CYBERSÉCURITÉ DES PME : UN ÉCART INQUIÉTANT ENTRE PERCEPTION ET RÉALITÉ

Dans un contexte où les cybermenaces se multiplient et deviennent de plus en plus complexes, une nouvelle étude mondiale attire l'attention sur la préparation réelle des petites et moyennes entreprises pour faire face à ces risques croissants. Réalisée par Devolutions, une entreprise technologique canadienne présente dans plus de 140 pays, dont la France, cette enquête met en lumière un constat préoccupant : 71 % des PME sondées se disent prêtes à gérer un incident de cybersécurité majeur, mais en fait, seules 22 % disposent réellement d'une posture de sécurité jugée suffisamment avancée.

Ce rapport mondial 2025 explore plusieurs axes essentiels servant à comprendre les vulnérabilités des PME : recours encore très fréquent à des outils manuels et obsolètes pour gérer les accès privilégiés, faible adoption de l'intelligence artificielle en matière de cybersécurité, budgets souvent mal répartis, ainsi que menaces internes largement sous-estimées. Ces constats résonnent fortement avec la situation observée en France, où la maturité en cybersécurité demeure très variable selon la taille des entreprises et les secteurs.

Six faits saillants principaux

Le sondage, comptant des choix de réponse et des questions ouvertes, a été mené du 12 février au 1er avril 2025 auprès de petites et moyennes entreprises situées au Canada, aux États-Unis, en Europe et ailleurs. L'étude préparée par Devolutions fait apparaître six points clés concernant le développement et l'efficacité des postures de cybersécurité des PME, et ce à travers le monde et dans de nombreux secteurs : finance, transports, santé, éducation, commercial, manufacturier et davantage.

> « Je le dis souvent : le sentiment de sécurité et le niveau réel de sécurité peuvent parfois être très différents, a déclaré David Hervieux, président et fondateur de Devolutions. Cette étude met en lumière les écarts pouvant exister entre l'impression d'avoir une posture solide et la réalité de la situation, sachant que le combat contre les cybermenaces évolue sans arrêt. Le but ici n'est jamais d'inquiéter, mais bien de sensibiliser les organisations et les encourager à être les plus résistantes et résilientes possibles. Cela fait partie de notre mission. »

Écart préoccupant entre confiance et capacité

Les résultats de l'étude menée par Devolutions démontrent que 71 % des PME se disent confiantes de pouvoir gérer un incident de cybersécurité majeur, mais seulement 22 % disposent réellement d'une posture suffisamment avancée pour résister aux attaques. Il est intéressant de noter que cette impression de confiance augmente à mesure que le rôle joué au sein de l'entreprise s'éloigne d'une spécialisation informatique et se rapproche d'un rôle de gestion.

Parallèlement, comparativement à l'étude de 2024, le niveau de confiance global a diminué de 9 % en 2025 et le nombre de PME se disant bien équipées a reculé de 8 %. Cela laisse entendre que les répondants sont aujourd'hui encore plus conscients des risques, mais moins certains de pouvoir réagir adéquatement en cas d'incident.

La gestion manuelle des accès privilégiés demeure trop fréquente

Bien que la protection des accès privilégiés aux systèmes, données et applications soit un pilier essentiel de tout plan de cybersécurité, une mince majorité des entreprises s'appuie sur des méthodes obsolètes pour gérer ces accès. 52 % des PME utilisent toujours des outils manuels, comme des documents ou des tableurs, alors que ce sont justement de telles sources que les rançongiciels et programmes d'intrusion prennent pour cible. Cette situation fait croître les risques d'incidents majeurs évitables.

Étonnamment, ces pratiques de gestion manuelle ont augmenté de 7 % entre 2024 et 2025. En effet, l'intégration de systèmes automatisés soulève des craintes parmi les entreprises et les fait hésiter, au détriment de leur posture de sécurité. Il faut les encourager à accélérer le déploiement de systèmes automatisés, sécurisés et renforcés de gestion des accès privilégiés, en démontrant aux décideurs à quel point les anciennes pratiques de gestion manuelle rendent leurs activités vulnérables.

L'utilisation de l'IA intéresse beaucoup, malgré les obstacles

Grâce à l'intelligence artificielle appliquée à la cybersécurité, les entreprises peuvent s'armer de la détection automatisée des menaces et des comportements inhabituels, entre autres mesures de protection. Les organisations se montrent enthousiastes à cet égard, 71 % ayant l'intention d'utiliser l'IA dans cet objectif et 62 % croyant que l'IA jouera un rôle critique d'ici cinq ans. Cependant, aujourd'hui, 40 % des répondants n'utilisent aucunement l'IA au sein de leur cybersécurité.

L'intérêt envers l'IA pour renforcer la posture de sécurité est clairement présent, mais des barrières se dressent : coûts, manque d'expertise, inquiétudes quant à la confidentialité, même une crainte de trop dépendre sur l'IA. L'important, c'est que l'utilisation de l'IA en cybersécurité semble inévitable pour la majorité.

Des budgets en hausse, mais mal répartis

Les budgets consacrés à la cybersécurité sont en croissance, 63 % des petites et moyennes entreprises y ayant alloué plus de fonds en 2025, mais ces ressources demeurent en-deçà des besoins pour contrecarrer l'augmentation des risques et menaces. Si 5 % des répondants ont lancé des programmes ambitieux représentant plus de 20 % de leur budget général, 29 % y consacrent moins de 5 %. 25 % ne connaissent pas le pourcentage.

Les équipes TI et de sécurité mentionnent des délais et des lacunes dans la mise en œuvre de nouvelles étapes de cybersécurité. 55 % font état de répartitions budgétaires mal équilibrées entre différents besoins, amenant ainsi un paradoxe entre progression budgétaire et ralentissement des avancées globales en matière de cybersécurité.

Un risque peu abordé : les menaces venues de l'intérieur

L'étude 2025 de Devolutions permet de démontrer que 78 % des PME sont préoccupées par des menaces pouvant venir de l'intérieur, mais seulement 20 % ont un plan pour contrer de tels risques. Malgré l'augmentation des vols de données et des sabotages effectués à l'interne, dans tous les secteurs à travers le monde, 28 % des entreprises sondées n'ont soit aucun plan en place, soit ne considèrent pas cela comme une menace prioritaire. De manière remarquable, la préoccupation à propos des menaces internes est montée en flèche entre 2024 et 2025, grimpant de 45 %. Pourtant, le nombre d'organisations ayant un plan de réponse n'a augmenté que de 5 %, même si les malfaiteurs internes peuvent plus facilement contourner les défenses de sécurité habituelles.

Les formations améliorent la cybersécurité

La cybersécurité va au-delà des outils sophistiqués, car il faut également que les spécialistes de l'entreprise soient formés pour exploiter efficacement ces outils et que le personnel sache comment éviter les pièges les plus courants. La pertinence des formations est claire : la majorité des brèches de sécurité sont le résultat d'une erreur humaine, allant d'une tentative d'hameçonnage réussie à la mauvaise configuration d'un système. Si 39 % des organisations répondantes offrent une formation continue et 32 % imposent une formation de sensibilisation, 17 % n'ont aucun programme à l'attention des talents pour assurer les meilleures pratiques et développer une culture de cybersécurité. Notons qu'entre 2024 et 2025, le nombre de petites et moyennes entreprises offrant de telles formations a reculé de 2 %.

Le fil conducteur du sondage sur la cybersécurité des PME

Au-delà des six faits saillants résultant de l'étude 2025 de Devolutions, un fil conducteur apparaît : les petites et moyennes entreprises prennent la cybersécurité au sérieux, toutefois elles peinent à mettre tous les éléments en œuvre pour renforcer leur posture de sécurité. La majorité souhaite y parvenir, mais le déploiement et la réalisation demeurent des défis. Selon le sondage, 43 % des PME ont connu au moins une cyberattaque au cours de la dernière année. Seulement 31 % ont été en mesure de détecter l'incident lors des premières minutes. La cybersécurité renforcée progresse, mais pas assez rapidement. Le plus grand de tous les risques étant de ne pas agir, la plupart des organisations sondées par Devolutions sont néanmoins sur la bonne voie.

Le rapport complet State of IT security in SMBs in 2025 est disponible ici.

Source : ITChannel – juillet 2025