capacité à faire face aux conséquences des incidents de sécurité.
Comparé à l'année passée, les TPE-PME ont tendance à moins accuser d'interruptions de service (29 % contre 35 %), de pertes financières (11 % / 15 %) ou de vol de données (22 % / 25 %).

Enfin, cette conscience des enjeux est également perceptible en termes budgétaires.
En 2025, les entreprises ont en effet témoigné d'une **augmentation significative de leur budget informatique par rapport à 2024 (19 vs 13 %)**. Côté cybersécurité, même si les investissements restent faibles avec moins de 2000 € pour les 3/4 d'entre elles, **15 % prévoient néanmoins de faire évoluer à la hausse ce budget, soit 5 points de plus.**

Par ailleurs, leur perception reflète une bonne connaissance de l'écosystème avec 39 % d'entre elles qui déclarent se tourner vers les prestataires informatiques pour s'informer ou se faire aider sur les sujets de cybersécurité, 31 % vers Cybermalveillance.gouv.fr, 19 % vers l'ANSSI et désormais 7 % vers le 17Cyber.

Malgré cette évolution de la perception cyber des entreprises, de vraies résistances subsistent

Si elles semblent plus avisées face aux risques, les TPE-PME n'en restent pas moins lucides. Ainsi, même si la tendance met en avant des TPE qui déclarent être plus exposées, **80 % reconnaissent qu'elles ne sont toujours pas préparées aux attaques (49 % + 3 points) ou l'ignorent (31 %) .**

D'autre part, près de 6 entreprises sur 10 (58 %) admettent encore qu'elles ne sauraient pas évaluer les conséquences d'une cyberattaque. Les principales inquiétudes concernent la perte ou le vol de données (94 %), les répercussions financières (88 %), l'interruption d'activité (87 %) et leur réputation (82 %).

En termes d'offres, si **2/3 des TPE-PME affirment connaître les solutions techniques**, notamment les plus grandes, **1/2 seulement les juge réellement adaptées,** essentiellement pour des questions de coût, de complexité d'utilisation ou de manque d'accompagnement. En dépit de la bonne connaissance qu'elles ont du marché et de son offre, l'étude révèle qu'encore **1/4 des entreprises ne fait appel à aucun acteur spécialisé,** témoignant d'un accompagnement encore trop fragmenté ou mal identifié par une grande partie du tissu économique.

Parmi les principaux obstacles à un niveau satisfaisant de sécurité informatique, les TPE-PME font état d'un manque de connaissances et d'expertise (63 %), de contraintes budgétaires (61 %), et d'un manque de temps (59 %). Près de 3 entreprises sur 10 considèrent ce sujet comme non prioritaire, un chiffre qui augmente auprès des entreprises répondantes cette année +11 points.

Des attentes fortes et une sensibilisation essentielle

Quand on les interroge sur la cybersécurité, les TPE-PME sont une majorité -près de 6 sur 10- à reconnaître que cet enjeu sociétal concerne tout le monde dans l'entreprise. Pour y répondre, la moitié d'entre elles expriment des besoins concrets en outils de sécurisation et en accompagnement. Le soutien financier est également plébiscité et il arrive juste après la sensibilisation, qui demeure légèrement priorisée par les répondants.

Ainsi, 6 TPE-PME sur 10 ont engagé des actions de sensibilisation et de façon plus régulière, les plus mâtures étant dans les structures de plus de 10 salariés (90 %) ou celles du domaine des services (71 %).

« Si l'étude met en évidence une meilleure conscience des enjeux et une légère amélioration du nombre d'entreprises qui semblent gagner en maturité sur le sujet de la cybersécurité, près de 6 TPE-PME sur 10 reconnaissent qu'elles ne sauraient toujours pas évaluer les conséquences d'une cyberattaque. Or cela fait partie des étapes clé à franchir pour décider de se sécuriser et se préparer. Force est de constater que nombre d'entreprises sont encore réticentes à la mise en place de mesures préventives et ne font pas de la cybersécurité une priorité, d'où l'importance de poursuivre la sensibilisation et de les convaincre plus que jamais de se sécuriser en amont » a déclaré Jérôme Notin, Directeur Général de Cybermalveillance.gouv.fr

Enquête OpinionWay pour Cybermalveillance.gouv.fr, réalisée en ligne entre le 02 juin et le 07 juillet 2025 auprès d'un échantillon de 588 entreprises de moins de 250 salariés en France métropolitaine et régions d'Outre-Mer, représentatif des entreprises françaises de moins de 250 salariés.

Contact presse : presse@cybermalveillance.gouv.fr
Béatrice Hervieu : 01 83 75 74 10/Pauline Fabry 14 19/Stella Azzolli 74 09

À propos de Cybermalveillance.gouv.fr

Cybermalveillance.gouv.fr *est la plateforme du Groupement d'Intérêt Public Action contre la cybermalveillance (GIP ACYMA). Créé en 2017, ce dispositif national a pour missions l'assistance aux victimes d'actes de cybermalveillance, la protection des organisations, la sensibilisation aux risques numériques, et l'observation de la menace sur le territoire français, qui s'illustrent notamment au travers du service d'assistance* 17Cyber mis en place en lien avec le ministère de l'Intérieur. *Ses 64 membres issus du secteur public, du privé et du domaine associatif contribuent à sa mission d'intérêt général pour ses 3 publics : particuliers, entreprises et collectivités. En 2024,* Cybermalveillance.gouv.fr *a accueilli 5,4 millions de visiteurs uniques sur son site Internet et plus de 420 000 personnes ont réalisé un parcours d'assistance.* www.cybermalveillance.gouv.fr

PREMIER MINISTRE

MINISTÈRE DE L'ÉDUCATION NATIONALE,
DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE

MINISTÈRE DE LA JUSTICE

MINISTÈRE DE L'INTÉRIEUR

MINISTÈRE DE L'ÉCONOMIE, DES FINANCES
ET DE LA SOUVERAINETÉ INDUSTRIELLE ET NUMÉRIQUE

MINISTÈRE DES ARMÉES

MINISTÈRE DÉLÉGUÉ CHARGÉ DE L'INTELLIGENCE ARTIFICIELLE
ET DU NUMÉRIQUE