VARGROUP

CYBER EXPOSURE

Cosa vede un attaccante quando guarda la tua azienda?

Asset esposti, informazioni pubbliche e visibilità dei dirigenti: la preparazione di un attacco può iniziare da ciò che è già online.

01

Tre dimensioni da osservare

A

Asset digitali

Siti, applicazioni, servizi cloud e accessi remoti raggiungibili da Internet.

COSA POSSONO RIVELARE

Possibili punti di ingresso e servizi da analizzare.

B

Informazioni aziendali

Documenti, comunicati, annunci di lavoro e contenuti pubblicati online.

COSA POSSONO RIVELARE

Tecnologie utilizzate, ruoli, progetti e relazioni commerciali.

C

Visibilità dei dirigenti

Profili professionali, interviste e partecipazioni a eventi.

COSA POSSONO RIVELARE

Responsabilità, contatti e contesti utili per impersonare una figura autorevole.

02

Il rischio cresce quando le informazioni si collegano

Un nome · Un progetto · Un partner · Un servizio esposto

→ Contesto aziendale ricostruito

Presi singolarmente possono sembrare dettagli innocui. Combinati, aiutano un attaccante a **ricostruire il contesto aziendale.**

Essere visibili online non significa essere vulnerabili. Comprendere ciò che questa visibilità rivela aiuta a valutare il rischio.

03

Da un'informazione pubblica a un attacco mirato

1 **Raccolta**

Individuazione di informazioni su azienda, persone e asset digitali.

2 **Correlazione**

Collegamento di ruoli, partnership, eventi e progetti.

3 **Messaggio credibile**

Creazione di una comunicazione che richiama persone e attività reali.

4 **Possibile compromissione**

Se il destinatario viene ingannato, l'attacco può portare al furto di credenziali o all'accesso a informazioni riservate.

ESEMPIO ILLUSTRATIVO

1. Un post annuncia una nuova partnership.
2. Un profilo pubblico identifica il responsabile del progetto.
3. **Una falsa email del partner chiede di accedere a un documento condiviso.**

04

Cosa può essere a rischio?

01 **Account e informazioni riservate**

02 **Processi e continuità operativa**

03 **Reputazione aziendale**

05

Guarda la tua azienda dall'esterno

01 **Mappa gli asset accessibili da Internet.**

02 **Valuta quali informazioni pubbliche possono essere correlate.**

03 **Analizza l'esposizione delle figure apicali.**

04 **Definisci le priorità di intervento.**

Se oggi un attaccante osservasse la tua azienda, cosa vedrebbe?

Approfondisci il tema scaricando il whitepaper gratuito

ANCHE IN SVIZZERA, IL RISCHIO È CONCRETO

QUASI

65.000

segnalazioni di cibericidenti ricevute dall'UFCS nel 2025.

19%

delle segnalazioni riguarda il phishing.

CIRCA

+35%

le segnalazioni di frode del CEO: da 719 nel 2024 a 970 nel 2025.

E LE PMI SVIZZERE?

37%

delle PMI è già stato vittima di un ciberattacco, contro il 20% del 2023[1].

42%

delle PMI si ritiene adeguatamente protetto in caso di attacco. Erano il 55% un anno prima[2].

58%

delle segnalazioni all'UFCS nel primo semestre 2025 riguarda truffe[3].

L'identità di un dirigente può diventare uno strumento di inganno.

Fonte: UFCS, bilancio 2025. Variazione delle segnalazioni di frode del CEO calcolata sui valori pubblicati. Le segnalazioni non rappresentano il totale degli attacchi avvenuti in Svizzera. [1] Deloitte, studio sui consigli di amministrazione, settembre 2026 (stima dei membri dei CdA). [2] Studio «Cybersicurezza nelle PMI 2025», digitalswitzerland, Mobiliare e partner. [3] UFCS, rapporto semestrale 2025/I.

VARGROUP