CYBERATTAQUES & IA

TENDANCES 2026

ozngo

Implications pour les organisations

10 500 Md$

Coût mondial cybercriminalité 2026

+72%

Cyberattaques IA YoY 2025

87%

Organisations visées par une attaque IA

LE PAYSAGE DES MENACES 2026

5 vecteurs d'attaque redéfinis par l'IA

ozngo

+1 265% — **Ingénierie sociale IA**

de phishing IA depuis 2023. 82,6% des emails de phishing contiennent du contenu IA.

Taux de clic x4 vs phishing humain.

97% — **Data poisoning**

des organisations touchées n'avaient aucun contrôle d'accès sur leurs modèles IA (IBM 2025).

13% ont déjà subi une violation de modèle.

+160% — **Inversion de modèles**

de vols d'identifiants IA en 2025. Vol de PI, espionnage industriel, rançon via extraction de modèles exposés.

69% — **Adversarial ML**

de mauvais diagnostics sur mammographies manipulées (UPMC Nature). Invisible à l'œil humain — vaut pour tout modèle décisionnel.

79% — **Supply Chain IA/Cloud**

des entreprises cloud ont subi une violation. Attaque 'one-to-many' via fournisseur central compromis.

Sources : IBM X-Force 2025 · Verizon DBIR 2025 · FBI IC3 · Microsoft Cyber Signals 2025 · SlashNext · CrowdStrike

LE HACKER 2026

Il attaque

- Vos données & modèles IA
- Votre perception de la vérité
- Vos émotions & biais cognitifs
- Vos chaînes de dépendance
- Le contournement MFA
- Vos infrastructures cloud

Son objectif

Crédibilité & Confiance
Fragmenter la vérité interne

Pertes en domino
Avoirs, business, réputation

Décisions biaisées
Via modèles IA compromis

Paralysie opérationnelle
53 000$/h de downtime moyen

93% des dirigeants anticipent des attaques IA quotidiennes d'ici fin 2026 - WEF Global Cybersecurity Outlook 2026

LES IMPLICATIONS CONCRETES

Les questions à se poser impérativement… entre autres

Communication de Crise

Avons-nous un narratif prêt pour une 'erreur IA' ? Notre communication est-elle alignée avec nos fournisseurs cloud ?

Gouvernance de la Vérité

Qui détient la vérité dans l'entreprise ? En combien de temps peut-on contrer un deepfake ou un faux rapport ?

Culture & Réflexes Humains

Nos équipes savent-elles identifier les signaux d'une IA manipulée ? Avons-nous un protocole 'stop-the-line IA' ?

Intégrité des Modèles IA

Nos modèles IA sont-ils monitorés contre la corruption ? Avons-nous un plan B sans IA si un modèle est compromis ?

Chaîne de Dépendance

Avons-nous cartographié nos fournisseurs IA/cloud ? Qui contrôle la sécurité de chaque maillon ?

Propriété Intellectuelle

Nos endpoints IA sont-ils protégés ? Avons-nous des preuves techniques si un modèle propriétaire est volé ou cloné ?

SIX LEVIERS IMMÉDIATS

Les fondations indispensables d'une défense moderne

Gouvernance de la vérité et stratégie de la preuve

Définir comment on établit ce qui est vrai, ce qui est douteux, qui tranche et comment. Protéger & authentifier les contenus officiels sensibles.

Circuit interne d'alertes & de veille critiques (spécial PME)

Canal simple pour remonter incidents, signaux faibles, incohérences IA et éléments repérés en ligne. Agréger, filtrer, diffuser l'info utile, même sans équipe cyber.

Résilience élargie à l'humain, au culturel et aux réflexes de décision

Approche psychologique et systémique de la résilience pour cultiver vigilance, cohésion et réflexes efficaces en situation d'incertitude, de manipulation.

Maîtrise de sa communication sous pression

Entraîner les dirigeants et porte-parole à gérer doute, confusion ou désinformation. Une parole structurée dès les premières minutes change tout.

Tests et Simulations en conditions réelles

Scénarios IA, faux messages, deepfakes, vishing, signaux contradictoires, etc. On ne teste pas son plan le jour de la crise.

Esprit critique & réflexes anti-manipulation

Former les équipes à repérer les signaux cognitifs faux, réagir sans panique, adopter les réflexes de protection et signaler factuellement les anomalies.

Un leadership préparé, sans budget cyber massif.

QUI EST OZNGO

Maryse Rebillot

Strategic Advisor on Cyber-AI crises and information integrity

- 20+ ans en marketing-communication dans le High Tech et la Cybersécurité
- Experte en gestion de crise, Communication sensible et Intégrité de l'Information
- International Executive Marketing Master, INSEAD

linkedin.com/in/maryse-rebillot

Réseau d'Experts

(mobilisables selon les missions, en fonction des besoins)

Cybersécurité

Cyber défense, White Hacking, Gouvernance Cyber, Gouvernance des données, Légal & Assurance

IA & Technologies

IA Générative, LLM, IA Vertical, Autres IA

Humain & Communication

Psychologie, Médias & Journalistes, Sociologie

À L'ÈRE DE L'IA, LA SEULE DÉFENSE DURABLE

c'est la cohésion humaine.

ozngo

contact@ozngo.com