VARGROUP

CYBER EXPOSURE

Que voit un attaquant lorsqu'il observe votre entreprise ?

Actifs exposés, informations publiques et visibilité des dirigeants : la préparation d'une attaque peut commencer par ce qui est déjà en ligne.

01

Trois dimensions à observer

A

Actifs numériques

Sites, applications, services cloud et accès à distance joignables depuis Internet.

CE QU'ILS PEUVENT RÉVÉLER

Des points d'entrée possibles et des services à analyser.

B

Informations sur l'entreprise

Documents, communiqués, offres d'emploi et contenus publiés en ligne.

CE QU'ILS PEUVENT RÉVÉLER

Technologies utilisées, rôles, projets et relations commerciales.

C

Visibilité des dirigeants

Profils professionnels, interviews et participations à des événements.

CE QU'ILS PEUVENT RÉVÉLER

Responsabilités, contacts et contextes utiles pour usurper l'identité d'une figure d'autorité.

02

Le risque augmente quand les informations se recoupent

Un nom · Un projet · Un partenaire · Un service exposé

→ Contexte de l'entreprise reconstitué

Pris isolément, ils peuvent sembler anodins. Combinés, ils aident un attaquant à reconstituer le contexte de l'entreprise.

Être visible en ligne ne signifie pas être vulnérable. Comprendre ce que cette visibilité révèle aide à évaluer le risque.

03

D'une information publique à une attaque ciblée

1 **Collecte**

Repérage d'informations sur l'entreprise, les personnes et les actifs numériques.

2 **Corrélation**

Mise en relation des rôles, partenariats, événements et projets.

3 **Message crédible**

Création d'une communication qui évoque des personnes et des activités réelles.

4 **Compromission possible**

Si le destinataire est trompé, l'attaque peut mener au vol d'identifiants ou à l'accès à des informations confidentielles.

EXEMPLE ILLUSTRATIF

1. Une publication annonce un nouveau partenariat.
2. Un profil public identifie le responsable du projet.
3. **Un faux e-mail du partenaire demande d'accéder à un document partagé.**

04

Qu'est-ce qui peut être menacé ?

01 **Comptes et informations confidentielles**

02 **Processus et continuité des activités**

03 **Réputation de l'entreprise**

05

Regardez votre entreprise de l'extérieur

01 **Cartographiez les actifs accessibles depuis Internet.**

02 **Évaluez quelles informations publiques peuvent être recoupées.**

03 **Analysez l'exposition des cadres dirigeants.**

04 **Définissez les priorités d'intervention.**

Si un attaquant observait votre entreprise aujourd'hui, que verrait-il ?

Approfondissez le sujet en téléchargeant le livre blanc!

EN SUISSE AUSSI, LE RISQUE EST RÉEL

PRÈS DE

65 000

signalements de cyberincidents reçus par l'OFCS en 2025.

19 %

des signalements concernent le phishing.

ENVIRON

+35 %

de signalements de fraude au CEO: de 719 en 2024 à 970 en 2025.

ET LES PME SUISSES ?

37 %

des PME ont déjà été victimes d'une cyberattaque, contre 20 % en 2023[1].

42 %

des PME s'estiment suffisamment protégées en cas d'attaque. Elles étaient 55 % un an plus tôt[2].

58 %

des signalements à l'OFCS au premier semestre 2025 concernent des escroqueries[3].

L'identité d'un dirigeant peut devenir un instrument de tromperie.

Source : OFCS, bilan 2025. Variation des signalements de fraude au CEO calculée sur les valeurs publiées. Les signalements ne représentent pas la totalité des attaques survenues en Suisse.
[1] Deloitte, étude sur les conseils d'administration, septembre 2026 (estimation des membres des CA). [2] Étude « Cybersécurité dans les PME 2025 », digitalswitzerland, la Mobilière et partenaires. [3] OFCS, rapport semestriel 2025/1.

VARGROUP