

OSINT

Wie Sie Informationen finden, verifizieren und
verknüpfen

» Hier geht's
direkt
zum Buch

DAS VORWORT

Kapitel 1

Einführung

Willkommen in der Welt der Open Source Intelligence. In diesem Kapitel machen Sie sich mit dem Themengebiet vertraut und verschaffen sich einen Überblick über die Inhalte des Buches. Anschließend erfahren Sie mehr über die Aus- und Fortbildung im Bereich OSINT sowie über mich als Autor.

Vielleicht wissen Sie noch gar nicht, was Open Source Intelligence, kurz *OSINT*, eigentlich ist. Vielleicht haben Sie spontan dieses Buch gekauft, weil schon der Titel eine ungeheure Faszination auf Sie ausgeübt hat. Selten hatte ich mit einem Begriff zu tun, der so oft missverstanden und fehlinterpretiert wird. Vielleicht hängt es auch ein wenig damit zusammen, dass es kein passendes deutsches Pendant zu »OSINT« gibt. Ich werde den Begriff daher nicht übersetzen, ihn aber hoffentlich gut genug erklären.

1.1 Was ist Open Source Intelligence?

Fangen wir also vorne an: Was ist *Open Source Intelligence*? Es handelt sich um die Informationsgewinnung aus *öffentlich zugänglichen Quellen* mit dem Ziel, daraus *Intelligence* zu gewinnen.

Das grundlegende Merkmal von OSINT, nämlich die Nutzung öffentlich zugänglicher Quellen (*open sources*), steht im krassen Gegensatz zu anderen (nachrichtendienstlichen) Disziplinen der Informationsbeschaffung, die grundsätzlich im Verborgenen erfolgen. Hier spricht man von *closed sources*.

Open Source

Open Source Intelligence hat nichts mit Open Source Software zu tun. Dieser Begriff bezieht sich darauf, dass der Programmcode (Quellcode) offengelegt und geteilt wird.

OSINT bedient sich also Quellen, die öffentlich zugänglich sind. Um die öffentliche Zugänglichkeit zu definieren, bedienen sich Juristinnen und Juristen des Begriffs *Jedermann*. Ohne zu tief in die Rechtswissenschaften einzusteigen: Bei *Jedermann* handelt es sich um eine beliebige Person *ohne besondere Eigenschaften*, die Ihnen vielleicht aus Gesetzen wie dem Jedermannsrecht nach § 127 der Strafprozessordnung

bekannt ist. Dieser Paragraph berechtigt alle Bürgerinnen und Bürger zur Festnahme einer straffälligen Person. Das Gegenteil des Jedermann ist eine Person mit besonderen Eigenschaften, z. B. ein Amtsträger.

Nehmen wir z. B. einen Polizisten. Dieser ist Amtsträger, weshalb er besondere Befugnisse und auch Zugänge hat, wie beispielsweise Zugriff auf polizeiliche Informationssysteme. Auf solche *closed sources* kann unser Jedermann nicht zugreifen.

Es lassen sich aber auch Informationen aus anderen Quellen gewinnen, z. B. aus diesem Buch. Um dieses Buch zu erwerben und von den darin enthaltenen Informationen zu profitieren, müssen Sie weder Amtsträger sein noch über andere besondere Eigenschaften verfügen – außer natürlich, dass Sie sich für das Thema interessieren.

Offen ist nicht gleich kostenlos

Das Buch-Beispiel zeigt außerdem, dass *öffentlich zugänglich* nicht mit *kostenlos* verwechselt werden darf. Sicherlich stehen heutzutage mehr Informationen kostenlos zur Verfügung als je zuvor, aber auch hier gilt das Motto: »*You get what you pay for!*« Oder anders gesagt: »*Qualität hat ihren Preis.*«

Das soll keinesfalls bedeuten, dass Sie zwangsläufig für gute Informationen und Zugänge zahlen müssen, oder dass der teuerste Anbieter eines Tools immer der beste ist. Sie werden in diesem Buch viele Beispiele kennenlernen, die Sie außer einer Internetverbindung keinen Cent kosten werden. Tatsächlich werde ich, soweit möglich, auf die Vorstellung kommerzieller Tools verzichten. Sollten diese jedoch eine kostenlose Demo oder ein Freemium-Modell anbieten und somit einen Mehrwert für die Recherche bieten, werde ich sie hier präsentieren.

Grundsätzlich beschränkt sich eine OSINT-Recherche fast nie nur auf ein einzelnes Medium oder nur eine Quelle. Informationen können aus Printmedien beschafft werden, aus dem Rundfunk, aus Kartendiensten oder auch aus dem Internet. All dies sind Quellen, aus denen **Daten** gewonnen werden können. (Wie Sie von Daten über Informationen zu Intelligence kommen, beschreibe ich in Abschnitt 5.4 noch etwas detaillierter.) An dieser Stelle ist für Sie vor allem wichtig: Nur weil etwas aus einer öffentlich zugänglichen Quelle stammt, handelt es sich nicht automatisch um **Open Source Intelligence**.

Stellen Sie sich öffentlich zugängliche Daten wie einzelne, lose Buchseiten vor. Diese Seiten kann jeder lesen und sammeln. Doch erst durch Kontextualisierung, Filterung und Analyse können Sie feststellen, ob Seiten zusammengehören oder ob sie vielleicht aus einem ganz anderen Buch stammen. Mitunter wurden Seiten verändert, etwa durch Beschädigungen oder durch absichtliche Manipulation. Nur durch die Analyse können Sie sich einen Überblick verschaffen, Lücken erkennen und ansprechen.

Denn Open Source Intelligence ist eine (nachrichtendienstliche) Disziplin, die durch das Sammeln, Auswerten und Analysieren öffentlich zugänglicher Informationen Intelligence gewinnt, um einen konkreten Informationsbedarf zu stillen.

Was heißt nun *Intelligence*? Anders als bei den »offenen Quellen«, die sich noch einigermaßen übersetzen lassen, stehen wir vor dem Problem, dass es keine wirklich treffende Übersetzung in die deutsche Sprache gibt. Es handelt sich in diesem Kontext jedenfalls nicht um »Intelligenz«. Deutlich näher dran wäre »Erkenntnisse«, aber perfekt passt auch diese Übersetzung nicht.

Nähern wir uns dem Begriff auf einem anderen Weg: Wie erhält man Intelligence?

Intelligence ist das Ergebnis mehrerer Analyseschritte:

- ▶ *Daten* werden gesammelt und ausgewertet. Daraus entstehen *Informationen*.
- ▶ *Informationen* werden kontextualisiert und interpretiert. Daraus entsteht *Intelligence*.

Lassen Sie mich dies an einem (historischen) Beispiel aus der Geheimdienstarbeit erklären: Stellen Sie sich vor, dass durch Luftaufnahmen gezeigt wurde, dass eine andere Nation ein Raketensystem installiert. Diese Bilder sind zweifelslos relevante Datenpunkte. Man muss aber einiges Fachwissen mitbringen, um solche Aufnahmen zu verstehen; diese Daten müssen also ausgewertet werden.

So erhält man zunächst nur die Information, dass Raketen aufgestellt werden. Es ist noch unklar, ob es sich um defensive Luftabwehrraketen oder offensive Angriffswaffen handelt – oder sind es vielleicht sogar Attrappen? Bereitet die Nation einen Krieg vor oder fühlt sie sich von ihren Nachbarn bedroht? Dienen die Raketen der Abschreckung oder sollen sie gar von anderen Zielen ablenken? All das bedeutet weitere Analysen, Kontextualisierung und Interpretationen, die aus dieser Information *Intelligence* machen.

Was ist Open Source Intelligence?

Was ist also Open Source Intelligence? Es ist die Nutzung von offenen Quellen, um Daten zu sammeln, Informationen zu gewinnen und daraus Erkenntnisse und Schlüsse zu ziehen.

Warum ist Open Source Intelligence überhaupt von Relevanz? Tatsächlich bietet OSINT viele Vorteile gegenüber klassischen Disziplinen der Informationsbeschaffung wie *Human Intelligence* oder *Signals Intelligence*. Das sind die klassischen Gegenstücke zur OSINT: menschliche Spione und das Abhören von Signalen, also beispielsweise von Telefonleitungen oder Satellitenverbindungen.

Nicht nur stehen diese Quellen nicht jedermann zur Verfügung, sondern sie sind auch ungleich teurer und aufwendiger. Oftmals lassen sich Informationen aus öffent-

lichen Quellen deutlich schneller und kostengünstiger beschaffen als auf anderen Wegen. Die Aufklärung einer Postanschrift mithilfe von Satellitenbildern oder Tools wie Google Street View kann binnen weniger Minuten erfolgen, und das sogar weltweit, wenn aktuelles und ausreichend hochwertiges Rohmaterial verfügbar ist. Die Kosten und der Zeitaufwand für eine echte Vor-Ort-Aufklärung durch eigenes Personal sind um ein Vielfaches höher. Dafür hätten Sie aktuelles und belastbares Material, wodurch die Notwendigkeit der Verifikation in den Hintergrund rückt. Diese spielt bei OSINT nämlich eine wichtige Rolle und wird in Abschnitt 9.1 näher beleuchtet.

Ein weiterer Vorteil von OSINT liegt in dem deutlich geringeren Risiko. Zugegebenermaßen ist dies nicht in allen Anwendungsgebieten von OSINT von hoher Relevanz. Aber ist es nicht wesentlich riskanter, sich an einen bestimmten Ort zu begeben und dort eine brisante Information zu übermitteln, als aus sicherer Entfernung eine Information zu übermitteln, die für jedermann zugänglich ist – d. h. eine Information, die keine Gefahr darstellt? Die so gewonnenen Informationen müssen trotzdem brauchbar sein, um daraus zumindest ähnliche Schlüsse ziehen zu können. Beispiel gefällig? Dann werfen Sie einen Blick in Abschnitt 5.1.

Ich möchte aber auch ehrlich sein: OSINT hat nicht nur Vorteile. Dass Informationen aus öffentlichen Quellen verifiziert werden müssen, habe ich bereits angedeutet. Darüber hinaus gibt es mit Daten aus öffentlichen Quellen häufig die gleiche Problematik wie mit Big Data: *Velocity*, *Volume*, *Value*, *Variety* und *Veracity*.

Diese Problematik entsteht, weil Daten aus öffentlichen Online-Quellen oft in riesigen Mengen (*Volume*) und mit unglaublich hoher Geschwindigkeit (*Velocity*) anfallen. Sie sind zudem sehr unterschiedlich in ihrer Art (*Variety*) und ihrem Wert (*Value*), und auch ihre Zuverlässigkeit (*Veracity*) ist nicht immer eindeutig. Das macht es schwierig, relevante und verlässliche Informationen herauszufiltern, sie schnell genug zu verarbeiten und richtig zu bewerten. Dadurch wird die Analyse dieser Daten zu einer besonderen Herausforderung.

Zu guter Letzt: Nicht jede Frage lässt sich mittels OSINT beantworten, jedenfalls nicht verlässlich. Sie können wirklich viele Informationen in öffentlichen Quellen finden, aber nicht alle.

1.2 Was Sie in diesem Buch lernen werden

Glückwunsch! Wenn Sie an diesem Punkt angelangt sind, haben Sie höchstwahrscheinlich schon eine solide Vorstellung davon, was OSINT ist. Was erwartet Sie nun in diesem Buch?

Die Inhalte sind zweigeteilt. Der erste Teil bildet das Fundament für Ihre Recherchen. Hier lernen Sie die Anwendungsgebiete von OSINT anhand von anschaulichen Beispielen kennen. Sie erfahren, welche Fähigkeiten Sie zum Recherchieren benötigen

und wie Sie Ihre Arbeitsumgebung einrichten, um effizient und sicher zu ermitteln. Danach werfen Sie einen kurzen Blick auf die Historie von Open Source Intelligence, erwerben die theoretischen Grundlagen der Informationsgewinnung und lernen den *Intelligence Cycle* kennen.

Ebendieser bildet die Struktur für den zweiten Teil. Entlang des Intelligence Cycle lernen Sie, wie Sie Ihre Recherche planen und dokumentieren, wie Sie zu unterschiedlichen Entitäten Informationen sammeln, diese verarbeiten, verifizieren und analysieren. Sie erfahren, wie Sie (Bild-)Dateien analysieren, woran Sie Manipulationen erkennen und was einen forensischen Bericht ausmacht. Dabei lernen Sie verschiedene Arten von Intelligence-Produkten kennen.

Das Buch schließt mit einem Ausblick auf die Trends, Chancen und Risiken von Open Source Intelligence.

1.3 Aus- und Fortbildung

Open Source Intelligence entwickelt sich stetig weiter. Wenn Sie in diesem Bereich erfolgreich sein möchten, benötigen Sie Durchhaltevermögen und Wissensdurst, denn Sie werden niemals auslernen. Das liegt einerseits an der Dynamik des Internets und andererseits an der Vielfalt der Anwendungsmöglichkeiten.

Wenn Sie den Werdegang verschiedener OSINT-Experten betrachten, werden Sie feststellen, dass die Lebensläufe unterschiedlicher kaum sein könnten. Das liegt einerseits daran, dass OSINT nach wie vor eine junge Disziplin ist (auch wenn ich Ihnen in Abschnitt 5.1 zeigen werde, dass OSINT schon länger angewendet wird, als man vielleicht annehmen würde). Andererseits ist OSINT eine unglaublich breite Disziplin, in der Technikbegeisterte genauso ihren Platz finden wie weniger technikaffine Menschen.

Mit OSINT ist es wie mit Rom: Viele Wege führen zum Ziel. Mit diesem Buch halten Sie den Reiseführer in Ihren Händen, den ich mir zu Beginn meiner eigenen Reise in die Tiefen von OSINT gewünscht hätte. Das Buch enthält mein gesamtes Wissen über Open Source Intelligence und alles, was Sie für Ihre Recherchen benötigen.

Natürlich können Sie auch ohne dieses Buch OSINT lernen. Und umgekehrt werden Sie durch die Lektüre allein nicht zum Profi. Ähnlich wie beim Erlernen eines Instruments oder einer Sprache müssen Sie Zeit investieren und Erlerntes regelmäßig anwenden. Probieren Sie die vorgestellten Techniken aus. Seien Sie mutig.

Andere Lernmethoden

Sie können das Buch als Fachbuch nutzen und im Selbststudium in das Thema eintauchen. Alternativ finden Sie Schulungen zu Open Source Intelligence von mir in verschiedenen Formaten unter <https://osintgeek.de>.

Falls Sie es nicht schon festgestellt haben, werden Sie in Kürze bemerken, dass Open Source Intelligence ein sehr dynamisches Thema ist, bei dem sich die Feinheiten bestimmter Techniken rasant ändern. Deshalb ist es wichtig, das eigene Wissen nach dem Erlernen der Grundlagen stets auf dem Laufenden zu halten. Theoretisch könnten Sie alle paar Jahre einen Einstiegskurs besuchen, doch davon möchte ich abraten. Mein Tipp: Besuchen Sie stattdessen vertiefende Workshops zu ausgesuchten Teilbereichen. Und: Nutzen Sie OSINT im Alltag. Ein guter Freund von mir sagt dazu: »Use OSINT to do OSINT.«

Es gibt eine Vielzahl von Möglichkeiten, die eigenen OSINT-Skills zu schärfen. Neben spielerischen Challenges wie *Quiztime* oder *GeoGuessr* können Sie Ermittlungen unterstützen, indem Sie Ihr Wissen im Rahmen der Öffentlichkeitsfahndung anwenden oder an dem von Europol initiierten Projekt *Trace an Object* teilnehmen (siehe Kapitel 12). Bei Letzterem werden Fragmente aus Missbrauchsdarstellungen von Kindern veröffentlicht, um so Hinweise auf den Ursprung sowie die Identität der Opfer bzw. Täter zu erlangen.

1.4 Über den Autor

Da Sie sich für das Thema Open Source Intelligence begeistern, kennen Sie mich unter Umständen schon. Falls nicht, möchte ich mich kurz vorstellen: Mein Name ist Samuel Lolagar. Als studierter Kriminalbeamter habe ich viele Erfahrungen mit Ermittlungen im Internet gemacht, ihre Möglichkeiten und Chancen, aber auch ihre Grenzen kennengelernt. Dabei ging es mir wie vielen anderen auch: Ich habe OSINT betrieben, ohne zu wissen, dass es diese Disziplin gibt.

Mein Interesse für Technik und das Internet reicht bis in meine Jugend zurück. Damals machte ich meine ersten Gehversuche, programmierte einfache Webseiten, betreute das eine oder andere Content-Management-System und betrieb sogar einen kleinen Blog. In dieser Zeit habe ich mich auch mit Bildbearbeitung auseinandergesetzt. Sie werden im Verlauf des Buches an einigen Stellen merken, dass dies durchaus eine wertvolle Fähigkeit sein kann.

Durch dieses grundlegende Verständnis für das Internet war es mir beispielsweise möglich, verschiedene Webseiten miteinander in Verbindung zu bringen und so Ermittlungskomplexe zu bilden. In manchen Fällen half mir eine simple Bilderrück-

wärtssuche, um beispielsweise festzustellen, ob beim Love Scamming fremde Bilder (z. B. die eines US-Generals) missbraucht wurden. In anderen Fällen half die Suche nach Textpassagen in Anführungszeichen, um zusätzliche Social-Media-Profile einer Person zu ermitteln. Und in wieder anderen Verfahren konnte ich die Aktivitäten einzelner Krimineller über mehrere Foren im Darkweb verfolgen und durch Analysen der Kommunikation wertvolle Hinweise und Beweise für konkrete Straftaten sammeln.

Gerne blicke ich auf meine Zeit als Ermittler bei der Polizei zurück, da ich dort viele Techniken erlernt und erprobt habe, die ich Ihnen in diesem Buch vermitteln möchte. Ich halte mich aber keinesfalls für allwissend und wehre mich gegen die Bezeichnung »Experte«, wenn auch zugegebenermaßen nicht mehr so vehement wie noch vor einigen Jahren. Ich bin überzeugt, dass es im Themenfeld OSINT keine allwissenden Experten geben kann. Dafür ist das Thema schlichtweg zu groß und zu vielfältig. Dennoch werde ich mich bemühen, Ihnen einen fundierten und umfassenden Überblick über die verschiedenen Anwendungsbereiche, aber vor allem auch über Strategien und Techniken für Ihre Recherchen zu geben.