

# DARK MATTERS

## Das unsichtbare Verbrechen

Wie sich Gangster und Spione verbünden  
und unsere Gesellschaft unterwandern.

Ein True-Crime-Podcast  
von Matthias Woestmann

Folge 2:  
„How to rob 100 million“

Musik

DARK MATTERS - Das unsichtbare Verbrechen

Musik

Wie Gangster und Spione sich verbünden und unsere Gesellschaft unterwandern.

Ein True-Crime-Podcast von Matthias Woestmann

Musik

„How to rob a hundred million - and get away with it“ - das ist der Traum der Unterwelt und unser Lernziel in der ersten Staffel.

Ein Grundkurs in fünf Lektionen für angehende Mafiosi. Keine unrealistischen Thriller-Szenarien, sondern ein bodenständiger Plan, nachvollziehbar - und machbar. Na gut, für jeden, der etwas Eigenkapital mitbringt. Das ist die einzige Voraussetzung, die nicht jedem zur Verfügung steht. Ansonsten braucht man nur Liebe zum Detail, zur Präzision. Ein Buchhalter wäre der ideale Täter. Und nicht etwa: James Bond.

In fünf Lektionen vom Rookie zum Profi - zumindest im Fach „Theorie“. Wichtigstes Ausbildungsziel: überhaupt erstmal zu verstehen, dass spurlose Verbrechen tatsächlich möglich sind.

Diese Erkenntnis wird euch verändern. Sie eröffnet einen Ozean voller Möglichkeiten.

**Musik**

Da ich als Journalist nicht die richtigen Credentials mitbringe, schlüpfte ich für diesen Kurs in eine andere Rolle: in die eines ehemaligen Agenten der Stasi, der eine zweite Karriere in der

Unterwelt gemacht hat und auf seine alten Tage beschlossen hat, ein wenig von seinem Wissen weiterzugeben.

Bevor ich loslege vorweg noch ein wenig Erwartungsmanagement: ihr lernt bei mir nicht Autos knacken oder Koks verticken. Unser Ziel ist es, keine Spuren zu hinterlassen. Und damit scheiden die vulgären Formen des Verbrechens schon mal aus: Drogen- und Menschenhandel, Raub, Einbruch, Zuhälterei. Das sind schmutzige Verbrechen, und sie führen oft zu Folgedelikten, bei denen Sachen und Menschen beschädigt werden. Schaden entsteht durch Kontakt, Kontakte produzieren Spuren, und Spuren führen zum Täter. So ähnlich formulierte das schon Edmond Locard, der Gründer der Forensik, vor über 100 Jahren. Und seine Regel gilt bis heute.

Und es gibt noch einen Grund, warum ich Kontaktsport nicht besonders schätze: der Fahndungsdruck. Wenn irgendwo Blut fließt, wird der Staatsanwalt nervös. Weil auch die Öffentlichkeit nervös wird. Und so werden in Deutschland 93% aller Morde aufgeklärt<sup>1</sup>. Gewalt ist also keine Option.

Und wir brauchen Gewalt auch gar nicht. Es gibt genug Möglichkeiten des Eigentumstransfers, bei denen KnowHow, Technologie und menschliche Schwächen die entscheidende Rolle spielen - im weiten Feld der Finanzmärkte zum Beispiel oder der Kryptowährungen. Ich will nicht angeben, da aber allein in diesem Bereich holt unsere Branche rund eine Billion Dollar raus - jedes Jahr. Bestätigt übrigens auch von Europol und FBI. In diesem Teich wollen wir also fischen. Unser Ziel: 100 Millionen, elegant und risikolos wie bei Arsen Lupin. Etwas altmodisch - ich weiß - aber auch der wurde nie erwischt, verzichtete auf Gewalt und ließ jeden Verdacht an sich abperlen wie Wasser auf einer Teflonpfanne.

Jingle

Lektion eins: Die Wahl des Opfers

Jingle

Das Opfer muss mit großer Sorgfalt ausgewählt werden. Natürlich muss es ein gewisses finanzielles „Mindestgewicht“ auf die Waage bringen - „Tax the Rich.“

Freundlicherweise hilft uns die UBS mit ihrem jährlichen „Global Wealth Report“, und Forbes mit seiner berühmten „Forbes List“ - dem Who is Who der Reichen und Superreichen.

Die großen Vermögensverwalter - UBS, Julius Bär, Rothschild und Pictet - haben für diese Kundengruppe ein Ranking geschaffen: da gibt es die

- High Networth Individuals (HNWIs), die einfachen Millionäre bis 30 Millionen Dollar;
- die Ultra High Networth Individuals (UNHWIs) ab 30 Millionen;
- und dann schließlich die wirklich Reichen ab einer Milliarde liquidem Vermögen.

Es ist eine Klassengesellschaft und wenn jemand glaubt, er kann mit 10 oder 20 Millionen ganz oben mitspielen - falsch gedacht: das sind die Stehplätze.

Wir werden uns natürlich auf die Logenplätze konzentrieren.

Denn: zwischen dem Vermögen der Zielperson und dem potentiellen Vermögensschaden muß eine vernünftige Korrelation bestehen. Wir können von jemandem, der 100 Millionen besitzt, nicht 100 Millionen fordern. Dann stünde er mit dem Rücken zur Wand und sein Widerstand würde unkalkulierbar.

Nein, es muß für das Opfer „leicht“ sein, oder - um es etwas präziser zu formulieren: in der Güterabwägung zwischen einem Übel, das wir ihm später androhen, und dem finanziellen Preis, mit dem er sich davon freikaufen kann, muß die Entscheidung eindeutig ausfallen - und zwar so eindeutig, dass sie ohne großes Zögern getroffen wird. Um diese Eindeutigkeit herzustellen, setzen wir 5% bis 10% vom Nettovermögen unseres Opfers als Obergrenze.

Das schränkt unseren Kundenkreis ein.

Wir sind damit schnell im Bereich der Milliardenvermögen. 2024 gab es 2780 Milliardäre weltweit, 1000 in Asien, 900 in den USA und knapp 700 in Europa. In dieser Zielgruppe suchen wir nun den Richtigen. Jemanden, der ein dunkles Geheimnis hat. Eines, das er nicht teilen möchte - weder mit seiner Familie noch mit den Ermittlungsbehörden. Ein Geheimnis, das ihm 100 Millionen wert ist.

Wir suchen also nicht nach einem Mann, der falsch geparkt oder ein geschütztes Nashorn erlegt hat. Sein Geheimnis muß von monströser Peinlichkeit sein und am besten auch strafrechtlich relevant. So etwas finden wir am ehesten im weiten Feld des sexuellen Übergriffs,

des Missbrauchs und der Kinderpornographie. Ja, ich weiß: das klingt unschön. Und tatsächlich gibt es ein breites Spektrum von Alternativen: vom Seitensprung, über Steuerhinterziehung, bis zu Drogenbesitz und Compliance-Verstößen. Aber nichts ist so wirksam wie der Vorwurf des Missbrauchs. Am besten gegenüber Kindern oder Jugendlichen.

Veröffentlicht bedeutet das den sozialen Tod; weder Geld, Berühmtheit oder Macht können davor schützen. Allein der Verdacht entfaltet eine vernichtende Wirkung - auch ohne jedes Gerichtsurteil. Das zeigt der Fall Kevin Spacey in wunderbarer Deutlichkeit. Spacey war ein gefeierter Theater- und Filmschauspieler, der auf dem Höhepunkt seiner Karriere die Rolle des skrupellosen US-Politikers Francis Underwood in der Netflix-Serie „House of Cards“ spielte. Bis im Herbst 2017 der Hollywood-Schauspieler Anthony Rapp in einem Interview behauptete, Spacey habe ihn 1986, als 14jährigen, sexuell belästigt. Über Spacey brach eine Welle der Empörung herein, er wurde aus der Produktion gekickt und mußte als Schadensersatz Millionen an Netflix zahlen. Innerhalb weniger Monate war seine Existenz völlig zerstört. Vor Gericht aber endeten alle Verfahren mit Freispruch. Solche Fälle sind für uns Gold wert, sie zeigen dem Opfer, was passiert, wenn es nicht kooperiert. Insofern sind wir der Me-Too-Bewegung zu großem Dank verpflichtet.

## **Musik**

Natürlich ist Erpressung älter als Me-Too. Ich habe schon in den 80er Jahren erste Erfahrungen damit gemacht. Damals im Schulungszentrum der Hauptverwaltung Aufklärung - kurz HVA - in Beetz. Für die Geheimdienst-Laien: die HVA war der Auslandsgeheimdienst der DDR. In Beetz, in der Abgeschiedenheit der Mark Brandenburg, brachte man uns die sogenannten Operativen Fähigkeiten bei. Für unsere Ausbilder hieß das Zauberwort: „Kompromat“, die Wunderwaffe im Kampf gegen Klassenfeind. Ganze Abteilungen haben sich damit beschäftigt, belastendes Material zu sammeln - draußen im Feld oder über abgehörte Autotelefone. Im Prinzip hatten wir damit einen großen Teil der westdeutschen Elite in der Hand. Deshalb ist auch fast keiner unserer Chefs nach der Wende eingefahren - die hätten ja was ausplaudern können. Aber davon später.

Konzentrieren wir uns erstmal auf das Opfer.

Suchkriterium eins kennen wir schon: es muß sich schuldig gemacht haben - oder: erpressbar sein.

Kriterium zwei: es taucht in den Reichen-Listen von Forbes auf.

Kriterium drei: es lebt in Europa - das entscheiden wir so, weil es die Logistik später einfacher machen wird.

Drei Datenpunkte - und das reicht für die digitale Fahndung.

Und jetzt stehen wir vor einer Zäsur: Kontaktaufnahme mit der Unterwelt. In unserem Fall: mit Hackern, die ihre Dienste anbieten - „Crime as a Service“.

Dieses Prinzip hat sich der Untergrund von den Konzernen abgeschaut: nicht mehr alles selber machen, sondern Teilaufgaben auslagern - an Spezialisten, die ihren Job präzise und günstig erledigen.

So muß man nicht mehr alle Fähigkeiten selber vorhalten und kann sich auf die Kernkompetenzen konzentrieren.

Klassische Betriebswirtschaftslehre.

In der Schattenwirtschaft betrifft das vor allem Hacking, Datenbeschaffung und Ransomware-Attacken. In Belarus, Russland und Israel hat sich eine ganze Industrie entwickelt, die diese Dienste anbietet. Sie ist für westliche Strafverfolgungsbehörden nahezu unerreichbar - auch deshalb, weil sie nicht nur kriminellen, sondern auch politischen Interessen dient.

Mit diesen Fachleuten wollen wir also Kontakt aufnehmen. „Kontakt“ - das haben wir gelernt - hinterläßt immer Spuren, und die müssen wir soweit wie möglich reduzieren. Was ich jetzt beschreibe, ist vielleicht etwas paranoid, aber der nächste Schritt ist der einzige in der gesamten Operation, der bei dem wir den Boden des Gesetzes verlassen:

nach **§202 StGB** ist die Anstiftung zu einem Hack strafbar. Man muss ihn nicht einmal selber durchführen.

Deshalb also: Quarantäne-Regeln beachten:

Erstens:

ein Notebook kaufen, das noch nie online war, bar bezahlt im Elektronikladen;

Zweitens:

Café oder Hotellobby aufsuchen, aber **ohne** Handy. Wir wollen ausschließen, dass die IP-Daten des WLAN mit den Funkzellendaten unseres Handys verknüpft werden können.

Drittens:

Mit dem neuen Notebook über Tor ins Darknet gehen und dort gezielt mit Begriffen wie Hacking oder Leaks nach einem Anbieter suchen.

Es wäre an dieser Stelle kontraproduktiv einen bestimmten Anbieter zu empfehlen.

Aber ein paar Beispiele für die renommiertesten Player im Markt kann ich schon nennen. Da ist die russische Black Basta Gruppe, den Namen finde ich übrigens großartig. Sie ist spezialisiert auf Ransom - d.h. sie dringen in IT-Systeme ein, verschlüsseln die Daten und fordern Lösegeld.

Das haben sie schon bei 700 Unternehmen erfolgreich durchgezogen, darunter Schwergewichten wie Rheinmetall, die als Rüstungskonzern eigentlich besonders geschützt sein müssten.

Der Chef von Black Basta nennt sich „Tramp“ und ist ein wahrer Virtuose im Knacken von Netzwerkrechnern.

Er bietet Ransomware-as-a-Service und verkauft seinen Schadcode an andere Hacker. Bezahlen lässt er sich mit einem Anteil der Beute. Das ist das Provisionsmodell, es setzt ein gewisses Vertrauensverhältnis voraus und ist vielleicht nicht der ideale Einstieg in die Geschäftsbeziehung.

Tramp heißt übrigens mit bürgerlichem Namen Oleg Nefedov und lebt in der Provinzstadt Joschkar-Ola, 1000 Kilometer hinter Moskau. Er genießt die Protektion der Kollegen vom GRU - dem russischen Militärgeheimdienst - und konnte deshalb schon mal bei einem Haftprüfungstermin in Armenien entkommen.

Das war unser Beispiel aus Rußland.

Israel ist ebenfalls eine gute Adresse.

Hier geben allerdings nicht Hacker im Hoodie den Ton an, sondern seriöse Hightech-Unternehmen - oft gegründet von ehemaligen Angehörigen der Armee und des Geheimdienstes.

Das bekannteste unter ihnen ist die NSO-Group.

Mit ihrer Spyware „Pegasus“ hat das Unternehmen zehntausende iPhones geknackt und ihre Besitzer ausspioniert. Ursprünglich entwickelt als Tool gegen den Terrorismus wurde es von Diktatoren gegen unbequeme Journalisten und NGOs eingesetzt - und flog dadurch auch auf.

Immer auf der Suche nach dem schnellen Geld ist die Hacker-Szene in Nordkorea.

Meistens arbeiten die koreanischen Coder für den eigenen Staat, der wegen Embargo und Atomprogramm chronisch klamm ist, aber gegen harten Devisen nehmen sie externe Aufträge gerne an.

Weltweit unübertroffen ist die Lazarus Group.

Sie brachten die Zentralbank von Bangladesch 2016 dazu, ihnen 81 Millionen Dollar zu überweisen;

2023 knackten sie das Online-Casino Stake.com

und im Januar 2025 die Kryptobörse Bybit - Beute 1,5 Milliarden Dollar.

Keine andere Gruppe hackt so systematisch, kontinuierlich und profitabel wie die Lazarus Gang. Der Name spricht für den trockenen koreanischen Humor: Lazarus war ein enger Freund des Erlösers Jesus, und wurde von ihm aus alter Verbundenheit von den Toten auferweckt.

## **Musik**

Stellen wir fest:

es gibt ein ausgeprägtes Ökosystem von Dienstleistern, die den entscheidenden Job für uns machen können.

Wir suchen uns zwei davon aus und teilen unsere digitale Fahndung in zwei Abschnitte:

Dienstleister 1 beschafft uns die IP-Adressen, Handy-Nummern und Identifikationsnummern der Handys, die sogenannte IMEIs - von allen Personen auf unserer Forbes-Liste.

Den Datensatz reichen wir dann - selbstverständlich anonymisiert - weiter an Dienstleister zwei.

Sein Auftrag: ein systematischer Abgleich unseres Datensatzes mit den Nutzerdaten von Plattformen, die Kinderpornographie anbieten. Ein Job, den eigentlich das FBI machen müßte.

Versteht sich, dass die Bezahlung bar erfolgt - und die Datenübergabe per Stick.

Was ich bis hierhin beschrieben habe, ist eine induktive Methode: wir definieren die Tat und suchen den Täter. Wir ziehen das Schleppnetz unserer Suchkriterien durch den digitalen Ozean wie der Trawler einer Fangflotte und suchen unter Tonnen von Beifang den goldenen Seestern.

Es ist der Datenpunkt, an dem Tat und Täter zusammenkommen und unser wertvollstes Werkzeug entsteht: das Kompromat.

Mancher von euch mag daran zweifeln, dass wir mit dieser Methode tatsächlich fündig werden.

Ich kann euch versichern: die Wahrscheinlichkeit ist hoch.

Ehrlicherweise muß ich aber gestehen, dass wir in unserer Startphase ganz anders gearbeitet haben.

Als wir anfangen, in den Jahren nach der Wende, gab es die heutigen technischen Möglichkeiten logischerweise noch nicht.

Wir hatten stattdessen Mikrofilme aus der Abteilung 12 der HVA, jener Abteilung, die sich auf die kleinen schmutzigen Geheimnisse der westdeutschen Elite spezialisiert hatte.

Das war ein gutes Startkapital.

Weil jedes Kompromat ein Verfallsdatum hat, haben wir systematisch Verdachtsfälle gesammelt, oft aus öffentlich zugänglichen Quellen, und eine Datenbank angelegt: Steuerhinterziehung, Korruption, Bordellbesuche, unorthodoxe Vorlieben.

Bei Bedarf haben wir dann gezielt recherchiert, um einen Verdacht zu erhärten und belastbares Material zu sammeln. Es war das gleiche System wie der HVA: erstmal alles sammeln, was man bekommen kann.

Auswerten.

Verbindungen herstellen - und bei Bedarf als Kompromat einsetzen.

Die digitale Revolution in den Nullerjahren hat unsere Arbeit kolossal erleichtert. Die Leute schleppen in ihrem Handy alles mit sich herum: ihre ganze Kommunikation, ihre Erinnerungen und ihre Geheimnisse. Das haben wir immer als Einladung verstanden.

In den vergangenen 30 Jahren ist aus unserer alten Mikrofilm-Datei auf diese Weise eine wirklich große Datenbank entstanden: eine Sammlung der Schwächen und Geheimnisse vieler Tausend Menschen - mit Schwerpunkt auf Europa.

Es sind nicht nur die Reichen.

Viel wichtiger ist die sogenannte Funktionselite: Leute, die an den Schalthebeln der Macht sitzen, in Banken, Behörden, Regierungen oder milliardenschweren Fondsgesellschaften.

Als Nachwuchstalents oder Startup hast du natürlich nicht den Zugriff auf eine solche Datenbank.

Ein Nachteil - zugegeben.

Aber du kannst ihn wettmachen: wenn dein Schleppnetz keine Ergebnisse bringt, such dir ein Dutzend potentieller Opfer und lass sie von Profis durchleuchten. Für solche Jobs gibt es Detekteien, auf die wir später noch mal zurückkommen werden.

Wenn ihr glaubt, dass sogenannte Sicherheitsfirmen bei einem solchen Auftrag Skrupel oder Zweifel hätten - falsch. Als sich der Flugzeugbauer Boeing wegen seiner fahrlässigen Produktionsmethoden mit internen Kritikern konfrontiert sah, nutzte er genau solche Unternehmen zur Einschüchterung.

In der Netflixserie „Suits“ gehörte es zum Standardrepertoire der Anwälte, bei Prozessgegnern nach Schwachstellen suchen zu lassen - „Find some Dirt“.

Falls euch das aber alles zu kompliziert erscheint - hier ein kleiner Bonus-Tipp: der lokale Kokain-Dealer.

Seine Zielgruppe sind die Besserverdienenden und die Oberschicht. Also genau unser Revier.

Und natürlich wird Stoff diesen Leute milieugerecht geliefert: mit dem Kokstaxi direkt in die Wohnung.

Der Dealer lebt vom Stoff.

Aber du weißt: Daten sind das neue Gold.

Also kaufst seine Kundenliste mit den Handy-Nummern aus Harvestehude oder Bogenhausen und gleichst sie mit den Telefon-Daten ab, die Dienstleister eins geliefert hat.

Ein Match findet sich immer.

Natürlich ist Koks nicht so schlimm wie Missbrauch.

Aber vielen ist der tiefe Sturz des Michel Friedmann noch in guter Erinnerung.

Gegebenenfalls muss man seine finanziellen Erwartungen eben an die Qualität des Kompromats nach unten anpassen.

Wenn es aber um die vollen 100 Millionen geht, ist fast jeder Aufwand gerechtfertigt. Da können wir durchaus 5 oder sogar 10 Millionen in die Recherche investieren und der Return of Investment bleibt immer noch attraktiv.

Und glaubt mir: mit 10 Millionen grabe ich so tief, dass ich Dinge finde, die ihr selbst vergessen habt.

Der Mensch, der kein Geheimnis hat, muß erst noch erfunden werden. Und das gilt ganz besonders für den Kreis der Superreichen.

Wir werden also etwas finden.

Und dann beginnt die nächste Phase. Davon mehr in Lektion 2.

---

<sup>1</sup> <https://de.statista.com/statistik/daten/studie/152525/umfrage/entwicklung-der-polizeilichen-aufklaerungsquote-bei-mord-seit-1995/>