VARGROUP

CYBER EXPOSURE

Was sieht ein Angreifer, wenn er Ihr Unternehmen betrachtet?

Exponierte Assets, öffentliche Informationen und die Sichtbarkeit der Führungskräfte: Die Vorbereitung eines Angriffs kann bei dem beginnen, was bereits online ist.

01

Drei Dimensionen im Blick

A

Digitale Assets

Websites, Anwendungen, Cloud-Dienste und Fernzugänge, die über das Internet erreichbar sind.

WAS SIE VERRATEN KÖNNEN

Mögliche Einstiegspunkte und Dienste, die analysiert werden können.

B

Unternehmens informationen

Dokumente, Medienmitteilungen, Stelleninserate und online veröffentlichte Inhalte.

WAS SIE VERRATEN KÖNNEN

Eingesetzte Technologien, Rollen, Projekte und Geschäftsbeziehungen.

C

Sichtbarkeit der Führungskräfte

Berufsprofile, Interviews und Auftritte an Veranstaltungen.

WAS SIE VERRATEN KÖNNEN

Verantwortlichkeiten, Kontakte und Zusammenhänge, mit denen sich eine Autoritätsperson imitieren lässt.

02

Das Risiko wächst, wenn sich Informationen verknüpfen

Ein Name + Ein Projekt + Ein Partner + Ein exponierter Dienst → Unternehmenskontext rekonstruiert

Einzeln betrachtet wirken sie wie harmlose Details. Kombiniert helfen sie einem Angreifer, den Unternehmenskontext zu rekonstruieren.

Online sichtbar zu sein heisst nicht, verwundbar zu sein. Wer versteht, was diese Sichtbarkeit preisgibt, kann das Risiko besser einschätzen.

03

Von einer öffentlichen Information zum gezielten Angriff

1 **Sammeln**
Ermitteln von Informationen über Unternehmen, Personen und digitale Assets.

2 **Verknüpfen**
Verbinden von Rollen, Partnerschaften, Veranstaltungen und Projekten.

3 **Glaubwürdige Nachricht**
Erstellen einer Mitteilung, die auf reale Personen und Aktivitäten verweist.

4 **Mögliche Kompromittierung**
Wird die empfangende Person getäuscht, kann der Angriff zum Diebstahl von Zugangsdaten oder zum Zugriff auf vertrauliche Informationen führen.

ILLUSTRATIVES BEISPIEL

1 Ein Post kündigt eine neue Partnerschaft an.

2 Ein öffentliches Profil nennt die projektverantwortliche Person.

3 **Eine gefälschte E-Mail des Partners fordert dazu auf, ein geteiltes Dokument zu öffnen.**

04

Was kann auf dem Spiel stehen?

01 **Konten und vertrauliche Informationen**

02 **Prozesse und Betriebskontinuität**

03 **Reputation des Unternehmens**

05

Betrachten Sie Ihr Unternehmen von aussen

01 **Erfassen Sie die über das Internet erreichbaren Assets.**

02 **Prüfen Sie, welche öffentlichen Informationen sich verknüpfen lassen.**

03 **Analysieren Sie die Exponierung der Geschäftsleitung.**

04 **Legen Sie Prioritäten für Massnahmen fest.**

Wenn ein Angreifer Ihr Unternehmen heute betrachten würde – was würde er sehen?

Vertiefen Sie das Thema mit unserem Whitepaper – jetzt herunterladen.

AUCH IN DER SCHWEIZ IST DAS RISIKO REAL

FAST

65'000

Meldungen zu Cybervorfällen gingen 2025 beim BACS ein.

19 %

der Meldungen betreffen Phishing.

RUND

+35 %

Meldungen zu CEO-Betrug: von 719 im Jahr 2024 auf 970 im Jahr 2025.

UND DIE SCHWEIZER KMU?

37 %

der KMU wurden bereits Opfer eines Cyberangriffs – 2023 waren es 20 %[1].

42 %

der KMU fühlen sich im Fall eines Angriffs ausreichend geschützt. Ein Jahr zuvor waren es 55 %[2].

58 %

der Meldungen an das BACS im ersten Halbjahr 2025 betreffen Betrug[3].

Die Identität einer Führungskraft kann zum Werkzeug der Täuschung werden.

Quelle: BACS, Bilanz 2025. Veränderung der Meldungen zu CEO-Betrug auf Basis der publizierten Werte berechnet. Die Meldungen bilden nicht alle in der Schweiz erfolgten Angriffe ab.
[1] Deloitte, Verwaltungsratsstudie, September 2026 (Schätzung der VR-Mitglieder). [2] Studie «KMU-Cybersicherheit 2025», digitalswitzerland, Mobiliar und Partner. [3] BACS, Halbjahresbericht 2025/1.

VARGROUP