Cybersécurité : l'alerte monte pour les entreprises françaises

16 janvier 2026 Cecile Vicini

Études, Cybersécurité

©LV4260 de Getty Images

Temps de lecture estimé : 5 minutes

Longtemps perçue comme un sujet technique, souvent relégué au second plan, elle s’impose désormais comme une priorité. Selon une étude des Echos Études (15 janvier 2026), la combinaison entre digitalisation accélérée de l’économie et sophistication des cyberattaques expose les entreprises à des risques mieux perceptibles.

Cette évolution concerne l’ensemble du tissu économique, des très petites entreprises aux grands groupes, dans un contexte où la dépendance aux outils numériques devient totale.

Une transformation numérique qui fragilise les organisations

Télétravail, solutions cloud, outils collaboratifs, mobilité professionnelle ou encore objets connectés : les systèmes d’information des entreprises se sont profondément transformés.

Cette modernisation a permis des gains de productivité, mais elle a aussi multiplié les points d’entrée pour les cyberattaques.

Les infrastructures reposent désormais sur des environnements hybrides et interconnectés, souvent difficiles à cartographier et à sécuriser.

Pour de nombreuses entreprises, en particulier les TPE et PME, cette complexité dépasse les capacités internes de gestion des risques numériques.

Des attaques plus discrètes et plus ciblées

Face à ces nouveaux environnements, les cybercriminels affinent leurs méthodes. Les attaques deviennent plus furtives, plus ciblées et plus difficiles à détecter.

→ L’objectif n’est plus uniquement de bloquer un système, mais de s’y maintenir, d’exfiltrer des données ou de perturber l’activité au moment le plus critique.

Ransomwares, hameçonnage, exploitation de failles logicielles ou attaques via des prestataires figurent parmi les modes opératoires les plus répandus.

Pour les entreprises, les conséquences sont multiples :

- interruption de l’activité,
- pertes financières,
- atteinte à la réputation,
- fragilisation de la relation client.

Le risque cyber s’impose comme une priorité

En France, la menace cyber est désormais perçue comme l'un des principaux risques pesant sur les organisations. Une part croissante des entreprises constate une augmentation des attaques, tandis que les dirigeants placent la cybersécurité au cœur de leurs préoccupations stratégiques.

Les cyberattaques visant des hôpitaux, des collectivités ou des entreprises industrielles ont contribué à accélérer cette prise de conscience.

→ Elles montrent que toutes les structures peuvent être ciblées, indépendamment de leur taille ou de leur secteur, et que les impacts peuvent être immédiats et durables.

Pour les petites entreprises, souvent moins préparées, une attaque peut suffire à désorganiser l'ensemble de l'activité, voire à compromettre la continuité de l'entreprise.

Un marché de la cybersécurité en forte croissance

Dans ce contexte, le marché français de la cybersécurité connaît une croissance soutenue. Les investissements se multiplient dans les solutions de protection, les services spécialisés et l'accompagnement des entreprises.

Cette dynamique est portée par la hausse des cybermenaces, mais aussi par le renforcement du cadre réglementaire (transposition de la directive NIS 2, l'entrée en vigueur de textes comme DORA ou le Cyber Resilience Act, ainsi que le développement de normes telles que l'ISO 27001) et par les

exigences croissantes des clients et partenaires. Elle devient progressivement un critère de confiance et de crédibilité économique, notamment dans les relations de sous-traitance.

Des obligations réglementaires pour mieux encadrer

L'étude souligne également l'impact croissant des réglementations européennes et nationales sur les entreprises. Directives, règlements sectoriels et normes de sécurité imposent des exigences accrues en matière de gouvernance des systèmes d'information, de gestion des incidents et de protection des données.

Même lorsque les obligations ne s'appliquent pas directement, leurs effets se diffusent dans l'ensemble de l'écosystème économique. Les entreprises sont de plus en plus sollicitées pour démontrer leur niveau de sécurité, transformant la cybersécurité en enjeu de pilotage global.

Sensibilisation et organisation interne

Pour les dirigeants, la cybersécurité ne peut plus être abordée uniquement comme un poste de dépenses informatiques. Elle implique une approche transversale, associant direction générale, équipes opérationnelles et collaborateurs.

La sensibilisation des salariés apparaît comme un levier majeur. De nombreuses attaques trouvent leur origine dans des erreurs humaines : clic sur un lien frauduleux, mot de passe insuffisamment sécurisé, usage non maîtrisé des outils

numériques. Former les équipes et structurer les procédures devient un investissement stratégique.

Assurance cyber et nouvelles technologies

Parmi les évolutions récentes, l’assurance cyber s’impose comme un outil complémentaire de gestion du risque, sans se substituer à une politique de prévention solide. En parallèle, la pénurie de compétences spécialisées pousse les acteurs publics et privés à développer des programmes de formation et à renforcer les coopérations.

Les technologies émergentes, notamment l’intelligence artificielle, ouvrent de nouvelles perspectives pour la détection et la réponse aux incidents, tout en introduisant de nouveaux défis en matière de sécurité.

Un enjeu de pérennité pour les entreprises

À l’horizon 2030, la cybersécurité s’affirme comme un facteur essentiel de la performance et de la crédibilité des entreprises françaises. Elle ne se limite plus à la protection technique des systèmes, mais conditionne la capacité des organisations à opérer durablement dans une économie numérisée et exposée en permanence aux menaces.

Pour les dirigeants, intégrer la cybersécurité dans la stratégie globale de l’entreprise est désormais une condition de continuité et de compétitivité.