Les 5 principales

TENDANCES EN MATIÈRE DE CYBERSÉCURITÉ POUR 2025

GILLES DAGUET

Responsable de la stratégie de Private Equity dédiée à la cybersécurité

FRANÇOIS LAVASTE

Executive Director, Stratégie de Private Equity dédiée à la cybersécurité

TIKEHAU CAPITAL

Les 5 principales tendances en matière de cybersécurité pour 2025

Depuis le lancement de sa **stratégie d'investissement en Private Equity** dédiée à la **cybersécurité en 2019**[1], Tikehau Capital est à l'avant-garde pour identifier et soutenir des solutions à l'un des défis les plus pressants d'aujourd'hui : la cybersécurité.

La cybersécurité est devenue une mégatendance mondiale, portée par la numérisation rapide des économies, l'explosion de la production de données et l'augmentation de la fréquence et de la sophistication des cyberattaques. En outre, des **cadres réglementaires** tels que la directive **NIS2**, le règlement **Cyber Résilience Act** et le règlement **DORA** transforment le paysage, en particulier en Europe, et créent de nouveaux défis et de nouvelles opportunités pour les entreprises.

Pour garder une longueur d'avance, nous avons identifié **les 5 principales tendances cyber pour 2025 – des prévisions** qui reflètent l'évolution dynamique du secteur. Ces prévisions seront réexaminées dans 12 mois afin d'évaluer leur exactitude et leur impact.

Principales étapes

DE LA STRATÉGIE DE TIKEHAU CAPITAL EN MATIÈRE DE CYBERSÉCURITÉ

Guider l'innovation cyber et la résilience dans l'économie numérique.

ANNÉE DE LANCEMENT : 2019

ACTIFS SOUS GESTION :

500 millions d'euros

dédiés à la cybersécurité[2] (à partir de septembre 2024)

[1] Tout investissement comporte des risques, y compris, mais sans s'y limiter, la perte de capital.
[2] La stratégie de cybersécurité comprend un véhicule géré par Tikehau Investment Management, réservé aux investisseurs qualifiés et qui n'est plus ouvert à la commercialisation et à la souscription.

DÉMOCRATISATION DE LA CYBERSÉCURITÉ : personne n'est à l'abri

En 2025, chaque appareil et réseau connecté – qu'il s'agisse de technologies de l'information[3] (IT) ou de technologies opérationnelles[4] (OT) – deviendra une cible potentielle pour les cyberattaques.

- Les grandes organisations restent à risque en raison des erreurs humaines et de l'attrait qu'elles exercent sur les cybercriminels.
- Les petites et moyennes entreprises (PME) et les professionnels sont des cibles plus faciles, souvent dépourvues de défenses solides.
- Les attaquants s'appuient désormais sur l'**automatisation** et l'**IA** pour industrialiser les campagnes, augmentant l'ampleur et la sophistication des attaques de phishing, de ransomware et de deepfakes.

Cette menace universelle entraîne une augmentation des **fusions et acquisitions dans le domaine de la cybersécurité**, avec la confirmation de l'arrivée d'acquéreurs non cyber. Parmi les exemples notables de 2024, citons l'acquisition de Recorded Future par MasterCard et celle d'Own Company par Salesforce.

L'impact DE L'IA

L'IA transforme la cybersécurité, mais donne aussi du pouvoir aux attaquants.

- **Attaquants :** L'IA permet des tactiques sophistiquées comme les campagnes basées sur les deepfakes, les contournements de CAPTCHA et l'hameçonnage ciblé. Selon les prévisions, 17% des attaques et des fuites de données en 2025 impliqueront l'IA générative (source : *Gartner, août 2024*).
- **Défenseurs :** L'IA améliore la gestion des données, la productivité et la réponse automatisée aux menaces, tout en créant un nouveau défi : la défense de l'IA elle-même.
- **Gouvernance de l'IA :** L'IA transparente et explicable devient essentielle pour maintenir la confiance et la conformité réglementaire, tout comme la gouvernance des données a évolué, le pilotage de la gouvernance de l'IA devient un enjeu essentiel.

LE *CRYPTOJACKING* fait son retour

L'augmentation du prix des crypto-monnaies fait du *cryptojacking* – une forme de minage illégal de crypto-monnaies – une alternative attrayante pour les attaquants.

- Contrairement au ransomware, le *cryptojacking* draine silencieusement les ressources sans causer de perturbations majeures, ce qui le rend plus difficile à détecter.
- Avec un retour sur investissement élevé et une visibilité réduite, les logiciels malveillants de *cryptojacking* devraient représenter une menace de plus en plus importante en 2025.

[3] Les technologies de l'information sont l'utilisation d'ordinateurs, de dispositifs de stockage, de réseaux et d'autres dispositifs physiques, d'infrastructures et de processus pour créer, traiter, stocker, sécuriser et échanger toutes les formes de données électroniques.

[4] La technologie opérationnelle est la pratique qui consiste à utiliser du matériel et des logiciels pour contrôler l'équipement industriel, et elle interagit principalement avec le monde physique.

4 Intensification
DE LA GUERRE HYBRIDE CYBERPHYSIQUE

Les tensions et conflits géopolitiques mondiaux continuent d'inspirer des **tactiques de guerre hybride cyberphysique :**

- Les attaques contre les infrastructures physiques (par exemple, les télécommunications, les réseaux électriques, les satellites) peuvent perturber les services essentiels et créer des vulnérabilités cybernétiques.
- Les cyberattaques peuvent à leur tour avoir des conséquences physiques, ce qui met en évidence l'interconnexion des menaces physiques et numériques.
- Les scénarios hybrides exploitant les faiblesses cyber critiques devraient se multiplier, posant des défis à la résilience des infrastructures.

5 Le retour de bâton
DE LA PLATEFORMISATION

La consolidation des outils de cybersécurité au sein de plateformes unifiées permet de réaliser des gains d'efficacité, mais présente des risques importants :

- **Avantages :** Les plateformes unifiées réduisent les angles morts, rationalisent les opérations et permettent une application cohérente des politiques.
- **Risques :** Le fait de s'appuyer sur une seule plateforme crée des points de défaillance uniques potentiels. Par exemple, la mise à jour erronée de CrowdStrike Falcon en juillet 2024 a provoqué une perturbation généralisée, clouant au sol 42 000 vols et affectant 8 millions d'appareils.

En 2025, les organisations donneront la priorité à l'équilibre entre l'**efficacité des plateformes**, la **redondance et la gestion des risques**, en évitant une trop forte dépendance à une solution unique.