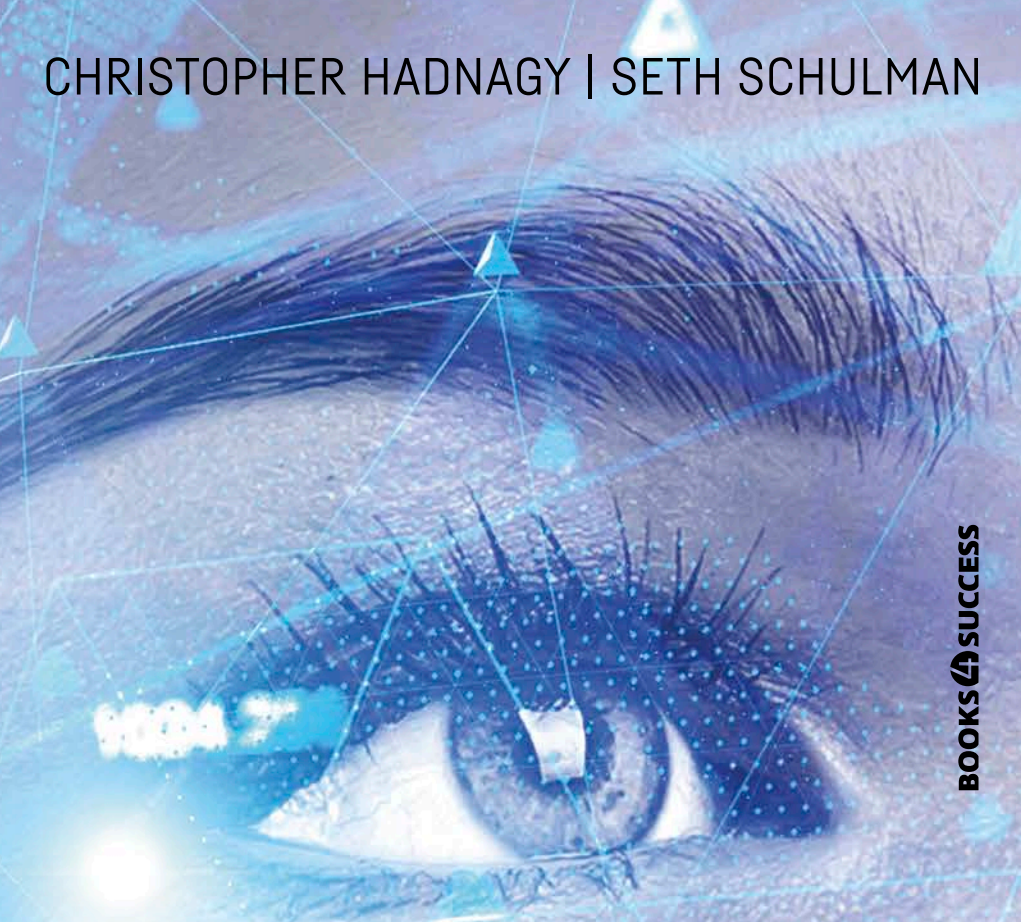
CHRISTOPHER HADNAGY | SETH SCHULMAN



BOOKS4SUCCESS

Wie Social Engineering funktioniert und wie Sie sich dagegen schützen

HUMAN HACKING

Die Originalausgabe erschien unter dem Titel
HUMAN HACKING
Win Friends, Influence People, and Leave Them Better Off for Having Met You
bei HarperCollins.
ISBN 978-0-06-300178-7

Published by arrangement with Harper Business, an imprint of HarperCollins Publishers, LLC.

Übersetzung: Frank Sievers
Gestaltung Cover: Daniela Freitag
Fotos (S. 215, 217, 221, 223, 224, 225, 226, 227):
Amaya Hadnagy and Christopher Hadnagy
Gestaltung, Satz: Sabrina Slopek
Herstellung: Daniela Freitag
Lektorat: Sebastian Politz
Druck: CPI books GmbH, Leck, Germany

ISBN 978-3-86470-759-9

Bibliografische Information der Deutschen Nationalbibliothek:
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

BÖRSEN MEDIEN
AKTIENGESELLSCHAFT

Postfach 1449 • 95305 Kulmbach
Tel: +49 9221 9051-0 • Fax: +49 9221 9051-4444
E-Mail: buecher@boersenmedien.de
www.books4success.de
www.facebook.com/plassenbuchverlage
www.instagram.com/plassen_buchverlage

Für Areesa, die Liebe meines Lebens.
Du bist meine beste Freundin und
einer der wunderbarsten Menschen,
denen ich jemals begegnet bin.

Für Colin. Zu sehen, wie du zu dem Mann wurdest,
der du heute bist, hat mich
unendlich hoffnungsfroh gemacht.
Ich bin wahnsinnig stolz auf dich.

Für Amaya. Es gibt keine Worte,
um meine Liebe für dich zu beschreiben.
Deine Schönheit und
dein Talent versetzen mich in Erstaunen.

CHRISTOPHER HADNAGY | SETH SCHULMAN

HUMAN HACKING

Wie Social Engineering funktioniert und
wie Sie sich dagegen schützen

BOOKS 4 SUCCESS

INHALT

BITTE VOR DER LEKTÜRE DIESES BUCHES LESEN UND UNTERSCHREIBEN

Die in diesem Buch beschriebenen Techniken sind extrem wirkungsvoll. Jahr für Jahr wenden unzählige Verbrecher sie weltweit an, um andere Menschen zu manipulieren, damit diese genau das tun, was sie wollen. Sie rauben Unternehmen und Einzelpersonen Milliardenbeträge, zerstören das Leben anderer Menschen und beeinflussen die politische Entwicklung ganzer Nationen. Wenn ich Ihnen diese Techniken darlege, vertraue ich darauf, dass Sie sie niemals zu unlauteren Zwecken einsetzen werden, sondern ausschließlich zum Guten. Nicht nur Sie, sondern auch alle anderen Menschen sollen davon profitieren und Sie dürfen sie niemals einsetzen, um Ihrem Gegenüber zu schaden. Ich meine es ernst. Es stehen Leben auf dem Spiel! Deshalb lesen Sie vor der Lektüre des Buches bitte das folgende Gelöbnis und unterschreiben Sie es:

Ich, _____, schwöre feierlich, diese Fähigkeiten nicht anzuwenden, um andere Menschen aus egoistischen Motiven zu manipulieren und mich einseitig zu bereichern. Ich darf diese Fähigkeiten einsetzen, um daraus Vorteile zu ziehen, achte dabei aber in jedem Fall darauf, dass die Menschen, denen ich begegne, ebenfalls davon profitieren und nicht ihren eigenen Interessen zuwiderhandeln, um meinen Wünschen nachzukommen. Außerdem verspreche ich, bei der Anwendung dieser Fähigkeiten die Privatsphäre anderer Menschen zu respektieren und meine Selbstwahrnehmung zu verbessern, sodass ich ein besserer Partner, Freund und Nachbar und ein besseres Familienmitglied sein kann. Vor allem aber verspreche ich, diese Fähigkeiten so einzusetzen, dass sich alle Menschen, mit denen ich zu tun habe, durch unsere Begegnung bereichert fühlen. Sollte mir das einmal nicht gelingen, was gelegentlich vorkommen mag, verspreche ich, aus dieser Erfahrung zu lernen und es das nächste Mal besser zu machen.

Gezeichnet:

_____

(Datum und Unterschrift)

IHRE NEUEN SUPERKRÄFTE

Es ist ein Uhr in der Nacht. Wir sitzen in einem gemieteten schwarzen Chevrolet Suburban und kriechen mit ausgeschalteten Scheinwerfern querfeldein durch ödes Buschland. Ich kneife die Augen zusammen, kurve im Mondlicht um Felsgestein, Gestrüpp und einige niedrige Bäume. Mein Kumpel Ryan krallt sich am Beifahrersitz so stark fest, dass die Knöchel weiß hervortreten. Alle paar Minuten dreht er den Kopf, um sicherzugehen, dass uns keiner folgt. Ich versuche ruhig zu bleiben, atme tief ein und aus. Unser Schweigen wird nur durchbrochen von gelegentlichen Flüchen, wenn der Wagen hart aufsetzt oder wir gerade wieder knapp einen Felsbrocken verfehlt haben.

Im Kriechtempo fahren wir auf eine Reihe unauffälliger kastenförmiger Gebäude zu, die von riesigen Flutlichtanlagen und vereinzelten anderen Industrieleuchten angestrahlt werden. Genauer gesagt: Wir fahren auf den drei Meter hohen Sicherheitszaun zu, der mit Stacheldraht abschließt und zwischen uns und den Gebäuden steht.

Eben, noch ein paar Kilometer vor dem Ziel, musste ich scharf bremsen, weil uns ein Kojote vors Auto rannte. Ich frage mich nur, was zum Henker wir hier eigentlich machen.

500 Meter vor dem Zaun sehe ich nun linkerhand eine breite, tiefe Furche. „Da?“, frage ich.

„Gut“, sagt Ryan.

Ich lenke den Wagen in die Vertiefung und versuche zu vermeiden, dass er vom dichten Buschwerk zerkratzt wird, das zu beiden Seiten aufragt. Erst als ich den tiefsten Punkt erreicht habe, halte ich an. Kein Wachmann und kein Arbeiter, der in dieser staubigen Einöde unterwegs ist, kann unser Auto sehen. Von jetzt an geht es für uns zu Fuß weiter. „Irgendwer zu sehen?“, frage ich und stelle den Motor ab.

„Niemand“, sagt Ryan.

„Dann los.“

Wir steigen aus und drücken leise die Türen zu. In dieser Gegend wimmelt es von Klapperschlangen und Skorpionen, weshalb wir uns auf Zehenspitzen vorantasten und auf die kleinste Bewegung achten. Wir öffnen den Kofferraum, ziehen eine Aluminiumleiter und ein paar Meter Seil heraus. Ansonsten haben wir keinerlei Gepäck – für den Fall, dass wir einmal schnell verschwinden müssen.

„Okay“, sage ich und deute auf einen Zaunabschnitt zu unserer Linken. „Der dunkle Bereich da hinten. Da ist offenbar ein Scheinwerfer kaputt. Was Besseres werden wir kaum finden.“

Wir heben gemeinsam die Leiter hoch und gehen los. Es ist gespenstisch still, bis auf ein tiefes Brummen, das von den Gebäuden herüberschallt, und das leise Klappern der Leiter. Wir sind 80 Kilometer von der nächsten Stadt entfernt, unbewaffnet und ungebeten. Wenn uns hier etwas zustößt, wird niemand davon erfahren. Und es kann immer etwas passieren. Ich bin schon verhaftet worden und hatte eine Knarre an der Schläfe. Und das waren leichte Jobs im Vergleich zu dem hier.

Ich kann Ihnen leider nicht sagen, von welchem Gelände die Rede ist oder wo es sich befindet. Ich kann Ihnen nur sagen, dass hinter diesem Stacheldraht eine mächtige Organisation über etwas wacht, das von immensem Wert ist. Ja, das, worüber sie wacht, ist derart wertvoll, dass die Organisation zig Millionen Dollar ausgegeben hat, um dieses Gelände zu bauen und es für Außenstehende – wie uns gesagt wurde – „ganz und gar unzugänglich“ zu machen. Es ist

einer der sichersten Gebäudekomplexe der Welt. Hinter dem Stacheldraht patrouillieren Dutzende bestausgebildete Wachleute mit automatischen Waffen. Die ganze Nacht ziehen sie ihre Runden über das Gelände. Weitere Männer stehen auf hohen Geschütztürmen Wache. Mächtige Scheinwerfer schweifen in regelmäßigen Abständen über den Zaun, Hunderte Kameras verfolgen jede Bewegung auf dem Gelände und rund um den Einfassungszaun. Zudem sind diverse hoch entwickelte kostspielige Geräte im Einsatz, die ich nicht näher benennen darf. Und das alles nur zu einem einzigen Zweck: damit Typen wie Ryan und ich keinen Zutritt zum Gelände erlangen.

Wir kennen die Sicherheitsmaßnahmen so genau, weil wir unseren Einsatz wochenlang vorbereitet haben. Von einem anderen Ort aus haben wir uns mittels Phishing und Vishing (Phishing per Telefon) detaillierte Informationen über den Komplex beschafft. In scheinbar unverfänglichen Gesprächen haben uns Personen, die hinter dem Stacheldraht und an anderen Standorten der Organisation arbeiten, operative Pläne, Einzelheiten in der Terminplanung und sogar die Namen von Mitarbeitern und Managern offengelegt, und zwar so viele Namen, dass wir in groben Zügen die Betriebshierarchie der Organisation an diesem Standort nachzeichnen konnten.

In den letzten Tagen haben wir dann noch weitere Informationen gesammelt, indem wir uns persönlich auf dem Gelände umgesehen haben. Wir hatten herausgefunden, dass die Organisation dabei war, in der Nähe ein weiteres Gebäude zu errichten, und in dieser Woche die Grundsteinlegung feiern wollte. Dass wir im Internet keinerlei Informationen über den neuen Standort fanden, war für uns kein Hinderungsgrund. Ein Lokalredakteur hatte mehrere Artikel über den Bau verfasst, und so schmiedeten wir den Plan, uns für diesen Journalisten und einen Kollegen vom selben Blatt auszugeben. Um den Standort zu erfahren, rief unsere Mitarbeiterin Debra in der Zentrale an und gab sich als Assistentin des Journalisten aus. „Hallo", sagte sie mit heller Stimme. „Mein Name ist Samantha, ich bin

die Sekretärin von Pete Robichaud bei *WXTT* (Name des Fernsehsenders geändert). Er kommt am Samstag um 10:30 Uhr zur Eröffnungsfeier, um für unseren Sender darüber zu berichten. Ich hätte nur kurz ein paar Nachfragen dazu."

„Einen Moment bitte", sagte der Mann am anderen Ende der Leitung. Wahrscheinlich wollte er überprüfen, ob Pete (Name ebenfalls geändert) tatsächlich auf der Gästeliste stand. „Gut, schießen Sie los."

„Okay, also als Erstes wollte ich fragen, was er mitbringen muss, um sich auszuweisen. Er braucht ein offizielles Dokument mit Foto, richtig?"

„Ja. Führerschein würde gehen. Oder ebenso ein Pass."

„Gut, wunderbar. Dann, zweite Frage, er würde gern seine eigene Kameraausrüstung mitbringen. Geht das in Ordnung? Irgendwas, worauf er achten muss?"

„Geht klar", sagte der Mann. „Aber er wird am Eingang natürlich durchsucht."

„Selbstverständlich", sagte unsere Mitarbeiterin. „Dann komme ich schon zu meiner letzten Frage ... nur um sicherzugehen. Wir haben anscheinend seine Einladung verlegt, deshalb wollte ich nur noch mal nach der genauen Adresse fragen und wo er genau hinmuss."

„Kein Problem", sagte der Mann. Und gab uns genau die Information, die wir brauchten.

Das Ganze wirkte wie ein belangloses Gespräch und dauerte kaum 30 Sekunden. Wahrscheinlich verschwendete der Mann am anderen Ende keinen weiteren Gedanken darauf. Aber es waren hier mehr als nur freundliche Worte ausgetauscht worden. Debra wollte eine einzige Information erhalten – die Adresse. Dazu stellte sie zunächst zwei Aufwärmfragen, um sich nach ganz einfachen Dingen zu erkundigen, die der Mann am anderen Ende der Leitung problemlos würde beantworten können. Diese Technik nennen wir in unserer Branche „Entgegenkommen". Die Aufwärmfragen dienten dazu, dem Mann das Gefühl zu geben, er könne ihrer Erwartung entspre-

chen, ihre Fragen zu beantworten. Wenn er schon zwei Fragen beantwortet hat, ist er geneigter, auch die dritte zu beantworten, sofern sie nicht zu absonderlich ist und keinen Argwohn weckt. Debra schlug sogar selbst noch eine Antwort auf die erste Frage vor, womit sie ihm signalisierte, dass sie wusste, was sie tat, Erfahrung mit solchen Dingen besaß und alles seine Ordnung hatte.

Debra wandte aber noch einige andere Techniken an. Die dritte Frage leitete sie damit ein, sie wolle nur „sichergehen" – so als wüsste sie die Antwort bereits. Damit stellte sie die Frage auf eine Weise, dass es ihrem Gegenüber ganz normal vorkommen musste, sie gestellt zu bekommen. Und noch davor, als sie fragte, ob ihr Chef auf irgendetwas achten müsse, stellte sie sich dumm und bat den Mann am anderen Ende der Leitung damit indirekt darum, Lehrer zu spielen. Damit schmeichelte sie seinem Ego, sie erkannte seine Autorität an und machte ihn entspannter und gesprächsbereiter – all das zusätzlich erleichtert durch den Geschlechterunterschied.

Dank dieses und anderer ähnlicher Gespräche konnten wir am Tag vor dem Fest das Gelände besuchen und hätten uns auch beinahe Zutritt verschafft. Doch dann schöpfte das Sicherheitspersonal Verdacht und hielt uns auf. Zuvor aber hatten wir bereits zahlreiche Einzelheiten über die Sicherheitsmaßnahmen und die Wachausbildung erfahren, welche Waffen die Wachen tragen und auf welche Bedrohungen sie achten, welche Kameras auf dem Gelände eingesetzt werden und so weiter.

Jetzt versuchen Ryan und ich erneut, uns Zutritt zu verschaffen, allerdings auf eine deutlich gefährlichere Art und Weise. Mitten in der Nacht konnte eine Wache leicht das Nervenflattern kriegen, wenn zwei ganz in Schwarz gekleidete Unbekannte auf den Zaun zuschlichen, und würde erst schießen und dann Fragen stellen. Mit meinen 1,90 Meter bin ich nicht gerade ein kleines Ziel. Ich versuche den Gedanken beiseitezuschieben, während wir uns zum Zaun vorarbeiten. Leicht ist es nicht. Immer wieder kommt mir das Telefongespräch in den Sinn, das ich zuvor mit meiner Frau und meinen

Kindern geführt hatte, um ihnen zu sagen, dass ich sie liebe. Bei jedem Geräusch schnellt mein Puls hoch und ich halte den Atem an. Erneut frage ich mich, was zum Henker wir hier machen.

Als wir den dunklen Bereich vor dem Zaun erreicht haben, sehen wir uns um. Die Luft ist rein. Ich lehne die Leiter an den Maschendraht, dann nehmen wir das Seil, um damit den Stacheldraht herunterzudrücken. Ryan filmt mich per Handy, als ich die Leiter hochsteige, um über den Zaun zu klettern. Ich schaue mich um, ob die Wachen uns gesichtet haben. Nein, zum Glück nicht.

Vielleicht eine Stunde lang erkunden Ryan und ich das Gelände, dringen in mehrere Gebäude und große Anlagen ein und machen Foto- und Videoaufnahmen von allem, was wir sehen. Nicht ein einziges Mal kommt ein Wachmann auch nur in unsere Nähe. Sie haben offenbar keine Ahnung, dass wir hier sind. Trotzdem ist jede Sekunde eine Tortur, Schläfenpochen, Adrenalinrausch.

Als wir der Ansicht sind, genug Material gesammelt zu haben, brechen wir unseren Erkundungsgang ab und kehren zum Wagen zurück. In den nächsten Tagen starten wir mit einfachen technischen Hilfsmitteln und psychologischen Tricks noch weitere Angriffe auf das Gelände. Irgendwann werden wir doch von Wachleuten angeschrien, die uns ihre Waffe an den Kopf halten, aber erst, nachdem wir schon stundenlang durch die Gebäude gelaufen und in die sensibelsten und bestbewachten Areale eingedrungen sind.

„Ganz und gar unzugänglich?“ Sieht nicht so aus.

Wer wir sind und was wir tun

Wenn Sie jetzt meinen, Ryan und ich wären Regierungsspione, Schwerverbrecher oder furchtlose Adrenalinjunkies, die die nächste Million Follower auf Youtube einfahren wollen, dann liegen Sie falsch. Wir sind nichts dergleichen. Wir sind Hacker.

Die meisten Menschen denken bei Hackern an junge Technikfreaks, die sich Energydrinks reinpfeifen, während sie auf ihren Computer einhacken, um Daten zu stehlen, Webseiten zum Absturz

zu bringen oder Viagra-Spammails zu verschicken. Aber es gibt auch „gute" Hacker, professionelle Sicherheitsleute, die von Regierungen und Unternehmen engagiert werden, um sie vor den „bösen Jungs" zu beschützen. Und unter diesen guten Hackern gibt es einige wenige, die sich nicht mit der technischen Seite befassen, dem Eindringen in fremde Computer, sondern der schmutzigen, der menschlichen Seite. Dieser Unterart von Hackern gelingt es, selbst strengste Sicherheitsvorkehrungen zu umgehen, nicht indem sie Codes programmieren und sich in Maschinen hacken, sondern indem sie Menschen hacken. Im Grunde sind sie Trickbetrüger, Sprücheklopfer, die arglose Menschen dazu bringen, ihnen Zugang zu Maschinen und gesicherten Räumen zu gewähren. Die besten Hacker sind so gut, dass sie nicht nur bekommen, was sie wollen, sondern es auf eine Weise anstellen, dass ihr Angriffsziel am Ende sogar meint, *eine angenehme Begegnung gehabt zu haben*.

Ryan und ich hacken Menschen. Keine Angst, wir gehören zu den Guten. Wir denken wie die Bösen und wenden ausgeklügelte psychologische Methoden und Techniken an, um in Server und Räume einzudringen. Wenn uns das gelingt, und das ist meistens der Fall, erfahren unsere Kunden dadurch, wo ihre Schwachstellen sind, und können sie beheben, sodass die Sicherheit für ihre Kunden und für die Gesellschaft insgesamt steigt. Genau das haben wir in jener Nacht in der Wüste gemacht – wir haben die Sicherheit eines angeblich hochsicheren Geländes auf den Prüfstand gestellt und seine Schwächen aufgedeckt, damit unsere Kunden sie beheben können, bevor die bösen Jungs kommen und verheerenden Schaden anrichten. Wir verdienen unseren Lebensunterhalt damit, fremde Menschen dazu zu bringen, zu tun und zu sagen, was wir wollen.

Ich habe mehr als zehn Jahre an meinen Techniken gefeilt und bin damit in hoch gesicherte Anlagen und Computernetzwerke eingedrungen, weshalb sich ein Journalist mit dem Spezialgebiet Sicherheit gefragt hat, ob ich womöglich „der gefährlichste Mann Amerikas"[1] sei. Das bin ich sicher nicht. Aber wir bringen unsere Methoden Spionen, Militärangehörigen und Sicherheitsleuten auf der ganzen

Welt bei, damit sie den *wirklich* gefährlichen Jungs jederzeit einen Schritt voraus sind. In diesem Buch verrate ich Ihnen unsere Geheimnisse, damit Sie sie privat und beruflich nutzen können. Sie werden lernen, schnell und effektiv die Körpersprache anderer Menschen zu lesen, mit den richtigen Sätzen andere im Handumdrehen auf Ihre Seite zu bringen, Bitten auf eine Weise zu äußern, dass die Wahrscheinlichkeit einer positiven Antwort erheblich steigt, Menschen zu erkennen, die Sie zu manipulieren versuchen, sich den Ablauf wichtiger Gespräch im Vorhinein genau zu überlegen, um Ihre Erfolgschancen zu erhöhen, und vieles mehr. Ob Sie befördert werden wollen, Menschen dazu bringen möchten, Ihnen etwas kostenlos zur Verfügung zu stellen oder Ihnen zu sagen, was sie wirklich denken, oder ob Sie Ihre Beziehungen verbessern wollen, indem Sie ein besseres Kommunikationsverhalten erlernen – machen Sie unsere Methoden zu Ihrer neuen Geheimwaffe.

Sie werden feststellen, dass unsere Methode des Menschenhackens jeder und jedem dabei helfen kann, Freunde zu finden, andere Menschen zu beeinflussen und die eigenen Ziele zu erreichen. Auch Ihnen.

Hacken auf die moderne Art

Vielleicht klingt es für Sie seltsam, dass jemand keine Computer, sondern Menschen hackt. Wer hätte gedacht, dass so etwas einmal „in Mode" kommt? Ich anfangs jedenfalls nicht. Es war 1991. Ich flog nach nur zwei Monaten vom College, weil ich ein bisschen herumgedaddelt hatte. Na ja, „ein bisschen" ist vielleicht untertrieben – ich hatte mich an den simplen Modems des Campus zu schaffen gemacht und damit am Ende praktisch das gesamte Telefonsystem von Sarasota, Florida, für einen Tag lahmgelegt.

Danach habe ich mich erst mal treiben lassen. Ich besaß die Gabe, andere Leute dazu zu bringen, mir Fakten zu verraten, die mich eigentlich nichts angingen. Die nutzte ich, um mir Jobs zu beschaffen, die mich interessierten. Etwa ein Jahr nach meinem Rausschmiss

– ich hatte gerade einen Job als Dokumentenlieferant – stiefelte ich ins Verwaltungsbüro eines Wohnkomplexes mit 25 Apartments und begann ein Gespräch mit dem Inhaber. Ich war ihm nie zuvor begegnet, hatte ihm aber binnen weniger Minuten meine tiefsten und dunkelsten Geheimnisse anvertraut. Es stellte sich heraus, dass er einige private Probleme hatte und verreisen musste, um sie zu lösen. Zwei Stunden später hatte ich einen gut bezahlten Job als stellvertretender Vermieter und Verwalter des Wohnkomplexes – ohne irgendeine berufliche Erfahrung auf dem Gebiet. Damals war ich 17 Jahre alt.

Ich machte den Job eine Weile und hörte auf, als er mir langweilig wurde. Inzwischen hatte ich mir in den Kopf gesetzt, dass es cool wäre, selbst der Chef zu sein. Ich kuckte mir ein piekfeines Restaurant aus und fragte – ohne Küchenerfahrung – nach einem Job. Kaum zu glauben, aber zwei Stunden später war ich eingestellt.

Irgendwann wurde mir auch das langweilig, weshalb ich nach einem anderen Job Ausschau hielt, in dem ich ebenfalls keine Erfahrung hatte. Und dann noch einen. Und noch einen. Mit Ende 20 arbeitete ich als internationaler Handelsvertreter für ein Unternehmen, das bizarrerweise Industrieprodukte aus Edelstahl produzierte. Ich reiste um die Welt, handelte Verträge aus und verdiente eine Menge Geld. Aber ich hatte auch gerade die Frau, die ich liebte, dazu überredet, mich zu heiraten und mit mir Kinder zu bekommen. Weil ich gern mehr Zeit daheim verbringen wollte, beschloss ich, zu kündigen und mir etwas anderes zu suchen.

Mir fiel ein, dass ich aufgrund meiner College-Erfahrung womöglich ein guter Hacker wäre. Ich stöberte ein wenig im Internet und fand einen Kurs einer Sicherheitsfirma, den ich belegte. Ich war der erste Teilnehmer in der Geschichte der Firma, der einen ihrer schwersten Server knackte. Sofort bot mir der Inhaber eine Stelle an. Ich sollte mithilfe technischer Methoden physisch in Computernetzwerke eindringen.

Es gab nur ein Problem: Trotz des Kurses war ich nicht besonders gut in diesen technischen Methoden. Meine Vorzüge lagen woanders,

ich war clever, gewieft und ein gewandter Redner. Wie sich herausstellte, sollte das voll und ganz genügen. Ein paar Jahre half ich dem Team auf unerwartete Weise aus: Meine Kollegen rackerten sich mit den Computercodes ab und versuchten verwundbare Stellen in einer Software oder Hardware zu finden, um in ein System einzudringen. Das machten sie 30, 40, 50 Stunden lang. Bis ich mich einschaltete und meinte: „Soll ich den Typen mal anrufen und nach seinem Passwort fragen?"

Sie zuckten die Schultern und sagten: „Kannst es ja mal versuchen."

Zehn Minuten später waren wir im System.

Dieses Szenario wiederholte sich unzählige Male. Manchmal rief ich jemanden an, um an Informationen zu gelangen, dann verschickte ich Phishing-Mails oder spazierte einfach ohne Furcht in ein Unternehmen hinein und überredete die Mitarbeiter, mir Zugang zu ihren Servern zu verschaffen. Ich wandte dazu keine vorgefertigten Methoden an, sondern nutzte einfach meine intuitive Menschenkenntnis und Cleverness. Es funktionierte so gut, dass ich meinem Chef vorschlug, einen Kurs zu meinen Methoden zu entwickeln. Zu meiner Überraschung sagte er Ja. Ich solle mir doch bitte was ausdenken. „Auf keinen Fall", erwiderte ich. „Ich habe keine Ahnung, wie man so was macht. Ich war ja nicht mal auf dem College."

„Das ist ganz einfach", sagte er. „Du besorgst dir einfach alles, was es an relevanten Büchern zu psychologischer Theorie und Forschung gibt, und denkst darüber nach, was du eigentlich genau Tag für Tag in deinem Job machst. Das schreibst du auf und entwickelst daraus ein einfaches Konzept, das du den Leuten beibringen kannst."

Das klang gut. Also beschloss ich, es zu versuchen. 2009, nachdem ich fast ein ganzes Jahr lang Bücher gelesen und nachgedacht hatte, war mein Konzept fertig und ich veröffentlichte es im Internet. Ich hatte es schon fast wieder vergessen, als sich einige Monate später ein Verlag bei mir meldete. Sie hätten mein Konzept gesehen und wollten mich fragen, ob ich ein Fachbuch für Personen in der

Sicherheitsbranche schreiben wolle. Ich sagte Nein. Ich sei nur ein schmieriger kleiner Hacker, und keiner würde lesen wollen, was ich schreibe. Dann erzählte ich meinem Chef von dem Angebot und dachte, er würde es genauso absurd finden wie ich. Er sprang von seinem Bürosessel auf. „Bist du verrückt? Ruf sie an und schreib dieses Buch!"

Wieder folgte ich seinem Rat, und so kam 2010 mein Buch *Die Kunst des Human Hacking: Social Engineering in der Praxis* heraus, die erste Anleitung, wie man Menschen hackt. Es verkaufte sich über 100.000 Mal, was ein ziemlicher Wahnsinn ist für ein nerdiges Fachbuch. Die Bezeichnung „Social Engineering", mit der ich meine Tätigkeit beschreibe, ist ein Begriff, der schon Ende des 19. Jahrhunderts aufkam und der in den 1990er- beziehungsweise 2000er-Jahren durch den bekannten Hacker Kevin Mitnick populär wurde. In meinem Buch heißt es dazu, Social Engineering sei „der Akt der Manipulation einer Person, eine Handlung auszuführen, die *vielleicht* im besten Interesse der ‚Zielperson' liegt – oder auch *nicht*."[2] Inzwischen habe ich die Definition erweitert und unterscheide zwischen dem Versuch, Menschen zu beeinflussen, damit sie sich so verhalten oder denken, wie man es möchte, und der Manipulation, jener dunklen Kunst, bei der man das gewünschte Verhalten erzwingt. In Anbetracht der ethischen Auflagen, unter denen gute Hacker operieren – ich komme gleich ausführlich darauf zu sprechen –, kann man sagen, dass die allermeisten Social Engineers wie ich damit arbeiten, Menschen zu beeinflussen. Wir bringen sie auf raffinierte Weise dazu, sensible Daten preiszugeben, ohne sie dazu zu nötigen.

Sollten Sie uns einmal begegnen, entweder persönlich oder am Telefon oder im Internet, werden Sie sich nachher sagen, dass Sie eine angenehme, vielleicht etwas banale Begegnung mit einem anderen Menschen erlebt haben. Und Sie werden sogar denken, dass diese Begegnung Ihnen etwas gegeben hat. Aber weil wir unser Gespräch auf eine bestimmte Art und Weise gelenkt, bestimmte Worte benutzt, genau auf Ihre Reaktion geachtet haben,

haben Sie uns mit ziemlicher Sicherheit auch ein Passwort, eine Sozialversicherungsnummer oder irgendeine andere Information verraten, die wir von Ihnen wissen wollten. Tatsache ist: Ein gut ausgebildeter Social Engineer hat es gar nicht nötig, andere Menschen zu manipulieren. Seine Beeinflussungstechniken sind wirkungsvoll genug.

Erinnern Sie sich noch an die nette ältere Dame, die Sie gestern angerufen hat, um Sie um eine Spende für einen wohltätigen Zweck zu bitten, und mit der Sie ein paar Minuten nett geplaudert haben? Oder an den freundlichen Mann von UPS, der Sie nach dem Weg gefragt und ganz nebenbei eine Bemerkung über Ihr Unternehmen gemacht, einen Witz gerissen und Sie scheinbar arglos über Ihre Arbeit ausgefragt hat? Ich will Ihnen keine Angst einjagen, aber vielleicht war die Dame gar nicht so nett und der Mann gar nicht so arglos. Vielleicht waren diese Fremden bösartige Hacker, die Informationen aus Ihnen herausquetschen wollten. Höchstwahrscheinlich waren sie es nicht – wir wollen mal die Kirche im Dorf lassen –, aber möglich wäre es. Verbrecher hacken Millionen von Menschen mithilfe von Beeinflussungstechniken, die unter dem Deckmantel einer harmlosen Unterhaltung laufen. Die Opfer wissen erst, dass sie an der Nase herumgeführt wurden, wenn sie entdecken, dass jemand in ihrem Namen ein kleines Geschäftsdarlehen aufgenommen oder ihren Computer gesperrt hat und von ihnen Geld fordert.

In *Die Kunst des Human Hacking* habe ich die Grundprinzipien und Grundtechniken dargelegt, mit denen man Menschen hacken kann, damit Angestellte in der Sicherheitsbranche Angriffe abwehren und die Sicherheit ihres Unternehmens aufrechterhalten können. Rückblickend muss ich sagen, dass ich nicht besonders stolz auf dieses Buch bin. Es hat zu viele Schwächen. Aber es hat dazu beigetragen, dass Social Engineering zum Thema wurde. Und für mich persönlich war es ganz klar ein Wendepunkt. Angespornt durch den Widerhall, den das Buch in der Sicherheitsbranche erfuhr, habe ich meinen Job an den Nagel gehängt und mein eigenes Unterneh-

men gegründet. Jetzt prüfe ich Unternehmen mithilfe von „Penetrationstests" – ich habe eingangs einen solchen beschrieben – auf Sicherheitslücken und zeige Leuten, die in diesem Bereich arbeiten, wie man effektiv Menschen hackt.

In den zehn Jahren seit der Gründung meines Unternehmens haben wir nach den Prinzipien des Social Engineering 14 Millionen Phishing-Mails verschickt und über 45.000 Vishing-Anrufe getätigt. Wir sind in Hunderte Server eingedrungen und haben uns Zutritt zu Dutzenden der bestbewachten Anlagen von Unternehmen und Regierungen verschafft, darunter Banken, Konzernzentralen, Produktionsanlagen, Warenlager und Wehranlagen. Wären wir echte Diebe, hätten wir uns hochsensible Staatsgeheimnisse verschafft, Milliarden Dollar gestohlen und Millionen Menschen geschadet, indem wir ihre Identität gestohlen und sensible Daten von ihnen veröffentlicht hätten. Wir waren derart erfolgreich, dass mich kürzlich das FBI einlud, neue Agenten in seiner Verhaltensanalyseeinheit auszubilden.

Mein Team und ich bezeichnen die Fähigkeit, Menschen zu hacken, als eine Superkraft, eine psychologische Kampfkunst, mit der wir Menschen dazu bringen, so gut wie alles zu tun, was wir wollen, und dabei noch zu glauben, unsere Begegnung – sprich wir – hätte ihnen etwas gegeben. Ja, in gewisser Weise kann man sagen, dass wir sie austricksen und betrügen, aber entscheidender ist, dass wir präzise dosierte Empathie und hoch entwickelten Menschenverstand einsetzen und zu unserem Vorteil nutzen. Mithilfe von Erkenntnissen aus der Psychologie sehen wir uns genau an, wie jemand denkt und fühlt, und setzen diese Einsicht ein, um ihn so weit zu bringen, dass er unserem Ansinnen nachkommen *will*. Richtig eingesetzt, führt Social Engineering dazu, dass sich mein Gegenüber glücklicher, ruhiger, stärker, schlicht und einfach *besser* fühlt, wenn es mir hilft. Es bekommt ein kleines emotionales „Geschenk" von mir und revanchiert sich, indem es mir gibt, was ich will. Und zwar in einem kurzen, angenehmen Gespräch, das nur ein paar Minuten dauert.

Menschen hacken im Alltag

Stellen Sie sich vor, Sie könnten sich diese Fähigkeiten in Ihrem privaten und beruflichen Leben zunutze machen. Denn das können Sie. Vor Kurzem war ich mit meiner Frau und meiner Tochter am Flughafen Heathrow in London. Ich schob einen Kofferkuli mit unserem Gepäck in Richtung Check-in-Schalter, und kurz bevor ich an den Schalter kam, holperte der Kuli über eine Bodenwelle und ein paar Taschen fielen herunter. In Anspielung auf die bekannte Londoner Autobahn M5 scherzte ich: „Oh, schwerer Unfall mit Amischlitten auf der M5." Die Dame hinterm Schalter lachte. „Okay, gut", dachte ich. „Da hat sie gleich schon mal gute Laune."

Meine Frau plauderte ein paar Minuten mit ihr. „Bevor wir einchecken", sagte meine Frau, „darf ich Ihnen sagen, dass Ihr Make-up einfach fantastisch aussieht? Es passt ausgezeichnet zu Ihrem Schal. Genau so einen Schal wollte ich immer schon haben. Ich frage mich, wo man den bekommt."

Die Dame freute sich über das Kompliment, nicht zuletzt, weil sie vermutlich ihren Arbeitstag bisher überwiegend mit gestressten und missmutigen Fluggästen verbracht hatte. Die beiden plauderten noch ein bisschen weiter über Schals und Make-up, und die Schalterdame entspannte sich sichtlich – ein Lächeln legte sich auf ihr Gesicht, die Falten auf ihrer Stirn strafften sich und ihre Schultern wurden locker. Meine Frau versuchte nicht, ihr Honig um den Mund zu schmieren. Sie trug auch nicht dick auf. Das Make-up dieser Dame gefiel ihr wirklich, und das wollte sie ihr einfach gern sagen. Die Dame am Schalter konnte spüren, dass meine Frau authentisch war.

Ich sah darin eine Gelegenheit. Ich beugte mich ein wenig vor, legte den Arm um meine Frau und lächelte. Mit leicht geneigtem Kopf sagte ich: „Hey, nur eine kurze Frage. Ich dachte, wo Sie uns gerade einchecken … Wahrscheinlich ist es für uns eh zu teuer, aber könnten Sie uns vielleicht eine Auskunft darüber geben, was uns ein Upgrade von der Economyclass in die Premium Economy kosten würde?"

Sie sah nicht mich, sondern meine Frau an und flüsterte: „Behalten Sie das bitte für sich." Dann tippte sie wild auf ihrer Tastatur herum. „Ich buche Sie alle drei in die Erste Klasse."

„Was??? Vielen Dank!", erwiderten wir. „Das ist ja großartig."

Schauen wir uns einmal an, was hier genau passiert ist. Wenn wir einem anderen Menschen zum ersten Mal begegnen, kommen uns prinzipiell zuerst vier grundlegende Fragen in den Sinn:

1. Wer ist dieser Mensch?
2. Was will er?
3. Wie lange wird unsere Begegnung dauern?
4. Ist dieser Mensch eine Bedrohung für mich?

Wenn Sie an Ihre letzte Begegnung zurückdenken, waren das sicher die entscheidenden Fragen, die Sie sich gestellt haben, selbst wenn sich das Ganze womöglich nur in Ihrem Hinterkopf abgespielt hat. Wenn Sie jemanden, dem Sie zum ersten Mal begegnen, dazu bringen wollen, etwas für Sie zu tun, dann müssen Sie ihm diese vier Fragen möglichst schnell beantworten, damit er sich entspannen kann und sich wohlfühlt. Ansonsten sind Sie geliefert. Dann können Sie sagen, was Sie wollen, Ihr Gegenüber wird sich vor Ihnen in Acht nehmen und Ihrem Ansinnen nur mäßige Begeisterung entgegenbringen.

Als ich am Gepäckschalter ankam, waren für die Dame dahinter drei der vier Fragen allein durch den Kontext und mein äußeres Erscheinungsbild sofort beantwortet. Mit meinem vollen Kofferkuli war ich höchstwahrscheinlich ein Fluggast und wollte höchstwahrscheinlich einchecken. Von daher würde unsere Begegnung wohl nur wenige Minuten dauern. Nur die vierte Frage war damit noch nicht beantwortet: War ich eine Bedrohung für sie? Vermutlich nicht, aber ganz sicher sein konnte sich die Dame nicht. Vielleicht war ich betrunken und würde laut und handgreiflich werden, wenn ich keinen Fensterplatz bekäme. Vielleicht war ich nicht betrunken, aber ein streitlustiger Idiot, der die Fluglinie