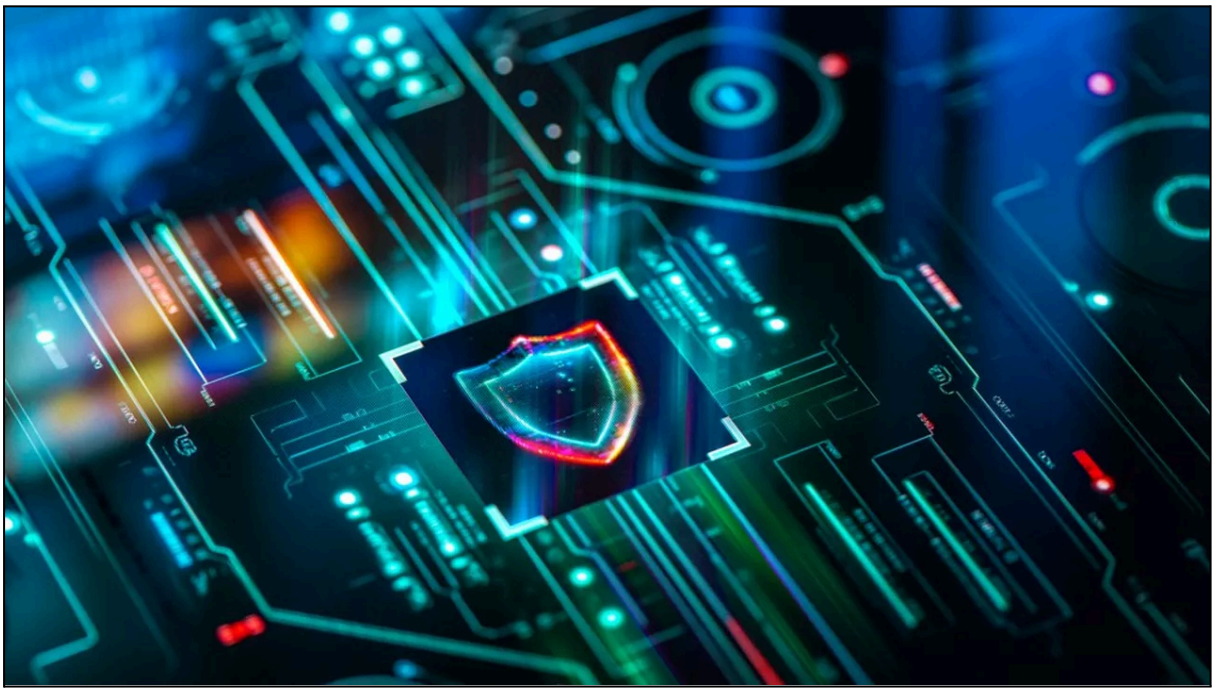
Accédé le 20 décembre 2025 via l'URL:

https://www.lesechos.fr/tech-medias/hightech/cybersecurite-les-entreprises-a-la-traine-face-a-la-vague-ia-2205447

Cybersécurité : les entreprises à la traîne face à la vague IA

Par Thomas Pontiroli, **18 décembre 2025**

Les cyberattaques dopées à l'IA progressent rapidement. Selon le Boston Consulting Group, 60 % des attaquants utilisent déjà l'IA, contre seulement 7 % des entreprises pour se défendre. Ce retard, lié à des budgets limités et un manque de compétences, expose les organisations à des risques croissants.



Seules 5 % des organisations déclarent avoir augmenté leurs budgets de cybersécurité en lien direct avec l'IA. (Photo iStock)

Au jeu du chat et de la souris, bien connu dans le monde de la cybersécurité, le premier a pris de l'avance sur le second grâce à l'IA. D'après une étude du Boston Consulting Group publiée jeudi, déjà 60 % des attaquants ont mis à profit les

nouvelles prouesses de l'intelligence artificielle pour mener des campagnes malveillantes, tandis qu'à peine 7 % des entreprises ont décidé de mettre l'IA de leur côté pour se protéger.

Pour le BCG, ce décrochage est d'autant plus préoccupant que la menace est désormais identifiée par les décideurs : selon l'étude, 53 % des dirigeants interrogés classent les cyberattaques dopées à l'IA parmi les trois principaux risques pesant sur leur organisation. Dans les faits, 14 % déclarent avec certitude avoir subi une attaque intégrant de l'IA au cours des douze derniers mois, et 46 % estiment que cela est très probable.

Combattre l'IA avec l'IA

L'étude, menée auprès de 500 dirigeants (dirigeants exécutifs, responsables cybersécurité et membres de comités de direction) dans toutes les grandes régions du monde, dans la banque, la santé, l'énergie ou la tech, met en évidence un retard généralisé. Dans l'immense majorité des cas, aucune stratégie structurée n'a été définie pour contrer les usages malveillants de l'IA ou pour renforcer les défenses grâce à ces technologies.

« L'IA générative a introduit des mécaniques non déterministes, qui sont plus difficiles à déjouer par les méthodes classiques », explique Vanessa Lyon, managing director et senior partner au BCG. Autrement dit : il est difficile de parer les attaques cyber IA… sans bouclier IA.

Le premier facteur expliquant le retard des entreprises est budgétaire. Malgré la montée en puissance des attaques, seules 5 % des organisations déclarent avoir augmenté leur budget de cybersécurité en lien direct avec l'IA. Mais pour Vanessa Lyon, « les ressources d'une entreprise ne sont pas qu'une question d'argent, mais aussi de compétences ». Or c'est un autre frein majeur.

Entre R&D et start-up

Près de 69 % des entreprises interrogées par le BCG disent rencontrer des difficultés pour recruter des profils combinant une double expertise cyber et IA. Un déficit qui limite la capacité à déployer et à opérer des dispositifs de défense avancés, même lorsque la volonté existe, pointe l'étude.

A cela s'ajoute une offre technologique encore immature. Parmi les entreprises ayant déjà adopté des outils de cyberdéfense basés sur l'IA, seules 25 % estiment disposer de solutions réellement avancées. « La plupart des projets les plus avancés sont soit en phase de R&D, soit portés par des start-up auxquelles les grands groupes n'accordent pas pleinement leur confiance », pointe Vanessa Lyon.

Seulement, en face, les attaquants exploitent déjà des techniques industrialisées : phishing généré par IA à grande échelle, deepfakes vocaux ou vidéo, fraudes financières automatisées ou malwares capables d'adapter leur comportement en temps réel. « N'importe qui peut mener des campagnes malveillantes. Nous voyons même des groupes proposant des rançongiciels sur étagère et des centres d'appels accompagner les offensives », illustre Vanessa Lyon.

Le risque d'un retard incurable

Pour le BCG, ce déséquilibre pourrait encore s'accentuer avec l'émergence des IA agentiques, capables d'agir de manière autonome. Dans un contexte de flou réglementaire persistant - 70 % des entreprises disent mal connaître les textes en vigueur - le risque est que, sans réveil des entreprises, elles puissent durablement rester à la traîne face à des attaquants qui redoublent d'ingéniosité.

L'argument massue qu'aime à remettre sur la table le BCG pour tenter de convaincre les directions : selon une précédente étude, une entreprise sur six concernée par une attaque cyber voit son cours de Bourse chuter de plus de 5 %, et deux tiers continuent à sous-performer un an plus tard.