Die Cyber-Profis

TINA GROLL UND CEM KARAKAYA

DIE CYBER-PROFIS

LASSEN SIE IHRE IDENTITÄT NICHT UNBEAUFSICHTIGT

Zwei Experten
für Internetkriminalität decken auf

ARISTON

Die in diesem Buch geschilderten Fälle basieren auf wahren Begebenheiten, wurden aber abgewandelt und anonymisiert. Aus persönlichkeitsrechtlichen Gründen wurden Namen, Adressen, Orte, Aussehen und Beruf verfremdet.

Penguin Random House Verlagsgruppe FSC® N001967

3. Auflage

Neumarkter Straße 28, 81673 München
produktsicherheit@penguinrandomhouse.de
(Vorstehende Angaben sind zugleich Pflichtinformationen nach GPSR)

Redaktion: Dr. Evelyn Boos-Körner
Umschlaggestaltung: Hauptmann & Kompanie Werbeagentur, Zürich
unter Verwendung eines Fotos von Kay Blaschke
Satz: Satzwerk Huber, Germering
Druck und Bindung: CPI books GmbH, Leck
Printed in the EU

ISBN: 978-3-424-20183-3

Für unsere Töchter, für eine bessere Zukunft

Inhalt

1. Eine Begegnung mit Folgen 11

Das Opfer 11
Der Präventionsexperte 15
Warum wir dieses Buch schreiben und an wen es sich richtet 18

2. Meine Identität gehört mir! (von Tina Groll) 25

Wie man die Identität eines anderen stiehlt 30
Identitätsdiebstahl, Identitätsmissbrauch und die Sache mit der Statistik 32
Ein Blick auf Täter und Taten 35
Cem Karakaya erzählt aus dem Polizeialltag: Gesucht und (nicht) gefunden 38
Cem Karakaya erzählt aus dem Polizeialltag: Stalking durch den Ex 44
Die Schuldfrage in Zeiten von Big Data 48
Die Täter werden selten erwischt 56
Cem Karakaya erzählt aus dem Polizeialltag: Cybermobbing an Schulen 59

3. Fake-Chefs, Fake-News, Fake-Pässe: Identitätsmissbrauch in Wirtschaft, Politik und für Terror 63

Cem Karakaya erzählt aus dem Polizeialltag: Gefakte Chefs 65

Entfesselte Skandale: Wenn ein Shitstorm die Reputation zerstört ... 79
Propaganda-Bots und Wählermanipulationen ... 81
Von Kettenbriefen und Hoaxes ... 92
Cem Karakaya erzählt aus dem Polizeialltag: Cybermachenschaften von Terroristen ... 97

4. Daten und Taten: Wozu sich Daten missbrauchen lassen ... 106

Wie Big Data uns ein zweites Ich verschafft ... 106
Datensammelwut frei Haus: Woher die Daten kommen ... 110
Abschied von der Anonymität ... 114
Was unsere Haushaltsgeräte über uns verraten ... 116
Cem Karakaya erzählt aus dem Polizeialltag: Die Taschenlampe, der Spion ... 118
Was wir zu verbergen haben ... 121

5. Kleinkriminelle Gauner, hochkriminelle Hacker und hackende Geheimagenten: Die Täter im Fokus ... 124

Die Maschen der Täter ... 129
Cem Karakaya erzählt aus dem Polizeialltag: Wie die Attacken funktionieren ... 131
Cem Karakaya und das Wiedersehen mit Julia ... 141
Cem Karakaya erzählt aus dem Polizeialltag: Ausgetrickst im Kaffeeladen ... 144
Cem Karakaya erzählt aus dem Polizeialltag: Ich will befördert werden! ... 148
Neuland Internetkriminalität? Wie die Polizei arbeitet ... 153
Cem Karakaya erzählt aus dem Polizeialltag: Stell dir vor, die Polizei glaubt dir nicht ... 155
Tatort Darknet ... 157

6. Wie aus digitaler Beute echtes Geld wird 168

Abenteuer Internetliebe 173
Bitcoins und Onlinecasinos 185

7. Die Folgen für die Opfer und wie man sich schützen kann 192

Noch Jahre später falsche Daten (von Tina Groll) 201
Tipps zum Schutz: Wie kann man sich gegen Cybercrime absichern? 207
Exkurs: Präventionstipps für Kinder und Jugendliche 214
Cem Karakaya erzählt aus der Präventionsarbeit: Wie man Kinder anspricht 215
Frühe Sensibilisierung 216
Vorsicht vor Challenges 217
Zur Medienkompetenz gehört auch Rechtsverständnis 218
Vertrauen ist der Schlüssel 219
Ein Test für die Medienkompetenz 220
Regeln für die Mediennutzung 221
Handy erst ab 16 Jahren 223

8. Verräterische Daten: In welcher Welt wollen wir leben? 226

Überblick über Verschlüsselungstechniken 235

Quellenangaben 240

Kapitel 1
Eine Begegnung mit Folgen

Das Opfer

Ich habe Angst, den Briefkasten zu öffnen.

Seit vielen Jahren.

Wenn ich nach Hause komme, gehe ich sofort zum Briefkasten. Wenn ich länger in den Urlaub fahre, werde ich schon Tage vor der Heimreise nervös beim Gedanken, den Briefkasten nach der Rückkehr öffnen zu müssen. Ist es dann so weit, pocht mein Herz laut, meine Hände schwitzen. Ich hoffe, dass ich im Briefkasten nichts Schlimmes finden werde. Und damit meine ich Schreiben, die ich »böse Post« nenne. Nein, ich bin nicht verrückt. Ich leide auch nicht unter einer seltenen Phobie.

Ich wurde im Jahr 2009 Opfer eines Identitätsdiebstahls.[1] Monatelang flatterten mir beinahe täglich Mahnungen und Drohschreiben von Inkassounternehmen ins Haus. Und obwohl der Datenmissbrauch schon so viele Jahre zurückliegt, bestimmen bis zum heutigen Tag falsche Daten mein Leben immer wieder fremd.

»Weil Sie auf die vorbenannten Forderungen noch immer nicht reagiert haben, leiten wir jetzt das Mahnverfahren ein«, stand beispielsweise in den Schreiben. Schulden sollte ich gemacht und Waren bezogen haben von Unternehmen, deren Namen ich noch nie gehört hatte. Die Sachen wurden an Adressen geliefert, die nie die meinen waren. Dort sollte es sogar Menschen gegeben haben, die – so stand es in einem Schreiben einer Inkas-

sofirma – »zweifellos bezeugen können, dass Sie, Tina Groll, dort gewohnt haben.«

Sogar Haftbefehle lagen gegen mich vor. Monatelang suchte die Polizei in anderen Städten nach mir, es gab Einträge ins Schuldnerverzeichnis, ich wurde sogar in Abwesenheit verurteilt. Alles das passierte, während ich nichts ahnend mein normales Leben als Journalistin in Berlin lebte.

Ich arbeite als Redakteurin in der Onlineredaktion einer großen deutschen Wochenzeitung. Durch meinen Beruf konnte ich für Berichterstattung über meinen eigenen Fall und das Phänomen an sich sorgen, dadurch schenkten mir die Inkassounternehmen schneller Glauben. Doch die allermeisten Opfer von Identitätsdiebstahl und Internetkriminalität können das nicht. Seit 2010 betreibe ich unter der Domain identitaetsdiebstahl.info eine Informationswebsite für Betroffene, die den Opfern die wichtigsten Antworten auf ihre meist drängenden Fragen geben soll. Mit Sorge stelle ich fest: Die Zahl der Betroffenen, die sich bei mir melden, steigt ständig. Waren es in den ersten Jahren eine Handvoll Menschen im Monat, schaffe ich es heute kaum noch, den vielen Anfragen nachzukommen. Und alle Opfer sehen sich wie ich damals einer Situation des Kontrollverlusts ausgesetzt, die aus der Feder von Franz Kafka stammen könnte. Unschuldig bedroht, völlig verunsichert, was gerade geschieht, und absolut im Unklaren darüber, welche falschen Daten im Umlauf sind und welches Ausmaß der Schaden hat.

Aber auch wenn so gut wie jedes Opfer den Eindruck hat, völlig allein zu sein: Identitätsdiebstahl und Identitätsmissbrauch sind zu einem Massenphänomen geworden. Studien zufolge soll schon jeder dritte bis fünfte Deutsche Opfer geworden sein.[2] Tendenz steigend.

Ob das wirklich stimmt, lässt sich nicht ohne Weiteres feststellen. Denn es fehlen verlässliche Statistiken. Niemand weiß, wie viele Identitäten in Deutschland, in der EU oder weltweit schon

gestohlen worden sind. Geschweige denn, was Kriminelle mit den gestohlenen Daten anfangen. In der Regel nutzen sie den Namen, das Geburtsdatum und andere personenbezogene Daten eines Fremden, um damit Straftaten zu begehen. Warenkreditbetrug wie in meinem Fall ist dabei noch eher harmlos.

Viele glauben, die falschen Forderungen seien der eigentliche Albtraum – aber das stimmt nicht. Der wahre Schaden entsteht dadurch, dass die falschen Daten mit den realen Daten des Opfers über Auskunfteien, datenverarbeitende Unternehmen, Behörden oder Institutionen zusammengebracht und weiterverteilt werden – schlimmstenfalls weltweit. Einmal im Umlauf, können falsche Daten eine fast toxische Wirkung entfalten und dazu führen, dass man in ständiger Angst lebt. Plötzlich gilt man als Schuldner, Krimineller oder Terrorist: Und selbst wenn man es erreicht, dass falsche Daten gelöscht werden, heißt das nicht, dass sie auch überall dort bereinigt werden, wohin sie weitergeleitet und weiterverarbeitet oder wiederum von dort gestohlen wurden. Im schlimmsten Fall muss man sich ein Leben lang gegen falsche Vorwürfe wehren. Da wird jede Ein- oder Ausreise in oder aus einem Land wegen der Furcht, unschuldig im Gefängnis zu landen, zur Nervensache.

Mich hat der Identitätsdiebstahl ein Jahr meines Lebens und rund 800 Arbeitsstunden gekostet. Allerdings nicht die Überzeugung, dass das Netz eigentlich etwas Gutes ist. Ich bin mit Computern groß geworden, das Netz war immer ein selbstverständlicher Teil meines Lebens und notwendiges Rüstzeug für meinen Beruf. Heute betrachte ich die Erfahrung, Opfer von Internetkriminalität geworden zu sein, als etwas, das leider zu den normalen Lebensrisiken in der digitalen Welt gehört.

Das war allerdings nicht immer so.

In den ersten Jahren nach dem Datendiebstahl wollte ich die Tat nur noch vergessen und auch nicht mehr damit in Verbindung gebracht werden. Warum? Weil ich immerzu gefragt wurde, wie

denn so etwas passieren konnte. Weil ich es satt hatte, dass Menschen staunend und gruselnd an meinen Lippen hingen, wenn ich von den Haftbefehlen erzählte und dem Kampf, die Behörden davon zu überzeugen, dass nicht ich die Kriminelle war, sondern dass schlicht Fremde unter meinem Namen Straftaten begangen hatten.

Und was mich am allermeisten ärgerte, war die ständige Annahme, ich sei nicht sorgfältig mit meinen Daten umgegangen. Mich machte diese Unterstellung zornig. Ich wollte nicht mehr das vermeintlich naive Opfer sein, das möglicherweise fahrlässig den Datenmissbrauch in Kauf genommen hatte. Ich wollte nicht mehr jeden davon überzeugen, dass es auch ihn hätte treffen können. Denn im Zeitalter der Digitalisierung, in Zeiten, in denen immer wieder neue Sicherheitslücken in Software und Hardware bekannt werden, ist es für Normalnutzer unmöglich geworden, verantwortlich mit seinen Daten umzugehen. Niemand weiß, wer welche Daten gespeichert hat. Angesichts von Prozessorlücken wie im Fall von Intel,[3] die erst Jahrzehnte später publik werden, kann niemand davon ausgehen, dass seine Geräte wirklich absolute Sicherheit bieten und Daten nicht einfach ausspioniert werden. Opfer von Cyberkriminalität sind in der Regel nicht nachlässiger mit Daten umgegangen als alle anderen auch. Sie sind auch nicht selbst schuld an dem, was ihnen widerfahren ist.

Es kann sogar Menschen treffen, die gar nicht Mitglied in einem sozialen Netzwerk sind, die nicht im Netz einkaufen und auch kein Onlinebanking nutzen. Und schon manch ein Kryptoexperte und Datenschutzspezialist ist bereits Opfer geworden. Wie das möglich ist, das werden wir in diesem Buch zeigen.

Der Präventionsexperte

Cem Karakaya kennt die Tricks der Täter. Er weiß, wie sie vorgehen, wie sie ticken. Er hat sie viele Jahre lang gejagt. Früher arbeitete er als Polizeibeamter im Auftrag der türkischen Interpol, heute kümmert er sich als Präventionsexperte bei der Münchner Polizei darum, dass weniger Menschen Opfer werden und es die Kriminellen im Netz etwas schwerer haben. Cem Karakaya hält Vorträge über die Gefahren im Netz. Seine Zielgruppe sind vor allem ganz gewöhnliche Internetnutzer. Außerdem berät er regelmäßig Bürger in der Telefonsprechstunde der Polizei München für Internetkriminalität. Ein besonderer Schwerpunkt seiner Arbeit liegt dabei auf Präventionsvorträgen an Schulen und in Bildungseinrichtungen. Denn gerade Kinder und Jugendliche sind sich der Gefahren häufig noch nicht bewusst.

In Cem Karakaya steckt aber nicht nur ein Polizist, sondern auch ein Technikfreak und Internetnutzer der ersten Stunde, der bis heute an die Idee eines freien Internets für alle Menschen glaubt und möchte, dass das Netz ebenso wie die reale Welt ein sicherer Ort ist, in dem sich alle Nutzer frei und gefahrlos bewegen können.

Leider ist der Polizeialltag im Bereich Internetkriminalität ein ständiges Katz-und-Maus-Spiel. Oft fühlen sich die Ermittler so, als verfolgten sie mit einem Dreirad Kriminelle, die mit einem Porsche davonbrausen. »Wir staunen immer wieder, wie ausgefuchst und erfinderisch die Täter sind«, sagt Cem Karakaya.

Schon seit 1988 ist er bei der Polizei. Seine Ausbildung begann er in der Türkei – genau an dem Tag, an dem sein Großvater nach vielen Dienstjahren in Pension ging. Später besuchte er die Polizeiakademie und noch später wurde er, der mehrere Fremdsprachen spricht, von Interpol rekrutiert. Hier arbeitete er in der Abteilung für auswärtige Angelegenheiten. Und weil er sich schon damals sehr gut mit Computern auskannte, war seine Karriere

gewissermaßen vorgezeichnet. Schon nach einem Jahr wurde er Feldagent bei Interpol, spezialisiert auf den Bereich neue Medien und Internetkriminalität. Nach einigen Jahren als Agent bei der türkischen Polizei wechselte er schließlich nach München, wo er seither in der Prävention tätig ist.

Auch Cem Karakaya ist mit Computern aufgewachsen. Seinen ersten bekam er von seinem Vater als Teenager, ein Commodore 64. Mit Computern und Technik hatte Vater Karakaya eigentlich nichts am Hut. Aber er spürte: Diese neue Technik würde die Welt verändern. Und dass es wichtig sein würde, dass sein Sohn sich so früh wie möglich mit der neuen Technologie auskennen sollte. »Noch bis heute bin ich meinem Vater dankbar dafür. Er gab mir den Rechner mit den Worten: ›Sohn, das ist die Zukunft. Schau, dass du damit klarkommst und lernst, wie man damit umgeht‹«, erinnert sich Cem Karakaya. Schon nach einer Woche hatte der Junge den Computer dazu gebracht, den Namen des Vaters blinkend anzuzeigen. Und so brachte sich Cem Karakaya das Programmieren selbst bei und auf den ersten Rechner folgten weitere. Nicht lange sollte es dauern, bis Cem Karakaya mit einem 56K-Modem ins Internet ging.

Diese Erinnerung ist bald 30 Jahre her. Seither hat sich extrem viel getan: Wir befinden uns mitten in der digitalen Revolution. Nicht nur die Arbeitswelt verändert sich rasant, auch unser Kommunikations- und Sozialverhalten wird tief greifend durch neue Techniken verändert. Die Jugendlichen von heute telefonieren nicht mehr stundenlang miteinander, sie chatten. Auch unser Umgang mit Privatsphäre hat sich völlig verändert. Als wir früher in einer Telefonzelle telefonierten, schlossen wir die Tür, um ungestört zu sein. Und heute? Finden wir nicht nur kaum noch Telefonzellen, denn jeder hat ein oder sogar mehrere Smartphones und wir sind fast immer online. Wir telefonieren in überfüllten ICE-Abteilen und plaudern sorglos über Firmeninterna. Wir posten bei Facebook, was wir gerade machen und wo wir uns gerade

befinden. Wir haben für diverse Apps die Ortungsfunktion eingeschaltet und unser Telefon meldet unseren Standort sowieso permanent. Unser Smartphone speichert alles. Denn es ist ein Computer, der Mikrochips und ein Betriebssystem hat. Und das Verrückteste dabei ist: Wir tragen damit freiwillig das allergrößte Spionagegerät der Menschheitsgeschichte mit uns herum und sind auch noch völlig verknallt in dieses Spielzeug. Wir können es kaum erwarten, bis das neueste Modell mit noch mehr Überwachungsfunktionen auf dem Markt ist. Und wir zahlen sogar noch viel Geld dafür.

Wir können auch andere mit diesem Gerät jederzeit überwachen – und wir machen auch fleißig und begeistert Gebrauch davon. Zum Beispiel beim Chatten: weil ein zweites Häkchen dem Gegenüber zeigt, dass wir eine Nachricht gelesen haben.

In der digitalisierten Welt bezahlen wir ständig und überall mit unseren Daten. Und es ist für uns völlig normal geworden. Wir denken nicht einmal mehr darüber nach und fragen auch nicht, was mit unseren Daten passiert oder wofür jemand Angaben wie Name, Adresse oder Geburtsdatum haben will. Manchmal kommt es uns sogar komisch vor, wenn wir nicht ständig nach diesen sensiblen Daten gefragt werden. Es hat eine völlige Bewusstseinsumkehr stattgefunden. Als verdächtig gilt mittlerweile, wer seine Daten nicht freiwillig angeben will. Doch es lohnt sich, für die Privatheit dieser Daten zu kämpfen. Denn in ihnen steckt so viel mehr: unsere Likes, Kontakte und Freunde, Gewohnheiten, Interessen, Träumen, Hoffnungen – unser Leben.

Warum wir dieses Buch schreiben und an wen es sich richtet

Die kriminellen Missbrauchsmöglichkeiten in Zeiten von Big Data sind schier unendlich. 23 Millionen Deutsche sind im Jahr 2017 Opfer von Cyberkriminalität geworden. Das zeigt eine aktuelle Studie des US-amerikanischen IT-Sicherheitsunternehmens Norton by Symantec.[4] Hinzu kommen erstens Sicherheitslücken wie beispielsweise Meltdown und Spectre,[5] die von Prozessoren ausgehen. Oder zweitens Hackerangriffe auf Unternehmen, die darauf abzielen, horrende Lösegelder zu erpressen mit zerstörerischer Software wie im Fall von WannaCry oder Petya. Diese sollten beispielsweise Krankenhäuser und Unternehmen aus der Versorgungs- und Energiewirtschaft lahmlegen. Oder auch drittens die Angst, dass Hacker Wahlen manipulieren könnten.

In der digitalen Welt lauern viele Gefahren, mit denen wir umgehen lernen müssen und an die sich die Gesetzgebung erst nach und nach anpasst. Die EU-Datenschutz-Grundverordnung (DSGVO) oder das Netzwerkdurchsetzungsgesetz (NetzDG) sind zwei Beispiele dafür, wie die Politik und Gesetzgebung erst Jahre später auf Phänomene des digitalen Zeitalters reagiert haben, um auf neue juristische Probleme eine Antwort zu geben.

Die digitalen Gefahren sind das eine. Wir möchten mit diesem Buch aber keine Ängste schüren, keine Technikkritik üben, nicht fatalistisch werden. Denn eine globalisierte, digitalisierte Welt bietet auch herausragende Möglichkeiten. Das Internet, Big Data und die Digitalisierung generell machen unsere Welt in vielen Bereichen besser. Menschen überall auf der Erde können miteinander jederzeit in Kontakt treten, Ideen und Gedanken teilen oder gemeinsam lernen und miteinander wachsen. Beteiligung und Teilhabe sind durch die neuen Technologien so viel einfacher möglich. Das ist eine Chance für die Demokratie, eine Chance für mehr Gerechtigkeit und Toleranz, für gegenseitiges Verständnis –

und somit auch eine Chance für mehr Frieden auf der Welt. Vorausgesetzt, wir überlassen das Netz nicht den Kriminellen, Schurken und Terroristen, aber eben auch nicht Staaten, Geheimdiensten und Wirtschaftsmächten allein. Das Internet hatte immer auch eine basisdemokratische Grundidee – und daher brauchen wir Netzkompetenz einerseits, digitale Bürgerrechte andererseits sowie Aufgeschlossenheit und Neugierde und den Mut, niemals aufzugeben.

Fakt ist: Kriminalität und Menschen, die keine guten Absichten verfolgen, gibt es in der Online- wie auch in der Offlinewelt. Man kann zwar Türen und Fenster verschließen, sein Haus mit einer Alarmanlage sichern und doppelte Schlösser anbringen – und trotzdem kann es doch passieren, dass es zu einem Einbruch kommt. Und nicht jeder kann sich ein umfassendes Sicherheitskonzept mit teuersten Vorkehrungen leisten. Auch das ist die Realität. Daher ist auch niemand schuld daran, wenn er oder sie zum Opfer wird. Das gilt für Verbrechen in der realen Welt ebenso wie Verbrechen in der digitalen Welt.

Doch noch immer wird in der Debatte über Datenschutz und Cybercrime so getan, als trügen die vielen Opfer eine Mitschuld daran. Dabei hantieren Unternehmen oft fahrlässig mit Kunden-, Nutzer- oder auch Mitarbeiterdaten. Behörden und Firmen halten sich oft nicht ans Datenschutzgesetz – und auch wenn das deutsche bzw. nun europäische Datenschutzgesetz eines der besten auf der ganzen Welt ist, so greift es doch in vielen Fragen viel zu kurz. Und nationalstaatliche Gesetze oder auch Regelungen auf europäischer Ebene sind zwar ein Schritt in die richtige Richtung, funktionieren aber in einer globalisierten Welt mit weltweit agierenden Akteuren wie Microsoft, Facebook oder Google einfach nicht.

Wir brauchen dringend einen besseren Datenschutz, der Opfer von Datenmissbrauch stärker schützt. Das neue Datenschutzgesetz sieht zwar eine Beweisumkehr und kräftige Bußgelder vor für den, der mit Daten schlampt – inwieweit normale Verbraucher