VARGROUP

CYBER EXPOSURE

What does an attacker see when they look at your company?

Exposed assets, public information and executive visibility: preparing an attack can start with what is already online.

01

Three dimensions to watch

A

Digital assets

Websites, applications, cloud services and remote access reachable from the Internet.

WHAT THEY CAN REVEAL

Possible entry points and services to probe.

B

Company information

Documents, press releases, job postings and content published online.

WHAT THEY CAN REVEAL

Technologies in use, roles, projects and business relationships.

C

Executive visibility

Professional profiles, interviews and event appearances.

WHAT THEY CAN REVEAL

Responsibilities, contacts and context useful for impersonating a person of authority.

02

Risk grows when information connects

A name · A project · A partner · An exposed service

→ Company context rebuilt

Taken one by one, they may look like harmless details. Combined, they help an attacker rebuild your company's context.

Being visible online does not mean being vulnerable. Understanding what that visibility reveals helps you assess the risk.

03

From public information to a targeted attack

1 **Collection**

Gathering information on the company, its people and digital assets.

2 **Correlation**

Linking roles, partnerships, events and projects.

3 **Credible message**

Crafting a communication that refers to real people and activities.

4 **Possible compromise**

If the recipient is deceived, the attack can lead to stolen credentials or access to confidential information.

ILLUSTRATIVE EXAMPLE

1. A post announces a new partnership.
2. A public profile identifies the project lead.
3. **A fake email from the partner asks them to open a shared document.**

04

What could be at risk?

01 **Accounts and confidential information**

02 **Processes and business continuity**

03 **Corporate reputation**

05

Look at your company from the outside

01 **Map the assets reachable from the Internet.**

02 **Assess which public information can be correlated.**

03 **Analyse the exposure of senior executives.**

04 **Set your priorities for action.**

If an attacker looked at your company today, what would they see?

Discover more, download the whitepaper!

IN SWITZERLAND TOO, THE RISK IS REAL

NEARLY

65,000

cyber incident reports received by the NCSC in 2025.

19%

of reports concern phishing.

ABOUT

+35%

CEO fraud reports: from 719 in 2024 to 970 in 2025.

AND SWISS SMES?

37%

of SMEs have already been hit by a cyberattack, up from 20% in 2023[1].

42%

of SMEs consider themselves adequately protected in case of attack, down from 55% a year earlier[2].

58%

of reports to the NCSC in the first half of 2025 concern scams[3].

An executive's identity can become a tool for deception.

Source: NCSC (Federal Office for Cybersecurity), 2025 annual figures. Change in CEO fraud reports calculated from published values. Reports do not represent all attacks that occurred in Switzerland.
[1] Deloitte, board of directors study, September 2026 (board members' estimate). [2] «SME Cybersecurity 2025» study, digitalswitzerland, Mobiliar and partners. [3] NCSC, semi-annual report 2025/1.

VARGROUP