

06.02.2026

# OSINT und Identitätsdiebstahl – wenn öffentlich verfügbare Daten zur Gefahr werden

**Persönliche Informationen sind heute so leicht zugänglich wie nie zuvor. Was viele nicht wissen: Cyberkriminelle nutzen gezielt Open Source Intelligence (OSINT), um Identitäten zu sammeln, Profile zu erstellen und Betrug vorzubereiten. In Kombination mit Identitätsdiebstahl entsteht so eine ernstzunehmende Bedrohung.**

## Was ist Open Source Intelligence (OSINT)?

OSINT bezeichnet das systematische Sammeln und Auswerten von öffentlich zugänglichen Informationen. Dabei handelt es sich nicht um gehackte Daten, sondern um Inhalte, die frei im Internet verfügbar sind. Oft werden diese von den Betroffenen selbst veröffentlicht. Diese Daten wirken meist harmlos, können aber kombiniert ein detailliertes Personenprofil ergeben.

Typische OSINT-Quellen sind:

- Soziale Netzwerke (Facebook, Instagram, TikTok etc.)
- Öffentliche Register und Verzeichnisse
- Webseiten, Foren und Kommentare
- Bilder, Videos und Metadaten
- Frühere Datenlecks und veröffentlichte Datensätze

## Wie funktioniert OSINT in der Praxis?

Cyberkriminelle nutzen OSINT gezielt und gehen dabei strukturiert vor. Ausgangspunkt ist die gezielte Sammlung frei zugänglicher Informationen wie Name, E-Mail-Adresse, Telefonnummer oder Benutzername. Anschliessend werden diese Daten miteinander verknüpft, indem Inhalte aus sozialen Medien ausgewertet werden, etwa Beiträge, Fotos oder Kommentare. Auch Informationen über Arbeitgeber, Hobbys oder häufige Aufenthaltsorte fliessen in diese Analyse ein. Aus der Vielzahl scheinbar harmloser Details entsteht so Schritt für Schritt ein umfassendes Profil einer Person, das Rückschlüsse auf Gewohnheiten, soziale Kontakte und Vertrauensbeziehungen zulässt. Auf dieser Grundlage bereiten die Täter gezielte Angriffe vor, etwa besonders glaubwürdige Betrugsversuche oder Identitätsdiebstahl. Der gesamte Prozess basiert auf legal zugänglichen Informationen, wird jedoch für illegale Zwecke missbraucht.

## So reduzieren Sie das OSINT-Risiko

Ein vollständiger Schutz vor OSINT-basierten Angriffen ist kaum möglich, doch das Risiko lässt sich deutlich reduzieren. Wichtig ist, die Privatsphäre-Einstellungen in sozialen Netzwerken regelmässig zu überprüfen und persönliche Informationen bewusst sowie sparsam zu teilen. Auch ältere Profile, Beiträge und Fotos sollten in regelmässigen Abständen kontrolliert und gegebenenfalls entfernt werden. Zusätzlich empfiehlt es sich, E-Mail-Adressen und Benutzernamen nicht plattformübergreifend identisch zu verwenden. Besondere Vorsicht ist bei An-

fragen oder Nachrichten geboten, die auffällig viele persönliche Details enthalten. Grundsätzlich gilt: Je weniger Daten öffentlich zugänglich sind, desto schwieriger wird deren Missbrauch.

## **Fazit**

OSINT zeigt, wie mächtig öffentlich zugängliche Informationen sein können, im Guten wie im Schlechten. In den falschen Händen werden sie zur Grundlage für Identitätsdiebstahl und gezielte Betrugsangriffe. Wer sich bewusst ist, welche Spuren er online hinterlässt, stärkt seine digitale Sicherheit nachhaltig.