NICLAS LAHMER

SOCIAL ENGINEERING

DIE NEUEN ANGRIFFSSTRATEGIEN DER HACKER

REDLINE | VERLAG

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.

TEIL I

RED TEAM

»Je intimer die Beziehung,
desto anfälliger sind wir für Manipulation.«

Alexander Fischer[8]

Hacker nutzen Schwachstellen digitaler Systeme aus. Ihr Angriff wird als sogenannter Exploit betitelt. Bei diesem Angriff wird eine Schwachstelle jenes digitalen Systems ausgenutzt, die beispielsweise bei der Entwicklung der Applikation oder des Systems entstanden ist. Beim Social Engineering nutzen wir ebenfalls den Exploit. Das Angriffsziel ist jedoch der Mensch selbst.

Betrachten Sie einen Computer, einen Server oder ein anderes Endgerät als Maschine, so können Sie Parallelen zum Menschen ziehen. Wo der Mensch ein Herz hat, besitzt die Maschine einen Prozessor. Wo der

Mensch ein Gehirn hat, besitzt die Maschine eine Festplatte. Selbstverständlich sind Maschine und Mensch verschieden. Dennoch können beide als System verstanden werden, welche auf unterschiedliche Weise funktionieren. Wir erinnern uns daher an die Aussage der ersten Seite. Jedes System ist angreifbar. Kein System ist sicher.

Das System Mensch hat ebenfalls fest eingebaute Schwachstellen, die uns durch die Natur mitgegeben wurden. Diese Schwachstellen können wir systematisch angreifen, manipulieren und für uns nutzen. Wir starten einen Exploit auf die menschliche Natur. Im Folgenden wollen wir zunächst die verschiedenen Phasen unseres Angriffs besprechen und unterschiedliche Variationen aufzeigen. Ich nenne den Angriff auf das Ziel Mensch daher auch einen Human-Exploit. Bevor wir aber damit beginnen, dieses System anzugreifen, müssen wir unseren Angriff planen. Wir müssen recherchieren, Vorbereitungen treffen und zuallererst unser Ziel definieren. Während Social Engineering häufig eingesetzt wird, um Zugriff zu digitalen Systemen und Daten zu erhalten, können, wie bereits besprochen, die Ziele mannigfaltig sein. Wir werden daher verschiedene Zielsetzungen möglich machen und auf diese konkret eingehen. Fangen wir damit an, die Phasen unserer Vorbereitung zu definieren.

DIE PHASEN DER VORBEREITUNG

Ich kann es nicht oft genug wiederholen: Vorbereitung ist alles! Die Vorbereitung Ihres Angriffs als Mitglied des Red-Teams ist entscheidend. Ein Großteil Ihrer Arbeit als Social Engineer findet in den Phasen der Vorbereitung statt. Diese Phasen müssen von einem erfolgreichen Social Engineer präzise und detailliert durchgearbeitet werden. Verpassen Sie eine Phase, planen Sie nicht diszipliniert genug; machen Sie Fehler in einer der Phasen Ihrer Vorbereitung, gefährden Sie den gesamten Angriff und womöglich auch den Erfolg der Operation oder Ihres Auftrags. Präzision, Sachverstand und Ruhe sind daher unverzichtbare Attribute des erfolgreichen Angreifers. Ob Sie die Eigenschaften eines erfolgreichen Social Engineers besitzen oder nicht, spielt keine Rolle. Jede Fähigkeit können Sie sich aneignen. Selbst wenn Sie eine Rolle nur spielen und einen fiktiven Charakter erstellen, können Sie sich Attribute zuordnen, welche normalerweise nicht zu Ihnen passen. Dazu ein hilfreicher Tipp: Schauspielunterricht kann Ihnen zu Fähigkeiten verhelfen, die viele gute Social Engineers nicht besitzen. Die Erschaffung einer fiktiven Person für den Angriff auf ein Ziel kann Ihnen als Angreifer ein gigantisches Arsenal an Möglichkeiten und Werkzeugen liefern. Vorab sollten Sie jedoch mit der ersten Phase Ihrer Vorbereitung beginnen.

PHASE 1: DEFINIEREN SIE IHR ZIEL

Zunächst einmal sollten wir uns keine Gedanken darüber machen, wen wir angreifen und was wir dabei alles tun könnten. Lassen wir uns nicht von der Faszination des Exploits mitreißen. Als Angreifer müssen wir vor allem rational, beharrlich und diszipliniert vorgehen.

Den meisten Angreifern, die von den Strafverfolgungsbehörden erwischt wurden, waren Fehler unterlaufen. Diese Fehler waren in den meisten Fällen auf die Schwachstellen der eigenen Persönlichkeit zurückzuführen. Hacker wurden übermütig, arrogant und somit unvorsichtig. Ihr Ego spielt eine kolossale Rolle bei jedem Ihrer Angriffe. Das dürfen Sie niemals vergessen. Kein Angriff ist es wert, ins Gefängnis zu gehen und seine Freiheit zu verlieren. Ich kann das gar nicht genug betonen.

So erging es Jonathan James, der auch als der Hacker c0mrade bekannt wurde. James hatte sich in verschiedene Unternehmen gehackt und erhielt somit Zugriff auf Tausende von Mitarbeiterdaten, Passwörtern, Benutzernamen und andere vertrauliche Daten. Darunter waren auch viele Daten von Regierungsmitarbeitern. Im Jahre 2000 wurde James festgenommen und zu sechs Monaten Hausarrest ohne die Nutzung von Computern verurteilt. Er verstieß jedoch gegen seine Bewährungsauflagen und verbrachte letztlich seine Zeit hinter schwedischen Gardinen. In den Jahren nach seinem Gefängnisaufenthalt war James immer wieder als Hacker aktiv. Er konnte es nicht lassen. Bevor er wieder geschnappt werden konnte, beging er Selbstmord. In seinem Abschiedsbrief schrieb er, dass er die Kontrolle verloren habe und nur durch seinen Selbstmord diese zurückerhalten könne. Sein Ego kostete ihn letztendlich das Leben.

Die Themengebiete der Philosophie und des Hackings sind untrennbar miteinander verbunden. Hätte James sich mit seiner eigenen Natur auseinandergesetzt, hätte er gelernt, sich zu mäßigen und seine Gefühle unter Kontrolle zu halten. Wäre er stoisch genug gewesen, im philo-

sophischen Sinne die Wahrheit zu erkennen, hätte James sich womöglich retten können. Wer weiß.

Wenn Sie also Ihr Angriffsziel definieren, beachten Sie, dass dieses Ziel für Sie nicht emotional belegt sein sollte. Viele der Racheangriffe von betrogenen Eheleuten oder Beziehungspartnern gegen ihre ehemaligen Partner gehen böse nach hinten los, da die Betreffenden emotional in der Situation gefangen sind. Die Emotionen Wut, Hass, Zorn und Angst vernebeln Ihre Sinne. Sie können nicht klar denken, nicht strukturiert arbeiten und rational das System aufbrechen. Daher meine Warnung: Wenn Sie emotional in den Angriff verstrickt sind, lassen Sie es! Sie werden unweigerlich Fehler machen und damit Ihre Freiheit oder Gesundheit riskieren. Wo emotionale Bindungen der Ziele ausgenutzt werden, sollte der Angreifer nicht seine eigenen Emotionen in die Gleichung einbringen. So könnten Sie schnell selbst zum Ziel und schlussendlich vernichtet werden.

Wählen Sie Ihr Ziel abhängig von seiner Attraktivität aus. Fragen Sie sich also:

- Was möchte ich erreichen?
- Möchte ich beispielsweise Text, Fotos, Videos, Programme oder Datenbanken abgreifen?
- Möchte ich Zugang zu einem System erhalten und zunächst nicht weiter agieren?
- Ist mein Ziel politischer, ideologischer, religiöser, krimineller, wirtschaftlicher oder privater Natur?
- Woher kommt meine Motivation zum Angriff?
- Welche Gefühle hege ich gegenüber dem Ziel? (KEIN ANGRIFF BEI EMOTIONALER BEFANGENHEIT!)

Bevor Sie damit beginnen, sich Gedanken um die Schwachstellen Ihrer Ziele zu machen, sollten Sie Ihre eigenen Schwachstellen kennen. So

schrieb der chinesische General Sun Tzu: »Wenn du den Feind kennst und dich selbst kennst, brauchst du den Ausgang keines Kampfes fürchten.«[9] Bedenken Sie bei der Auswahl Ihres Angriffsziels, dass die Auswahl des Angreifers genauso wichtig ist wie die der Verteidigung. Ist der Verteidiger zu stark, sollten Sie vorab eine andere Strategie verfolgen. Als Angreifer müssen Sie strategisch vorgehen. Mein Tipp: Das persönliche Studium militärischer Strategen hilft enorm. Lesen Sie von Clausewitz und Sun Tzu. Je breiter Ihr Wissen aufgestellt ist, desto leichter fällt es Ihnen, das Ziel richtig zu definieren. Dabei kann es häufig hilfreich sein, Ihr Ziel nicht direkt anzugreifen, sondern kleinere Ziele anzugehen, welche mit dem Hauptziel verbunden sind.

Während der napoleonischen Kriege zwischen 1807 und 1814 kämpften die Spanier gegen Frankreich. Die Spanier waren den Franzosen jedoch beim Kampf um die iberische Halbinsel unterlegen. Statt den Feind auf dem offenen Feld anzugreifen, attackierten die Spanier kleine Ziele der Franzosen. Versorgungsrouten, kleine Stoßtruppen und andere Ziele wurden durch spanische Freiheitskämpfer im Rahmen eines Guerillakrieges eingenommen oder vernichtet. Carl von Clausewitz definiert dies als den kleinen Krieg.

Nutzen Sie lieber kleinere Angriffsziele, bevor Sie sich an einen Walfisch wagen. Wenn Sie Ihr Ziel zermürben wollen, sind kleinere Angriffe meist die bessere Strategie. Vor allem, wenn Ihr Ziel mächtig und groß erscheint, können Sie so leichter Erfolge verzeichnen und wichtige Punkte gewinnen.

PHASE 2: BETREIBEN SIE RECHERCHE

Wenn Sie Ihr Ziel definiert haben, beginnt die wichtigste Phase Ihres Angriffs. Während der Recherche sind alle Informationen, die Sie erhalten können, von größter Relevanz. Bevor Sie die Daten, die Sie er-

halten, clustern und sortieren, müssen diese erst einmal beschafft werden. Die Daten über Ihr Opfer können Dokumente, Fotos oder Videos sein. Sammeln Sie gnadenlos alle Informationen, die es gibt. Sammeln Sie Social-Media-Profile, Verbindungen zu Dritten, Veröffentlichungen, Posts und Zeitungsartikel. Definieren Sie Tagespläne. Wann fährt Ihr Opfer zur Arbeit? Wann kommt derjenige heim? Wie oft ist er auf Geschäftsreise? Wann fährt er in den Urlaub? Geht es am Wochenende raus in die Berge, an den Strand oder in ein Ferienhaus? Wie und wo lebt das Angriffsziel? Verheiratet? Ledig? Kinder? Geburtstage, Kennenlerntage, Tag der Eheschließung? Glückliche Ehe oder Probleme inklusive Eheberatung? Auf welche Schulen gehen die Kinder? Haben die Kinder Social-Media-Profile? Mit wem treffen sich die Kinder regelmäßig? Gibt es Zerwürfnisse zwischen Vater, Mutter und Kindern wegen Noten oder dem falschen Umgang? Raucht jemand im Haushalt? Gibt es Abhängigkeiten? Drogen, Sex, Alkohol, Partys, Spielsucht? Wo geht man Einkaufen? Welche Kleidung trägt man? Welche Autos fährt man? Gibt es ein Motorrad, ein Boot oder ein Flugzeug? Welchen Hobbys geht man nach? Fußball, Tennis, Golf, Schießsport oder gar ein bestimmter Kampfsport? Ist das Ziel Jäger oder Sportschütze und hat Zugriff auf Schusswaffen? Wohin fährt man in den Urlaub? Fliegen oder fahren? Sonne, Meer und Süden oder eher Norden, Kälte und Schnee? Exotische Ziele oder Standardziele in Spanien und Italien? Wie viele Endgeräte besitzt der Haushalt? Smartphones, Laptops, Tablets, Desktop PCs oder gar ein Home-Server? Welchen Anbieter hat man für das Netzwerk gewählt? Wie ist das Netzwerk geschützt? Welche Pakete kommen regelmäßig an? Amazon, Zalando oder bestimmte Bekleidungsmarken?

Die Liste der Fragen kann seitenweise so weitergehen. Häufig stellt sich die Frage, wie wir an diese Informationen und Daten herankommen. Obwohl es neben der Observation und Internetrecherche viele Wege gibt, ist eine interessante dritte Möglichkeit das Durchsuchen des Hausmülls. Mülleimer stehen häufig ungeschützt und frei zugänglich

auf dem Gelände. Vor allem bei Wohnkomplexen sind die Mülltonnen meist zusammen an einem Ort gelagert und für die Müllabfuhr erreichbar. Es ist in den meisten Ländern sogar legal, diese Orte aufzusuchen und im Müll zu stöbern. Verständlicherweise ist das keine besonders angenehme Arbeit, doch der Müll kann uns eine ganze Menge Informationen über unser Opfer liefern. Im Müll finden wir Rechnungen, Belege, Kontoauszüge, Briefe und andere Post. Die meisten Menschen machen sich nicht die Mühe, diese Post gründlich zu vernichten. Die wenigsten Privathaushalte nutzen einen Schredder. Selbst bei vielen Firmen ist man da sehr nachlässig. Im Müll finden wir deshalb einen Haufen nützlicher Informationen über unser Ziel.

Sobald wir diese Informationen gesammelt haben, werten wir sie aus. Clustern und strukturieren Sie alle gesammelten Daten. Erstellen Sie Mindmaps, Diagramme, Beziehungscharts und legen Sie Akten zu den verschiedenen Personen an, während Sie das Netzwerk der Personen offenlegen. Dies ist heutzutage besonders einfach, da die allermeisten Menschen naiv all ihre Daten ins Netz stellen. Sie veröffentlichen Kinderbilder, Urlaubsfotos, Fotos vom neuen Auto, Videos von der letzten Gartenparty, tragen Kleidung, welche verschiedene Interessen widerspiegelt und veröffentlichen wahllos alles, was mit ihrer Persönlichkeit in Verbindung steht. Doch Fotos liefern uns nicht nur Informationen über den Hintergrund der Person, sondern auch über die Örtlichkeiten. Stellen Sie sich das so vor: Hinter jedem Foto liegen Daten. Diese sogenannten Metadaten enthalten nicht nur Informationen zum Datum, sondern auch zur Örtlichkeit des gemachten Fotos. Geolokationsdaten sind in den Metadaten enthalten und können praktisch von jedem Menschen ausgelesen werden. Mithilfe von Google Maps können Sie den Standort jedes Fotos triangulieren und somit Routenprofile erstellen. Plötzlich wissen Sie, wo und wann Ihr Angriffsziel dort war und mit wem.