DCOD - 2026

CYBERMENACES EN SUISSE

État des lieux, volumes d'attaques et évolution technologique sur le territoire suisse.

SOURCES : OFCS / CHECK POINT / ALLIANZ / SOPHOS 2026

TENDANCES CLÉS EN 2026

IA de Précision

L'IA générative automatise désormais la personnalisation des emails de phishing en français, allemand et italien.

SOURCE : CHECK POINT MIERCOM 2026

Législation

L'obligation d'annonce pour les infrastructures critiques révèle une fragilité accrue des services vitaux.

SOURCE : OFCS RAPPORT ANNUEL 2026

Identité

89% des organisations suisses ont subi une violation d'identité au cours des 12 derniers mois.

SOURCE : SOPHOS STATE OF IDENTITY 2026

VOLUME GLOBAL DES SIGNALEMENTS

64'733

Cas traités en un an

Le volume de signalements volontaires à l'Office Fédéral (OFCS) reste historiquement haut, marquant une pression constante sur le tissu économique.

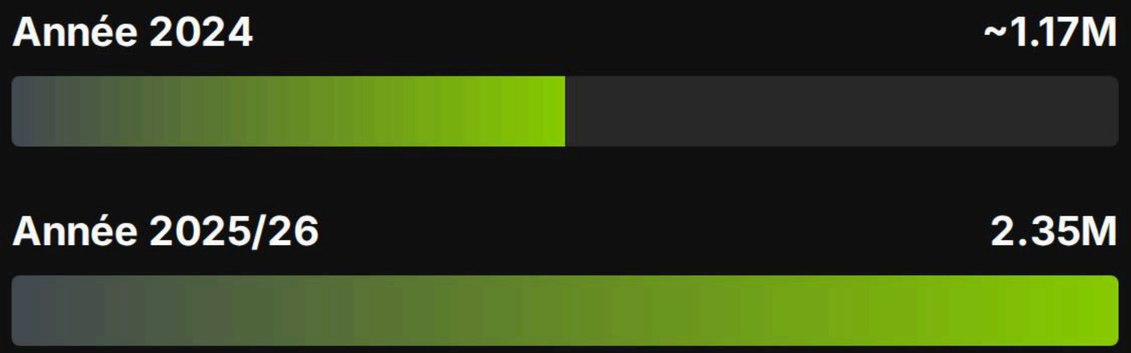
SOURCE : OFFICE FÉDÉRAL DE LA CYBERSÉCURITÉ (FÉV. 2026)

INFECTIONS PAR MALWARES

2'347'618 appareils infectés ont été identifiés par les capteurs fédéraux.

Ce chiffre représente une multiplication par deux du nombre de détections par rapport à l'année précédente, illustrant une prolifération massive de codes malveillants.

SOURCE : STATISTIQUES OFCS 2026



INFRASTRUCTURES CRITIQUES

260+ Signalements

Nombre d'incidents critiques rapportés par les exploitants d'infrastructures vitale (énergie, eau, santé) depuis la mise en œuvre de la nouvelle loi.

- **Énergie :** Secteur le plus visé par les tentatives d'intrusion.
- **Santé :** Forte pression des ransomwares sur les hôpitaux.

SOURCE : RAPPORT ANNONCE OBLIGATOIRE OFCS 2026

LE RISQUE MAJEUR DES ENTREPRISES

42%

Risque n°1 en Suisse

Pour la 5ème année consécutive, le risque cyber supplante les interruptions d'activité et les catastrophes naturelles dans les préoccupations des dirigeants.

SOURCE : ALLIANZ RISK BAROMETER SUISSE 2026

VULNÉRABILITÉ DES IDENTITÉS

Catégorie de Risque	Taux de Violation (Suisse)	Impact
Moyenne Nationale	**89 %**	Taux le plus élevé au monde
Secteur Public / Énergie	80 %	Menace sur les services vitaux
Services Financiers	75 %	Risque de fraude massive

SOURCE : SOPHOS STATE OF IDENTITY SECURITY (MAI 2026)

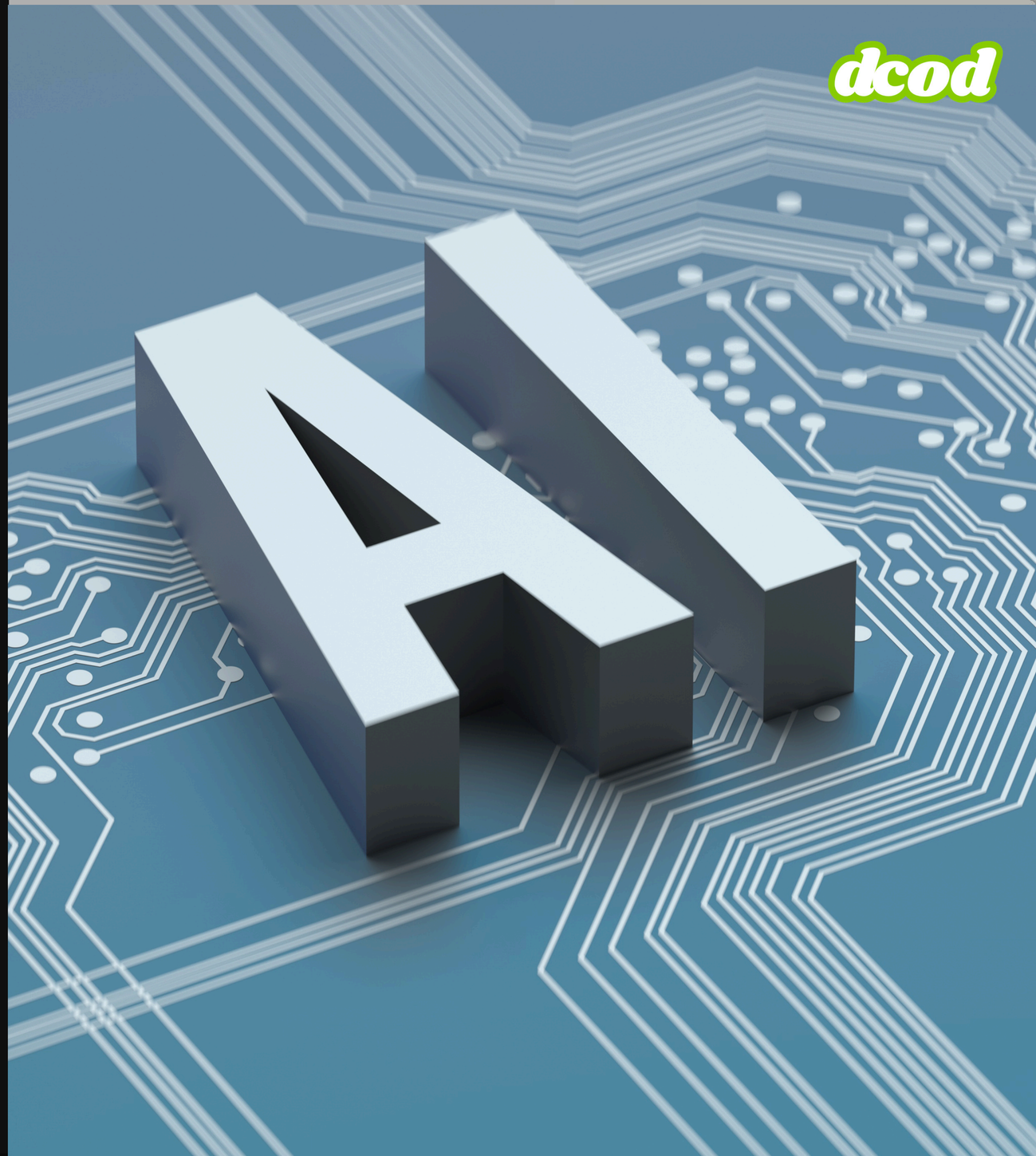
L'IA : L'ARME À DOUBLE TRANCHANT

+56% de Détection

Si l'IA générative facilite la fraude, les outils de détection basés sur l'IA (EDR/XDR) augmentent l'efficacité des réponses de 56% dans les premières 24h.

Phishing 2.0 : L'IA permet désormais de cloner parfaitement la voix d'un dirigeant pour valider des virements frauduleux.

SOURCE : CHECK POINT RESEARCH / MIERCOM 2026



FRAGILITÉ DU TISSU PME

- **36% des PME suisses** déclarent avoir déjà subi une cyberattaque réussie.
- **Double Extorsion :** Dans 82% des cas de ransomwares, les données sont volées avant d'être cryptées.
- **Coût moyen :** Environ 850'000 CHF par sinistre majeur pour une PME.

SOURCE : GFS BERN / CYBERVERSICHERUNG.CH 2026

PRESSION HEBDOMADAIRE

1'093

Attaques / Semaine / Organisation

Bien que le volume global ait baissé de 11% début 2026, la précision du ciblage maintient une menace critique sur chaque entreprise helvétique.

SOURCE : CHECK POINT RESEARCH SUISSE (JANV. 2026)

IMPÉRATIFS STRATÉGIQUES

Gouvernance Identité

Déploiement MFA et Zero-Trust face au taux de violation de 89%.

Défense Active (MDR)

Externalisation du SOC pour une réponse 24/7 face à l'IA adverse.

Culture Risque

Sensibilisation ciblée sur les deepfakes et la fraude au vishing.

SOURCE : CONSEIL FÉDÉRAL - CYBERSTRATÉGIE NATIONALE 2026

Lire la suite sur dcod.ch

dcod

Cybersécurité • IA • Tech

Capter l'info, retenir l'essentiel

Newsletter – dcod.ch

Telegram – @ledecodeur

Discord – DCOD