**L'IA et la cybersécurité en entreprise**

**Un enjeu majeur pour les entreprises.**

La cybersécurité est devenue un enjeu stratégique pour les organisations. Les cyberattaques se multiplient, gagnent en sophistication et peuvent avoir des conséquences graves sur l'activité d'hôpitaux, de collectivités ou d'entreprises privées.

Avec l'évolution de l'intelligence artificielle (IA), les attaques sont désormais plus automatisées, plus rapides et plus difficiles à détecter. Les cybercriminels utilisent notamment l'IA générative pour : Créer des programmes malveillants / Automatiser le scan de réseaux / Perfectionner des campagnes de phishing

Ces attaques exploitent fréquemment la faille humaine pour pénétrer les systèmes informatiques.

**L'IA : un outil offensif… mais aussi défensif**

Si l'IA renforce les capacités des pirates, elle constitue également un outil essentiel de défense. Des entreprises comme Microsoft (avec Microsoft Defender et Azure Security Center) ou CrowdStrike (avec la Falcon Platform) intègrent l'IA dans leurs solutions afin de : Détecter les menaces en temps réel / Analyser d'importants volumes de données / Anticiper et prévenir les attaques

À l'échelle internationale, la coopération s'intensifie également. À Singapour, Interpol a mis en place un centre de cyber analyse capable de traiter des millions de données (adresses web, logiciels malveillants, codes de pirates).
En 2025, l'opération « Secure » menée en Asie a permis de neutraliser 20 000 adresses IP et domaines malveillants liés à des groupes criminels.

**Les limites et les choix stratégiques pour les entreprises**

Malgré ses avantages, l'IA n'est pas encore adoptée partout. Plusieurs freins existent : Risque de détournement à des fins malveillantes / Manque de compétences internes / Coût élevé

**Utiliser une IA développée par un fournisseur externe**

Les entreprises peuvent choisir des solutions déjà existantes (comme celles proposées par CrowdStrike ou Microsoft). Avantages : Déploiement rapide / Expertise avancée / Mise à jour continue. Inconvénients : Risque pour la confidentialité des données / Moins de contrôle sur l'algorithme / Dépendance au fournisseur / En cas d'attaque du fournisseur, les entreprises clientes peuvent être impactées

**Développer sa propre IA en interne**

Une autre option consiste à créer une IA interne. Le coût peut varier entre 30 000 € et 300 000 €, voire davantage selon la complexité du projet. Avantages : Contrôle total des données / Indépendance vis-à-vis d'un fournisseur / Adaptation parfaite à l'environnement de l'entreprise

/ Potentiel avantage concurrentiel Inconvénients : Investissement financier important / Besoin d'experts spécialisés / Maintenance continue

**Conclusion**

L'intelligence artificielle joue aujourd'hui un double rôle dans la cybersécurité : Elle renforce les capacités des cybercriminels / Elle constitue un levier stratégique majeur pour la défense des entreprises

L'enjeu futur pour les organisations sera d'adopter et d'exploiter l'IA plus rapidement et plus efficacement que les attaquants, afin de transformer cette technologie en avantage compétitif plutôt qu'en vulnérabilité.

Source : CNews, ITSocial, Bilan