REDLINE | VERLAG

NICLAS LAHMER

# SOCIAL ENGINEERING

## DIE NEUEN ANGRIFFSSTRATEGIEN DER HACKER

So wird man immun
gegen Manipulation, Phishing
und Internetattacken

NICLAS LAHMER

# SOCIAL ENGINEERING

## DIE NEUEN ANGRIFFSSTRATEGIEN DER HACKER

REDLINE | VERLAG

**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.

**Für Fragen und Anregungen:**
info@redline-verlag.de

1. Auflage 2022


Türkenstraße 89
D-80799 München
Tel.: 089 651285-0
Fax: 089 652096



Redaktion: Silvia Kinkel
Umschlaggestaltung: Marc-Torben Fischer
Umschlagabbildung: Sergey Nivens/shutterstock.com
Satz: Daniel Förster
Druck: GGP Media GmbH, Pößneck
Printed in Germany

ISBN Print 978-3-86881-898-7
ISBN E-Book (PDF) 978-3-96267-443-4
ISBN E-Book (EPUB, Mobi) 978-3-96267-444-1


*Weitere Informationen zum Verlag finden Sie unter*

www.redline-verlag.de

Beachten Sie auch unsere weiteren Verlage unter www.m-vg.de

*Für eine sichere Welt, die wir uns gemeinsam teilen*

# INHALT

# EINLEITUNG

*»Die Organisationen stecken Millionen von Dollar in Firewalls und Sicherheitssysteme und verschwenden ihr Geld, da keine dieser Maßnahmen das schwächste Glied der Sicherheitskette berücksichtigt: die Anwender und Systemadministratoren.«*

Kevin Mitnick[1]

Jedes System kann geknackt werden. Machen Sie sich das bewusst. Selbst ein analoges System kann verbrannt, vernichtet oder zerstört werden. Absolute Sicherheit gibt es nicht. Jedes System hat Schwachstellen, welche von professionellen Hackern, Dieben, Kriminellen, Unternehmen oder gar von der Regierung genutzt werden können, um Daten und Informationen zu gewinnen. Diese Daten und Informationen sind die neue Währung dieses Jahrtausends. Wo wir gestern noch mit Scheinen und Münzen bezahlt haben, sind heute Informationen und Daten mindestens genauso wertvoll, wenn nicht wertvoller.

In den letzten Jahren ist das Thema Datenschutz, Privatsphäre und Cybersecurity allgemein in seiner Bedeutung größer geworden als jemals zuvor. Das mag auch an der sich immer weiter digitalisierenden Welt liegen oder an den Enthüllungen von Whistleblowern wie Edward

Snowden. Vielleicht aber liegt es auch daran, dass es eine wachsende Zahl von Menschen gibt, die ihre Grundrechte und ihre Freiheit im digitalen Zeitalter stärker unter die Lupe nehmen wollen.

Der Schutz unserer Daten ist eines der wichtigsten Themen unserer Zeit geworden. Obgleich immer noch einige Menschen behaupten, dass sie nichts zu verbergen hätten und die digitale Privatsphäre kein Thema für sie sei. Vor allem da die Technologiekonzerne wie Meta (ehemals Facebook) durch seine Plattformen Facebook, Instagram und WhatsApp, Google durch seine Applikationen YouTube, Google Search, Analytics, Maps, Drive, Photos und Co. oder die Unternehmen Apple und Amazon, sowie Dienste wie Spotify, Netflix, Amazon Prime oder diverse gesprächige Damen wie Siri, Cortana und Alexa, fleißig Daten über ihre Nutzer sammeln. Der gläserne Mensch entsteht. »Alles kein Problem. Ich habe ja nichts zu verbergen«, höre ich dann. Ach ja? In dem Falle lassen Sie am besten die Fenster offenstehen, wenn Sie auf der Toilette sitzen und Ihr Geschäft verrichten. Lassen Sie Kameras mitlaufen, wenn Sie sich mit Ihrem Schatz vergnügen und veröffentlichen Sie doch auch gleich Ihre Kontodaten und Passwörter. Nein? Natürlich nicht! Der Grund ist: Wir alle haben etwas zu verbergen und ein Teil unseres Lebens geht niemanden etwas an. Das ist auch gut so. Wer glaubt, dass die Regierung sowieso mithört, unterschätzt die Möglichkeiten für den Schutz der eigenen Privatsphäre. Wir schließen nachts unsere Häuser, Türen und Fenster ab. Digital aber öffnen wir unsere Türen und lassen alles weit offenstehen. Schlimmer sogar. Wir veröffentlichen freiwillig im Internet Fotos von unseren Urlauben, unseren Kindern, den intimsten Momenten und Orten, an denen wir uns täglich befinden. Wer das nicht gruselig findet, dem ist nicht zu helfen.

Doch die neue digitale Welt bringt nicht nur Probleme mit sich. Die Digitalisierung schafft Komplexität, aber auch Effizienz, Klarheit, Komfort und Verfügbarkeit. Diese Vorteile nutzen uns privat sowie unseren Unternehmen. Wer sich dem entziehen will und ein rein analoges Leben

führt, verpasst den Wandel der Welt und all die Vorteile, die mit dieser Entwicklung auf uns zurollen. Wer die Digitalisierung vollständig miterleben möchte, muss sich jedoch auch an einige Spielregeln halten, welche wir noch nicht vollständig manifestiert haben. Wir spielen bereits, doch die Regeln werden uns erst so langsam bewusst. So war es auch mit den modernen Datenschutzregeln, welche uns in der EU und speziell in Deutschland durch die Datenschutzgrundverordnung, kurz DSGVO, präsentiert wurden. Die meisten dieser Anforderungen sind für Unternehmen de facto nicht umsetzbar. Das, was zwischen Theorie und Praxis entsteht, nennen wir nicht umsonst Realität, und diese ist im digitalen Zeitalter voller Hindernisse, Herausforderungen und Risiken. Überbordende Regeln lösen das Problem nicht. Ein Schritt in die richtige Richtung ist es aber.

Wer heute Dienste wie Spotify, Amazon Prime und die diversen Cloud-Systeme der Technologiekonzerne verwendet, sollte sich über die Grundlagen dieser Dienste und Systeme bewusst werden. Was machen die Wolken eigentlich? Kann Spotify Nutzerdaten analysieren und die emotionalen Momente seines Nutzers anhand der gehörten Musik interpretieren? Kann Alexa auch zuhören, wenn das Gerät gar nicht angesprochen wird?

Selbst wenn wir den Unternehmen Glauben schenken wollen und davon ausgehen, dass die Versprechungen des Datenschutzes eingehalten werden, so bleibt das Sicherheitsrisiko bestehen. Selten ist dieses Risiko ein rein digitales. Das Hauptrisiko für unsere Daten ist und bleibt der Mensch. Wir sind das Problem. Während die Schlagzeilen der letzten Jahre vermehrt von Cyberangriffen berichten und ganz langsam auch dem Otto Normalverbraucher klar wird, dass die weltweit agierenden Technologiekonzerne keine Heiligen sind, wird immer wieder vergessen zu erwähnen, dass das schwächste System der Welt der Mensch ist und auch seine eigenen Systeme das Ziel eines Angriffs sein können. Ein digitales System kann Schwachstellen haben. Denn jedes digitale System ist

in der einen oder anderen Form durch den Menschen erschaffen worden. Das bedeutet auch, dass in die Programmierung einer Maschine, einer Applikation oder eines Systems Gehirnschmalz und Zeit hineingeflossen sind. Wir hoffen, dass die Hersteller und Entwickler Sicherheitsgedanken in diese Systeme haben einfließen lassen. Das menschliche System jedoch wurde nicht durch uns, sondern durch die Natur geschaffen. Als Spezies beginnen wir gerade erst damit, zu verstehen, dass jedes sich entwickelnde System auch gegen uns verwendet werden kann. So wie eine Batterie dafür entwickelt wurde, ein anderes Gerät mit Energie zu versorgen, kann diese Batterie sich auch gegen uns wenden, überhitzen, schmelzen, brennen oder gar explodieren. Jedes System hat seine Schwachstellen. Das gilt für Server, Betriebssysteme, Hardware und vor allem für den Menschen.

Das Problem sind also wir Nutzer. Die Hauptschwachstelle des Menschen sind seine Emotionen. Psychologisch und sozialwissenschaftlich gesehen sind diese unsere größten Stärken, doch in puncto Cybersicherheit sind unsere Emotionen die reinste Pest. Aber auch aufgrund von Naivität, Dummheit, Ignoranz, Arroganz und Neugierde haben bereits einige Unternehmen und Privatpersonen Terabytes an Daten und somit auch viel Geld an Kriminelle oder andere Unternehmen verloren. Manchmal passiert Schlimmeres und ganze Unternehmen schließen ihre Pforten, da wieder einmal ein Angreifer die digitalen Systeme des Unternehmens vollständig lahmgelegt hat und der Zugang zu diesen durch listenreiche Methoden blockiert und verweigert wird.

## SCHWACHSTELLE MENSCH

Obwohl die Budgets der meisten Unternehmen für sicherheitsrelevante Themen stark beschränkt sind, investieren Unternehmen zunehmend in ihre IT-Sicherheit. Anlässlich der heutigen Bedrohungslage durch kriminelle Hacker, sogenannte Black Hats, oder durch Industriespionage haben Unternehmen verstanden, wie wichtig es ist, in ihre digitale

Sicherheit zu investieren. So stellen Unternehmen mittlerweile Hacker ein oder beauftragen sie, ihre Systeme zu testen. Was allgemein als Penetration-Testing oder auch Pen-Testing bekannt wurde, ist heute ein gängiges Mittel vieler Unternehmen, ihre Systeme sicherheitstechnisch zu prüfen. Ein ethisch agierender Hacker, auch White Hat genannt, wird hierfür gegen den Einwurf einer kleinen Münze das System eines Unternehmens – in dessen Auftrag – angreifen, Schwachstellen erkennen und Empfehlungen aussprechen, diese zu schließen. So weit so gut. Ein Penetration-Tester wird jedoch vor allem versuchen, das digitale System anzugreifen. Dazu gehören Datenbanken, Betriebssysteme, die Infrastruktur der Server und Mailserver, um nur einige zu nennen. Ein guter Penetration-Tester weiß, dass die größte Schwachstelle der Mensch ist und er diese leicht nutzen kann, um beispielsweise Malware oder Ransomware in das Unternehmen zu schleusen. Ein Beispiel:

Nehmen wir an, dass Sie in einem großen Unternehmen arbeiten und täglich 500 bis 1500 Mitarbeiter auf dem großen Firmenparkplatz ihren Pkw parken oder mit dem Bus über die Bushaltestelle auf der anderen Straßenseite zur Arbeit gelangen. Alle diese Menschen spazieren also täglich mindestens einmal zu ihrem Arbeitsplatz und einmal zurück aus dem Büro nach Hause. Stellen wir uns vor, dass ein Angreifer auf diesem Parkplatz Dutzende USB-Sticks an verschiedenen Stellen fallen gelassen hat. Tatsächlich gibt es die Möglichkeit, sogenannte Rubber-Duckies zu verwenden, welche mit einem Skript präpariert wurden, um beispielsweise Schadsoftware oder Ransomware auf dem System des Nutzers zu installieren.[2] Findet nun also jemand diesen USB-Rubber-Ducky auf dem Parkplatz, steckt diesen interessiert ein und später im Büro in den Firmenrechner, installiert sich die Schadsoftware binnen eines Moments von selbst und infiziert das System des Nutzers oder das gesamte Netzwerk. Das Skript auf dem USB-Stick gaukelt dem Rechner vor, dass es eine Tastatur wäre und die hinterlegten Eingaben im Skript von Ihnen eingetippt wurden. Selbst wenn keine Schadsoftware heruntergeladen oder installiert wurde, könnte ein Keylogger installiert werden, welcher

von nun an alle Ihre Tastenanschläge aufzeichnet und an den Empfänger übermittelt. Sie selbst merken davon nichts.

Sie mögen denken, dass niemand so dämlich sein kann, einen gefundenen USB-Stick in einen Firmenrechner zu stecken. Nein? Denken Sie doch nur an all die kostenlosen USB-Sticks, die auf Messeveranstaltungen verteilt und täglich von Mitarbeitern weltweit verwendet werden. Tatsächlich ist die Wahrscheinlichkeit sehr hoch, dass mindestens ein Mitarbeiter von 1500 potenziellen Opfern einen auf dem Parkplatz gefundenen USB-Stick mitnimmt und in den eigenen Rechner steckt, um zu prüfen, was sich auf diesem USB-Stick befindet. In diesem Fall ist dieser Angriff ein Angriff auf den Menschen.

Das Erstaunliche an einem Rubber-Ducky-Fall ist nicht die Technik oder das Skript. Erstaunlich ist hingegen, wie einfach es ist, die menschliche Natur zum eigenen Vorteil zu nutzen. Der Hacker nutzt in diesem Fall lediglich die angeborene Neugierde des Menschen für seine Zwecke. Der Hauptangriffspunkt ist also der Mensch und nicht etwa das durch den Menschen erschaffene digitale System.

Auch mithilfe kostenloser USB-Sticks auf Messeveranstaltungen kann die Naivität des Menschen ausgenutzt werden. Wir gehen in der Regel davon aus, dass der Mensch an sich nicht böse ist und uns auch nicht täuschen will. Folglich vertrauen wir Menschen, Organisationen und Behörden, die wir im Grunde genommen gar nicht kennen. Urplötzlich wird so der Mitarbeiter zum Täter.

## BEDROHUNG INNENTÄTER

Eines der großen Probleme des Menschen ist die Dualität seiner Gedanken. Im Grunde sind die meisten Menschen ziemlich einfach gestrickt. In ihnen ist der feste Glaube an das Gute und Böse verankert.

Alles hat zwei Seiten. Es gibt die Bösen und die Guten. Es gibt falsch und richtig. Es gibt die Legalität und die Illegalität. Es gibt das Opfer und den Täter. Doch ganz so simpel, wie wir uns die Welt vorstellen, ist sie nicht. Obwohl ein Mitarbeiter keine bösen Absichten in sich tragen muss, kann dieser aufgrund seiner menschlichen Natur, Naivität, Ignoranz und Neugierde zum Täter werden und das gesamte Firmennetzwerk lahmlegen. Erweitern wir diesen Gedanken einmal.

Stellen Sie sich vor, dass Sie bei einem Luftfahrtunternehmen arbeiten. Die letzten Monate war Ihr Budget ziemlich knapp, der Familienzuwachs geht ganz schön ins Geld und Sie müssen sparen. Nichtsdestotrotz muss ein neues Smartphone her, da Ihr altes kaputt gegangen ist. Sie entscheiden sich also, kein neuwertiges Gerät zu erwerben, sondern Ihrem guten Freund sein gebrauchtes Telefon abzukaufen. Am darauffolgenden Montag wählen Sie sich mit diesem neuen Mobiltelefon in das Firmennetzwerk über die WLAN-Verbindung ein, so wie es alle Mitarbeiter in Ihrer Abteilung tun, um kein eigenes Datenvolumen zu verbrauchen. Kurze Zeit später ist das gesamte Netzwerk des Unternehmens kompromittiert.

In diesem Beispiel hatte Ihr guter Freund das Smartphone ebenfalls über einen Bekannten bezogen. Diesen kennen Sie nicht. Sie wissen auch nicht, dass dieser das Smartphone wiederum von seinem Cousin erworben hat, welcher Verbindungen zu Radikalen im Jemen pflegt. Ob die Hardware, die Software oder das gesamte Betriebssystem Ihres Endgeräts manipuliert wurde, wissen Sie nicht. »Alles kein Problem. Ich setze das Gerät zurück auf die Werkseinstellung«, könnten Sie denken. Aber Sie haben sicherlich bereits den Spruch gehört: »Gelöscht ist nicht gelöscht.« Haben Sie schon einmal darüber nachgedacht, dass auch ein Smartphone nichts anderes ist als ein kleiner Computer, dessen Werkseinstellung angepasst werden kann? Sicherlich steht hinter einem solchen Vorhaben ein großer Aufwand, doch auch Terroristen scheuen keine Mühen und Kosten, um ihre Ziele zu erreichen.

Verstehen Sie mich nicht falsch. Ich bin auch ein Freund von gebrauchten Geräten und bastle für mein Leben gerne. Doch woher Ihre Endgeräte stammen und wer diese vor Ihnen in den Händen hielt, ist wichtiger als der günstigere Preis auf eBay. Einst habe ich dieses Beispiel in einem Vortrag für eine deutsche Aufsichtsbehörde genutzt. Die Teilnehmer waren sichtlich überrascht und hatten großen Gefallen an dem Beispiel. Gerne hätte man es für interne Schulungszwecke genutzt. Die Leitung der Behörde entschied jedoch, dieses Beispiel nicht in eigenen Unterrichtsmaterialien zu verwenden, weil ich angeblich ein fremdenfeindliches Beispiel verwendet hätte. Ich hatte nämlich gesagt, dass der Drittkontakt das Telefon in der Türkei erworben hatte und dort auch präparieren konnte.

Der Drittkontakt wiederum reiste nachweislich regelmäßig über die türkische Grenze nach Syrien, um dort mit islamistischen Terroristen zu sympathisieren. Ein ähnliches Szenario kannte eine andere deutsche Strafverfolgungsbehörde, die auch im Ausland tätig war, bereits. Davon wollte man aber hier in Deutschland nichts hören. Dass meine Absichten weder fremdenfeindlich noch rassistisch motiviert waren oder sind, ist, denke ich, selbstverständlich.

Stellen Sie sich also vor, dass kriminelle oder gar terroristische Vereinigungen Ihr Unternehmen, Ihren Arbeitgeber oder Ihre Organisation leise oder lautlos angreifen – das Ziel wären nämlich in erster Linie die Daten. Wie wäre es mit Flugrouten? Mit der Hilfe von flightradar24.com können Sie live im Internet verfolgen, wo sich Flugzeuge gerade befinden. Über interne Quellen, welche Sie vorab identifiziert und kompromittiert haben könnten, gelänge es Ihnen vor Abflug, die Routen der Flugzeuge zur Vorbereitung auf Ihren Angriff genau zu definieren. Alles was Sie für das Ziel des Terrorangriffs nun bräuchten, wäre eine Flugabwehrrakete (FlaRak/SAM), die das Flugzeug wenige Minuten nach dem Start in niedriger Höhe trifft und zerfetzt. Alternativ wäre die Wahl eines Innentäters ideal.

Als Innentäter beschreiben wir Menschen, die innerhalb eines Betriebes tätig sind und durch ihre Zugänge und Kenntnisse dem Unternehmen direkt schaden könnten, ohne dabei selbst in Erscheinung treten zu müssen oder dass andere von ihrem schädigenden Verhalten Kenntnis erlangen. Sie halten das für unmöglich oder Panikmache?

Etwas Ähnliches passierte mit dem russischen Flug 7K-9268. Das Flugzeug verschwand kurz nach dem Start über dem Sinai vom Radar. Wenig später meldete sich die lokale dschihadistische Gruppe namens Wilayat Sinai auf Twitter und erklärte, dass sie das Flugzeug vernichtet hätte. Wörtlich hieß es, die »Soldaten des Kalifats haben es geschafft, ein russisches Flugzeug in der Provinz Sinai herunterzuholen«. Die mehr als 220 »Kreuzzügler« an Bord der Maschine seien getötet worden.[3] Videoaufnahmen zeigten, dass die Maschine, die von Scharm el-Scheich nach Russland fliegen sollte, kurz nach dem Start in der Luft explodierte. Die Ägypter bestritten zu Beginn einen terroristischen Anschlag. Später jedoch wurde bekannt, dass ein Mitarbeiter des Flughafens in der Frachtabfertigung eine USBV (Unkonventionelle Spreng- und Brandvorrichtung) in einer Coladose versteckt hatte und diese an Bord des Flugzeugs bringen konnte, ohne selbst das Flugzeug zu besteigen. Der Mitarbeiter pflegte Kontakt zu Terroristen und Mitgliedern des islamischen Staats. Als Folge dieser abscheulichen Tat stellten viele Luftverkehrsgesellschaften, darunter auch die deutsche Lufthansa, ihre Flüge von Scharm el-Scheich ein. Der wirtschaftliche Schaden für die Ägypter war immens. Die Informationen, die der Mitarbeiter der Frachtabfertigung am Flughafen Scharm el-Scheich an seine radikalen Kollegen weitergeben konnte, wurden den Menschen zum Verhängnis.

## SOCIAL ENGINEER & HACKER

Die größte sicherheitsrelevante Herausforderung unserer Zeit ist der Schutz von Menschen, Tieren und Betriebsvermögen vor Innentätern.

Warum sollten kriminelle Hacker versuchen, nahezu unüberwindbare digitale Sicherheitsmaßnahmen zu überbrücken, wenn diese günstiger, leichter und in einem Bruchteil der Zeit durch den Menschen vor Ort überwunden werden könnten?

Genau an dieser Stelle kommt das Social Engineering ins Spiel. Das Bundesamt für Sicherheit in der Informationstechnik erklärt auf seiner Homepage das Social Engineering wie folgt: »Beim Social Engineering werden menschliche Eigenschaften wie Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität ausgenutzt, um Personen geschickt zu manipulieren. Cyberkriminelle verleiten das Opfer auf diese Weise beispielsweise dazu, vertrauliche Informationen preiszugeben, Sicherheitsfunktionen auszuhebeln, Überweisungen zu tätigen oder Schadsoftware auf dem privaten Gerät oder einem Computer im Firmennetzwerk zu installieren.« Persönlich halte ich diese Definition für viel zu kurz gedacht. Ein Hacker, der sich des Social Engineerings bedient, kann dieses Werkzeug der Manipulation für deutlich breiter gefächerte Angriffe nutzen. Das Thema selbst ist wesentlich komplexer, als ich es in diesem Buch darstellen kann.

Ich würde das Social Engineering daher eher als eine angewandte Sozialwissenschaft definieren, welches das Ziel verfolgt, durch Manipulation zwischenmenschliche Beziehungen und Verhaltensweisen Dritter zu beeinflussen und so kriminelle oder unethische Ziele zu erreichen. Diese Ziele können finanzieller, politischer, ideologischer, religiöser oder auch persönlicher Natur sein. Hier verwendet ein Social Engineer oder Hacker verschiedene psychologische Mittel, um die Schwächen eines Menschen bewusst auszunutzen.

Diese angesprochenen psychologischen Mittel können beispielsweise Lügen, Täuschungen, die Illusion oder die Manipulation umfassen. So kann das Social Engineering über die allgemeine Thematik IT-Sicherheit weit hinausgehen. Ich lege großen Wert darauf, das in diesem Buch zu

betonen. Social Engineering ist deutlich mehr als die reine Anwendung manipulativer Mittel, um als Hacker Zugriff zu einem Unternehmen zu erlangen. Die Mittel des Social Engineerings sind so vielfältig, dass ich in diesem Buch nur die Oberfläche der Thematik streifen kann. Sie werden mir daher verzeihen, dass ich die komplexe Psyche eines Menschen und mögliche Angriffspunkte nicht auf ein paar Seiten darstellen kann.

Mein Ziel ist es, mit diesem Buch das bisher selten behandelte Thema des Social Engineerings und seine Bedeutung für unsere Sicherheit zu beleuchten. Daher richtet es sich vor allem an ethisch verantwortungsvoll handelnde Menschen. Das Thema Social Engineering steckt nach wie vor in den Kinderschuhen. Eine kühne Behauptung? Nein, denn wenn wir in die Curricula (Stundenpläne) der meisten zertifizierten Kurse, wie dem CEH (Certified Ethical Hacking) schauen, sehen wir, dass gerade einmal 6 Prozent des Kurses das Thema Social Engineering abdecken. IT-Profis unterschätzen häufig die Möglichkeiten eines Social Engineers. Davon abgesehen, sitzen die meisten von ihnen den lieben langen Tag hinter einem Bildschirm, während menschliche Kontakte eher selten zu ihrem Tagesgeschäft gehören. Man meidet lieber den Kontakt. Zertifizierte Kurse, wie der CEH, enthalten daher häufig kaum Elemente zwischenmenschlicher Kommunikation oder des Social Engineerings im Allgemeinen. Viele professionelle Hacker und sogar Ausbilder sind nach wie vor eher durchschnittliche bis unterdurchschnittliche Social Engineers, während sie in den technischen Bereichen brillieren.

Um dem Ziel dieses Buches gerecht zu werden, gliedere ich es in zwei Teile, um Ihnen die Seiten des Angreifers und der Verteidigung vorzustellen. In Fachkreisen spricht man vom Red Team (den Angreifern) und dem Blue Team (den Verteidigern). Diese beiden Ausdrücke haben sich in den letzten Jahren fest in der Sicherheitsszene etabliert, um die Ziele, Angriffsmöglichkeiten und Szenarios zur Abwehr von Angriffen besser zu beschreiben. Daher ist dieses Buch ähnlich aufgebaut, um Ihnen die Werkzeuge der Angreifer besser aufzeigen zu können und auch, um

Ihnen schlussendlich die Möglichkeiten zu erläutern, wie Sie sich und Ihr Unternehmen bestmöglich vor den Angriffen des Red Teams schützen können.

Die Ziele von Hackern können mannigfaltig sein. In erster Linie stellen wir uns häufig Hacker als bebrillte Nerds vor, die bei Oma im Keller hausen. Doch in Wahrheit gibt es viele verschiedene Arten von Menschen, die sich diverse Fähigkeiten selbst angeeignet haben und diese für ihre Ziele einsetzen. Denken Sie an sogenannte Hacktivisten.

Das Kofferwort, bestehend aus Hacker und Aktivist, beschreibt einen Menschen, der Systeme angreift, um seine politische und ideologische Propaganda zu verbreiten. Das Ziel ist nicht die Tötung von Menschen oder die Verbreitung von Terror und Panik, sondern die Verbreitung von neuen, subjektiv als wahr empfundenen Informationen.

Ein weiteres Beispiel sind Hacker mit wirtschaftlichem Interesse, die beispielsweise mit einem DDoS- (Distributed Denial of Service) Angriff Webseiten für Stunden lahmlegen. Bei diesem Angriff wird im Grunde genommen eine Webseite mit so vielen Anfragen auf einmal überschwemmt, dass der Server unter der Last dieser Anfragen zusammenbricht und die Seite somit vom Netz geht. Für Onlineshops kann dies zu fatalen Umsatzeinbußen führen und wirtschaftliche Schäden entstehen lassen. Kleine Unternehmen können sich von den Schäden und Kosten der Wiederherstellung häufig nicht wieder erholen.

Hacker haben verschiedene Interessen, die nicht nur politisch oder wirtschaftlich getrieben sein müssen. Denken Sie an das weitverbreitete Problem des Stalkings. Ein Hacker könnte in diesem Fall persönliche oder sexuelle Interessen verfolgen. Aber auch die Verbreitung von Propaganda und die Beeinflussung von Menschen, mit der dazu führenden Destabilisierung von Systemen, kann für einen professionellen Black Hat eine willkommene Herausforderung darstellen. Hacker sind häufig Tüftler, die die Herausforderung lieben. Das Problem stachelt sie an. Das ist

mit ein Grund dafür, warum nicht wenige von ihnen einen naturwissenschaftlichen Hintergrund haben. Für die Fachbereiche Mathematik, Physik, Chemie, Informatik und Ingenieurwesen benötigen Sie Neugierde und den unbändigen Willen, Herausforderungen zu lösen. Dies ist eine wesentliche Eigenschaft eines Hackers. Keine Mauer ist zu hoch und kein Problem zu groß. Den Fehler im System zu finden, ist häufig aufregender als eine Schnitzeljagd. Das, was begeistert, ist die Jagd nach einer neuen Möglichkeit. Das ist auch der Grund, warum einige kriminelle und illegal tätige Hacker in der Vergangenheit gefasst werden konnten. Ihr Ego stieg ihnen zu Kopf. Sie wurden Opfer ihrer eigenen menschlichen Fehler.

Doch wie bereits erwähnt, sind nicht alle Hacker kriminell und nicht alle IT-Nerds komische Wesen in Omas Keller. Viele technikbegeisterte Menschen nutzen ihre Fähigkeiten für ethische Zwecke. *Ethical Hacking* ist so fast zum Sport geworden; auch deshalb, weil dieser Sport von den Unternehmen mitunter hervorragend bezahlt wird.

Bei einem Social Engineer ist es ähnlich. Der Social Engineer wird häufig von der Jagd nach dem Ziel angestachelt. Während der Social Engineer sein Ziel vor Augen hat, recherchiert, bastelt und tüftelt er an allen Möglichkeiten, dieses über die Manipulation oder Beeinflussung von Menschen zu erreichen. Das Social Engineering wird häufig als moralisch höchst verwerflich betitelt, da die Identifizierung und Klassifizierung anderer Menschen als reines Werkzeug oft mit den Verhaltensweisen von Soziopathen und Psychopathen verglichen wird.

## MYTHOS SOCIAL ENGINEERING

So haben sich in den letzten Jahren viele verschiedene Mythen um das Thema Social Engineering gebildet. Plötzlich hieß es, dass alle Hacker auch Social Engineers wären und mit einem Laptop und Zugang ins Netz, ähnlich wie Götter, alles erreichen könnten. Auf einmal waren

Hacker professionelle Betrüger, Lügner und Spione und durch fantastische Techniken in der Lage, alles zu bekommen und Menschen dazu zu bringen, alles nur Erdenkliche zu tun. So wechselte das Thema des Social Engineerings häufig seinen Platz hinüber zu den Verschwörungstheoretikern und ihren wilden Theorien und auch zu all jenen, die dieses Thema für ihre eigenen Zwecke missbrauchen wollten. Bitte gestatten Sie mir also, etwas mehr Rationalität und Vernunft in diese Sache zu bringen.

Zunächst einmal ist zu sagen, dass nicht alle professionellen Hacker auch professionelle Social Engineers und andersherum sind. Häufig haben Hacker hervorragende Kenntnisse, was den Angriff auf digitale Systeme betrifft, während sie im Gespräch am Telefon oder im direkten Kontakt mit den Menschen versagen. Auf der anderen Seite gibt es Social Engineers, welche nur die wesentlichsten Grundlagen des Ethical Hackings, der Sprache Python und von Kali Linux verstehen und dennoch in der Lage sind, nahezu jedes Ziel über die Manipulation des Systems Mensch zu erreichen. Verbinden Sie beide Expertisen in einer Person, können Sie entweder jemanden sehr Gefährliches vor sich haben, oder einen unglaublichen Mitarbeiter gewinnen, der sich um die Sicherheit Ihrer Organisation kümmert.

So spielt die philosophische Frage der Moral eine zentrale Rolle. Die Motive der Philosophie und der IT-Sicherheit sind untrennbar miteinander verknüpft. Ich lege großen Wert darauf, dass die in diesem Werk beschriebenen Methoden nur für Bildungsmaßnahmen oder zum Schutz Ihrer Organisation, Ihrer Person oder Ihrer Liebsten genutzt werden sollten. Sie mögen mir daher verzeihen, wenn ich für uns eindeutig abscheuliche Taten und Verhaltensweisen rational und wertfrei darstelle, während ich verspreche, das Thema der Ethik nicht zu kurz kommen zu lassen. Nicht alle Verhaltensweisen sind von Psychopathie oder Soziopathie geprägt. Doch um ehrlich zu sein, sind selbstverständlich einige Formen der Manipulation sozial verwerflich