Parmy Olson

Inside Anonymous

Aus dem Innenleben des globalen Cyber-Aufstands

Übersetzung aus dem Englischen von Dagmar Mallett, Sigrid Schmid, Friedrich Pflüger, Enrico Heinemann und Ursula Held

REDLINE | VERLAG

Kapitel 1: Der Raid

Am 6. Februar 2011 ließen sich in ganz Amerika Millionen Menschen auf ihre Sofas fallen, rissen Chipstüten auf und gossen Bier in Plastikbecher; alles zur Vorbereitung auf das größte Sportereignis des Jahres. An diesem Sonntag fand das Super-Bowl-Endspiel zwischen den Footballmannschaften der Green Bay Packers und der Pittsburgh Steelers statt. Während die Packers gewannen, musste Aaron Barr, Manager einer Internetsicherheitsfirma, hilflos zusehen, wie sieben Menschen, denen er nie begegnet war, sein Leben auf den Kopf stellten. Super Bowl Sunday war der Tag, an dem er mit Anonymous konfrontiert wurde.

Nach diesem Wochenende hatte das Wort *anonymous* eine neue Bedeutung gewonnen. Es stand nicht mehr nur für »anonym«, sondern bezeichnete jetzt – mit großem A – auch eine ungreifbare, finstere Gruppe von Hackern, die mit allen Mitteln Gegner des freien Informationsflusses angriffen, darunter auch Menschen wie Barr. Dieser, verheiratet und Vater von Zwillingen, hatte den Fehler gemacht, herausfinden zu wollen, wer sich tatsächlich hinter Anonymous verbarg.

Der Schlag erfolgte schon zur Mittagszeit, sechs Stunden vor dem Anstoß im Super Bowl. Barr saß in Jeans und T-Shirt auf dem Wohnzimmersofa in seinem Washingtoner Vororthaus, als er bemerkte, dass das iPhone in seiner Tasche sich seit einer halben Stunde nicht mehr gemeldet hatte. Normalerweise kam etwa alle Viertelstunde eine E-Mail. Als er sein iPhone nahm und die E-Mails aufrufen wollte, erschien ein dunkelblaues Fenster mit drei Worten, die sein Leben verändern sollten: *Cannot Get Mail* – kein E-Mail-Empfang. Das E-Mail-Programm fragte nach seinem Passwort, und Barr tippte es gehorsam in die Account-Einstellungen des iPhones: »kibafo33«. Es half nichts, er bekam immer noch keine E-Mails.

Ratlos starrte er das Display an. Langsam wurde ihm klar, was diese Fehlermeldung bedeutete, und er bekam Angst. Vor einigen Stunden hatte er mit einem Hacker namens Topiary von Anonymous gechattet und seit-

dem geglaubt, dass er aus dem Schneider sei. Jetzt sah er, dass jemand seinen Account bei HBGary Federal geknackt, damit Zugang zu Zehntausenden Firmen-E-Mails gewonnen und ihn dann ausgesperrt hatte. Das hieß, dass irgendjemand irgendwo vertrauliche Vereinbarungen und Dokumente eingesehen hatte, die eine internationale Bank, eine angesehene Behörde der US-Regierung und auch seine eigene Firma kompromittieren konnten.

Immer mehr Geheimdokumente und nicht für die Öffentlichkeit bestimmte Nachrichten fielen ihm ein; nach jeder folgte eine Welle der Übelkeit. Barr stürmte die Treppe zu seinem Arbeitszimmer hinauf und setzte sich an den Laptop. Er wollte sich in seinen Facebook-Account einloggen, um mit einem ihm bekannten Hacker zu sprechen, der ihm vielleicht helfen würde. Aber dieses Netzwerk, in dem er mehrere hundert Freunde hatte, war blockiert. Er versuchte es mit Twitter, wo er einige Hundert Followers hatte. Nichts. Dasselbe bei Yahoo. Fast alle seine Internet-Accounts waren gesperrt, sogar der für World of Warcraft, ein Online-Rollenspiel. Barr verfluchte sich im Stillen selbst dafür, dass er überall dasselbe Passwort verwendete. Auf seinem WLAN-Router blinkten wild die Kontrolllichter – er wurde mit Anfragen überschwemmt, mit denen die Angreifer sich weiter in sein Heimnetzwerk vorarbeiten wollten.

Er zog den Stecker. Die blinkenden Lichter erloschen.

Aaron Barr war früher beim Militär gewesen. Der breitschultrige Mann mit den pechschwarzen Haaren und dichten Augenbrauen, die auf entfernte südeuropäische Vorfahren schließen ließen, hatte nach zwei Semestern das Collegestudium abgebrochen und sich bei der US-Marine gemeldet. Ziemlich schnell wurde er zum SIGINT Officer, also zum Abhörexperten im Geheimdienst, und zwar als Analytiker, ein eher seltenes Fachgebiet. Es folgten zahlreiche Auslandsposten: vier Jahre in Japan, drei in Spanien, Aufträge in ganz Europa, von der Ukraine über Portugal bis nach Italien. Er diente auf Landungsbooten und geriet im Kosovo unter Feuer. Dieses Erlebnis machte ihm bewusst, wie sehr der Krieg Soldaten gegenüber dem Wert des menschlichen Lebens abstumpfte.

Nach zwölf Jahren bei der Marine suchte er sich einen zivilen Job bei Northrop Grumman, einem Konzern mit vielen Rüstungsaufträgen. Er gründete eine Familie, versteckte seine Seemannstätowierungen und

wurde zum Geschäftsmann. Im November 2009 fragte ihn dann ein Sicherheitsberater namens Greg Hoglund, ob er interessiert sei, sich an einer Firmengründung zu beteiligen. Hoglund betrieb bereits eine Computersicherheitsfirma namens HBGary Inc. und wollte Barr mit seinem militärischen Hintergrund und seiner kryptografischen Erfahrung für eine Schwesterfirma gewinnen, die Dienstleistungen für Behörden der US-Regierung anbieten sollte. Dieses Unternehmen sollte HBGary Federal heißen, und HBGary Inc. würde 10 Prozent der Anteile halten. Barr ergriff ohne Zögern die Chance, sich selbstständig zu machen – wenn er von zu Hause aus arbeitete, hatte er viel mehr Zeit für seine Frau und die beiden Kinder.

Zunächst genoss er den neuen Job. Im Dezember 2009 blieb er drei Nächte hintereinander auf, weil er so viele Ideen für neue Projekte hatte. Manchmal schrieb er Hoglund um halb zwei Uhr morgens, um ihm seine Einfälle mitzuteilen. Fast ein Jahr später machte er mit all diesen Ideen aber immer noch kein Geld und brauchte unbedingt Aufträge. Inzwischen hielt er die winzige Firma mit ihren drei Angestellten durch »Social Media Training« für Manager über Wasser. Diese Seminare brachten jeweils 25.000 Dollar ein. Man lernte dort nicht, wie man seine Facebook-Freundschaften pflegte, sondern wie man die sozialen Netzwerke wie Facebook, LinkedIn oder Twitter zur Informationsgewinnung nutzte – deutlicher gesagt, wie man Menschen ausspionierte.

Im Oktober 2010 kam dann endlich die Erlösung. Barr bekam Kontakt zu Hunton & Williams, einer Anwaltskanzlei, deren Mandanten – darunter auch die U. S. Chamber of Commerce und die Bank of America – Probleme mit bestimmten Gegenspielern hatten. WikiLeaks hatte zum Beispiel neulich angedeutet, es säße auf einem Berg vertraulicher Daten der Bank of America. Barr und zwei andere Sicherheitsberatungsfirmen führten PowerPoint-Präsentationen vor, in denen unter anderem auch Verleumdungskampagnen gegen Journalisten vorgeschlagen wurden, die WikiLeaks und Internetangriffe auf die WikiLeaks-Webseite unterstützten. Er grub seine fiktiven Facebook-Profile aus und demonstrierte, wie man die Gegner damit ausspionieren konnte, indem er Freundschaftsanfragen an die Anwälte bei Hunton & Williams schickte und damit an Informationen über ihr Privatleben kam. Die Kanzlei wirkte durchaus interessiert, aber im Januar 2011 floss immer noch kein Geld, und HBGary Federal brauchte immer noch dringend welches.

Dann hatte Barr eine Idee. In San Francisco würde demnächst eine Konferenz von Sicherheitsberatern namens B-Sides stattfinden. Wenn er dort einen Vortrag darüber hielt, wie seine Schnüffelei in sozialen Netzwerken ihm Informationen über einen geheimnisvollen Unbekannten enthüllt hatte, konnte er sich in seinem Fachgebiet profilieren und würde vielleicht endlich den ersehnten Auftrag bekommen.

Barr konnte sich kein besseres Ziel als Anonymous vorstellen. Ungefähr einen Monat zuvor, im Dezember 2010, waren die Nachrichten voll von Berichten über eine große und geheimnisvolle Hackergruppe gewesen, welche die Webseiten von MasterCard, PayPal und Visa angegriffen hatte, und zwar als Vergeltung dafür, dass diese Firmen sich weigerten, Spenden an WikiLeaks weiterzuleiten. WikiLeaks hatte damals gerade mehrere Zehntausend geheime diplomatische Telegramme der USA veröffentlicht, und der Gründer und Leiter Julian Assange war in Großbritannien festgenommen worden, formell wegen eines Sexualvergehens.

»Hacker« war ein sehr vage definiertes Wort. Dahinter konnte ein begeisterter Programmierer oder ein Internetkrimineller stecken. Die Mitglieder von Anonymous, die Anons, wurden oft Hacktivisten genannt – Hacker, die als Aktivisten eine Botschaft verbreiten wollten. Soweit man wusste, traten sie für absolut freien Informationsfluss ein, und wer anderer Meinung war, musste damit rechnen, dass seine Webseite angegriffen wurde. Angeblich hatten sie weder eine Hierarchie noch eine Leitung. Sie behaupteten, keine Gruppe zu sein, sondern »alles und nichts«. Die zutreffendste Kategorisierung war vielleicht »Markenname« oder »Kollektiv«. Die wenigen Regeln, die sie hatten, erinnerten an den Film *Fight Club:* Sprich nicht über Anonymous, enthülle nie deine wahre Identität und greif nicht die Medien an, denn die brauchen wir, um unsere Botschaften zu verbreiten. Die Anonymität verführte natürlich auch zu gelegentlichen Gesetzesverstößen – Einbrüche in Server, Diebstahl von Kundendaten, Blockade und Defacement einer Webseite. Das konnte zehn Jahre Gefängnis einbringen, aber den Anons schien es egal zu sein. Die Gruppe versprach Stärke und Schutz, und überall in Blogs, auf gehackten Webseiten und wo es nur ging, las man ihr ominöses Motto:

Wir sind Anonymous
Wir sind Legion
Wir vergeben nicht

Wir vergessen nicht
Rechne mit uns

Die digitalen Flyer und Nachrichten der Gruppe zeigten das Logo eines kopflosen Anzugträgers in einem dem UN-Wappen nachempfundenen Lorbeerkranz. Die Figur beruhte angeblich auf einem berühmten Gemälde des Surrealisten René Magritte: ein kopfloser Mann mit einem Apfel auf dem Hut. Oft sah man auch die höhnisch grinsende Guy-Fawkes-Maske, die durch den Film *V wie Vendetta* bekannt geworden war, in dem sie einer gesichtslosen Menge von Rebellen als Symbol diente. Niemand wusste, wie viele Angehörige Anonymous hatte, aber es waren nicht nur ein paar Dutzend oder wenige Hundert. Im Dezember 2010 hatten sich Tausende User aus aller Welt in den Hauptchatroom eingeloggt, um an den Angriffen auf PayPal teilzunehmen. Blogs, die sich mit Anonymous befassten, und neue Seiten wie AnonNews.org hatten Tausende von Besuchern. Jeder, der mit Internetsicherheit zu tun hatte, redete über Anonymous, aber niemand schien zu wissen, wer diese Leute eigentlich waren.

Barr faszinierte das. Die ganze Welt hatte dem Anwachsen dieser geheimnisvollen Gruppe zugesehen, und es hatte Dutzende Razzien und Festnahmen gegeben, sowohl in den USA wie in Europa – aber niemand war verurteilt worden, und die Anführer der Gruppe blieben im Dunkeln. Barr glaubte, er könne es besser als das Federal Bureau of Investigation – vielleicht konnte er dem FBI ja sogar helfen –, weil er sich in den sozialen Netzwerken auskannte. Es mit Anonymous aufzunehmen war gefährlich, aber selbst wenn er ins Fadenkreuz des Kollektivs geriete, konnte das, so glaubte er, höchstens bedeuten, dass es die Webseite von HBGary Federal ein paar Stunden lang lahmlegte, vielleicht auch ein paar Tage, aber nichts Schlimmeres.

Zunächst trieb er sich in den Chatrooms herum, wo sich die Anonymous-Unterstützer trafen, das heißt, er hörte nur zu, ohne selbst zu posten. Darauf wählte er sich einen Spitznamen – zuerst AnonCog, dann CogAnon – und schaltete sich ein. Er passte sich dem Slang der Gruppe an und gab vor, ein begeisterter Neuling zu sein, der gerne die eine oder andere Firmenwebseite angreifen würde. Während der Chats notierte er sich laufend die Spitznamen der anderen im Chatroom. Es waren Hunderte, aber er verfolgte nur die häufigen Gäste und jene mit den meisten Antworten. Wenn solche Leute sich ausloggten, schrieb Barr sich den genauen Zeitpunkt

auf und wechselte zu Facebook. Barr arbeitete dort mit mehreren fiktiven Identitäten; diese gefälschten Accounts hatten Dutzende echter Freunde, die offen ihre Unterstützung für Anonymous bekundeten. Wenn einer dieser Freunde auf Facebook aktiv wurde, kurz nachdem ein bestimmter Spitzname den Anonymous-Chatroom verlassen hatte, verbuchte Barr das als Identifikation des einen mit dem anderen.

Ende Januar hatte Barr eine zwanzigseitige Aufstellung von Namen mit Beschreibungen und Kontaktinformationen angeblicher Unterstützer und Anführer von Anonymous zusammengestellt. Am 22. Januar 2011 schickte er Hoglund und der Kopräsidentin von HBGary Inc., Penny Leavy (Hoglunds Ehefrau), sowie seinem eigenen Stellvertreter Ted Vera eine E-Mail über den angekündigten Vortrag zu Anonymous auf der B-Sides-Tagung. Der große Nutzeffekt sollte in der Aufmerksamkeit der Medien liegen. Außerdem wollte er in der Rolle einer seiner fiktiven Netzidentitäten einigen Anonymous-Leuten von den Recherchen eines »sogenannten Cyber-Security-Experten« namens Aaron Barr erzählen. »Das wird die Anonymous-Chatkanäle ganz schön aufscheuchen, und die Presse liest die ja mit«, schrieb Barr an Hoglund und Leavy. Also würde es noch mehr Medienaufmerksamkeit geben. »Allerdings«, fügte er hinzu, »werden wir dadurch auch selbst zum Angriffsziel. Was meint ihr dazu?«

Hoglund antwortete kurz: »Ich möchte nicht unbedingt einen DDoS-Angriff abkriegen, wenn das passiert, was machen wir dann? Können wir den auch irgendwie ausnutzen?« DDoS bedeutet Distributed Denial of Service; bei einem DDoS-Angriff wurde eine Webseite mit so vielen Anfragen und Daten von möglichst vielen Rechnern überflutet, dass sie zusammenbrach und offline ging. Anonymous griff meistens auf diese Weise an. Man könnte das etwa mit einem Faustschlag ins Auge vergleichen – es gab einen hässlichen blauen Fleck und tat weh, brachte einen aber nicht um.

Barr hielt es für vorteilhaft, wenn er sich schon vor dem Vortrag direkt an die Presse wandte. Er bot Joseph Menn, einem Reporter der *Financial Times* aus San Francisco, ein Interview an, in dem er schildern wollte, wie seine Daten zu weiteren Festnahmen »wichtiger Leute« bei Anonymous führen konnten. Er gab Menn eine kurze Zusammenfassung: Von den mehreren Hundert Teilnehmern an Internetattacken von Anonymous waren nur etwa 30 dauerhaft aktiv, und nur etwa zehn zentrale Figuren trafen den Großteil der Entscheidungen. Barrs Erkenntnisse und die Geschichte

seiner Untersuchung zeigten zum ersten Mal, dass Anonymous sehr wohl eine Hierarchie hatte und nicht so »anonym« war, wie es glaubte. Die Zeitung brachte am Freitag, dem 4. Februar, die Geschichte unter der Überschrift »Internetaktivisten müssen mit Festnahmen rechnen« und berief sich auf Barr.

Der war ein bisschen stolz darauf, es in die Zeitung geschafft zu haben, und schrieb Hoglund und Leavy eine E-Mail mit dem Betreff »Story kommt jetzt wirklich in Gang«. »Wir sollten das auf unserer Eingangsseite posten und ein paar Tweets rausschicken«, antwortete Hoglund. »Etwa: ›HBGary setzt neue Maßstäbe mit detektivischer Höchstleistung‹.«

Im Laufe des Freitags hatten auch Beamte der Internetkriminalitätsabteilung des FBI den Artikel gelesen und bei Barr angefragt, ob er bereit sei, seine Informationen an sie weiterzugeben. Er verabredete ein Treffen am Montag nach dem Super-Bowl-Endspiel. Ungefähr zur selben Zeit hatte auch eine kleine Gruppe von Anonymous-Hackern die Zeitung gelesen.

Es waren drei; sie kamen aus ganz verschiedenen Weltgegenden, und sie waren in einen Online-Chatroom eingeladen worden. Ihre Spitznamen lauteten Topiary, Sabu und Kayla, und mindestens zwei von ihnen, Sabu und Topiary, trafen sich zum ersten Mal. Die Person, die sie eingeladen hatte, führte den Spitznamen Tflow und war ebenfalls eingeloggt. Keiner kannte den wirklichen Namen, das Alter, das Geschlecht oder den Aufenthaltsort der anderen. Zwei von ihnen, Topiary und Sabu, benutzten ihre Spitznamen erst seit knapp einem Monat in öffentlichen Chatrooms. Was sie voneinander wussten, war nur ein bisschen Klatsch und Tratsch und dass sie alle an Anonymous glaubten. Das war die Gesprächsgrundlage.

Der Chatroom war abgeschlossen, das heißt, man kam nur auf Einladung hinein. Die Unterhaltung war zuerst ein bisschen steif, aber nach einigen Minuten war alles ganz ungezwungen, und es zeigten sich Persönlichkeitszüge. Sabu war selbstsicher und dominant und benutzte Slangausdrücke wie »yo« und »my brother«. Die anderen wussten es natürlich nicht, aber er war in New York geboren und aufgewachsen und stammte aus einer puerto-ricanischen Familie. Hacken hatte er als Teenager gelernt, als er zunächst den Call-by-Call-Internetzugang des Familiencomputers manipulierte, um umsonst ins Netz zu kommen. Ende der neunziger Jahre eignete er sich in Hackerforen weitere Tricks an. Etwa 2001 war der Spitzname Sa-

bu dann aus dem Netz verschwunden und erst jetzt, fast ein Jahrzehnt später, wieder aufgetaucht. Sabu war das Schwergewicht und der Veteran in der Gruppe.

Kayla gab sich kindlich und freundlich, aber dahinter verbarg sich messerscharfe Intelligenz. Sie war angeblich weiblich; fragte man sie nach ihrem Alter, behauptete sie, sechzehn zu sein. Das hielten viele für eine Lüge, denn bei Anonymous gab es zwar viele jugendliche Hacker und auch viele weibliche Unterstützerinnen, aber kaum weibliche Hacker. Die Lügengeschichte, wenn es eine war, war allerdings sehr detailreich. Kayla war gesprächig und gab viele Einzelheiten aus ihrem Privatleben preis: Sie arbeitete in einem Kosmetiksalon, verdiente sich mit Babysitten ein bisschen Geld dazu und machte gerne Ferien in Spanien. Sie behauptete sogar, Kayla sei ihr echter Vorname, den sie aus Trotz beibehalte, für den Fall, dass jemand sie identifizieren wolle. Was die Sicherheit ihres Rechners anging, war sie allerdings geradezu paranoid. Sie tippte nie ihren wirklichen Namen in ihr Netbook ein, falls jemand die Tastatureingaben mitlas, hatte keine eigene Festplatte und betrieb ihren Rechner mithilfe einer winzigen MicroSD-Speicherkarte, die sie notfalls hinunterschlucken konnte, falls die Polizei kam. Es hieß, eines Tages habe sie ihre Webcam mit einem Messer außer Gefecht gesetzt, damit niemand sich in ihren PC einhacken und sie ohne ihr Wissen filmen konnte.

Topiary hatte in der Gruppe am wenigsten Ahnung vom Hacken, aber dafür ein anderes Talent, das diesen Mangel ausglich: seinen Esprit. Topiary war vorlaut und voller Ideen; außerdem besaß er eine große Überredungsgabe und einen Sinn für Öffentlichkeitswirksamkeit. Beides setzte er ein, um sich langsam durch die Hierarchie der geheimen Planungschatrooms von Anonymous emporzuarbeiten. Andere durften kaum an der Tür horchen; Topiary wurde immer sofort eingeladen. Er genoss so großes Vertrauen, dass die Netzwerkbetreiber ihn mit der Abfassung der offiziellen Anonymous-Presseerklärungen zu den Angriffen auf PayPal und MasterCard beauftragten.

Sein Spitzname war das Ergebnis einer Laune. Er mochte den Low-Budget-Zeitreisefilm *Primer,* und als er hörte, dass der Regisseur Shane Carruth an einem Nachfolgeprojekt namens *A Topiary* arbeitete, gefiel ihm einfach das Wort so gut, dass er es als Spitznamen übernahm, ohne zu wissen, dass ein Topiarium eigentlich ein Ziergarten mit in Form geschnittenen Büschen und Sträuchern ist.

Tflow, der sie alle zusammengebracht hatte, war ein erfahrener Programmierer und ziemlich schweigsam; er hielt sich an die Anonymous-Regel, nicht über sich selbst zu sprechen. Er gehörte seit mindestens vier Monaten dazu, lange genug, um die Gruppenkultur und die wichtigen Leute zu kennen. Die Verständigungswege und die Nebendarsteller in dieser Szene kannte er besser als die meisten.

Er war es auch, der aufs Geschäft zu sprechen kam. Jemand musste sich Aaron Barrs und seiner »Recherchen« annehmen. Barr hatte behauptet, Anonymous habe Chefs, und das stimmte nicht. Das wiederum hieß, dass seine Rechercheergebnisse vermutlich unzutreffend waren. Dann war da noch das Zitat aus der *Financial Times,* wo es hieß, Barr habe »Informationen über die Spitzenleute gesammelt, darunter auch viele Klarnamen; diese Leute könnten festgenommen werden, wenn die Polizei die Daten bekommt«.

Das war ein neues Problem: Wenn Barr die richtigen Namen hatte, bedeutete das Ärger für einige Anons. Die Gruppe fing an, Pläne zu schmieden. Zuerst wollten sie den Server, auf dem die Webseite von HBGary Federal lief, auf wunde Punkte in seinem Quellcode absuchen. Wenn sie Glück hatten, fanden sie eine Lücke, durch die sie eindringen konnten. Dann würden sie Barrs Homepage übernehmen und den Inhalt durch ein großes Anonymous-Logo und die schriftliche Warnung ersetzen, das Kollektiv besser in Ruhe zu lassen.

Am Nachmittag googelte jemand den Namen »Aaron Barr« und stieß auf die offizielle Fotografie für seine Firma. Sie zeigte einen Anzugträger mit zurückgekämmtem Haar, der ernst in die Kamera blickte. Die Gruppe lachte angesichts des Fotos. Er sah so ... unbedarft aus, wie eine leichte Beute. Sabu suchte HBGaryFederal.com nach einer Schwachstelle ab. Wie sich herausstellte, benutzte Barrs Webauftritt ein fremdentwickeltes Publikationssystem, das einen schweren Fehler aufwies. Hauptgewinn!

HBGary Federal zeigte zwar anderen Firmen, wie man sich vor Internetangriffen schützte, war aber selbst anfällig für eine einfache Form der Attacke namens SQL-Injection, die auf Datenbasen zielte. Datenbasen sind eine der vielen Schlüsseltechnologien, auf denen das Internet beruht. Man kann darin Passwörter, Firmen-E-Mails und viele weitere Arten von Daten speichern. Um die Informationen in Datenbasen zu verwalten, bedient

man sich oft der sogenannten SQL (Structured Query Language, im Englischen wird die Abkürzung gewöhnlich »sequel« ausgesprochen). SQL-Injection bedeutete das »Injizieren« von SQL-Befehlen in den Server, auf dem die Seite lief, um verborgene Informationen herauszuholen, womit die Programmiersprache praktisch gegen sich selbst eingesetzt wurde. Der Server las die eingegebenen Zeichen nicht als Text, sondern als auszuführende Befehle. Manchmal erreichte man das schon, indem man seine Befehle einfach in das Suchfenster einer Homepage eingab. Es kam nur darauf an, das richtige Suchfenster zu finden, das ungenügend abgesichert war.

Der betroffenen Firma konnte ein solcher Angriff sehr schaden. Wenn DDoS ein bloßer Faustschlag war, dann glich eine SQL-Injection der Entfernung lebenswichtiger Organe im Schlaf. Die Programmiersprache selbst, die aus Symbolen und Codewörtern wie SELECT, NULL und UNION bestand, war Menschen wie Topiary völlig unverständlich, für Sabu und Kayla aber wie eine zweite Muttersprache.

Nachdem die Hacker sich einmal Zutritt verschafft hatten, forschten sie nach Namen und Passwörtern von Administratoren des Servers wie Barr und Hoglund. Wieder ein Treffer: Sie fanden eine Liste mit Usernamen und Passwörtern von HBGary-Mitarbeitern. Aber es gab eine Schwierigkeit: Die Passwörter waren »zerhackt«, also verschlüsselt, und zwar mit einer Standardmethode namens MD5. Wenn alle Administratorenpasswörter lang und kompliziert waren, konnten sie womöglich nicht geknackt werden, und die Hacker wären um ihren Spaß gebracht.

Sabu suchte sich drei zerhackte Passwörter aus, lange Reihen von Zufallszahlen und -buchstaben, die den Passwörtern von Aaron Barr, Ted Vera und einem anderen Manager namens Phil Wallisch entsprachen. Er erwartete, dass sie besonders gut verschlüsselt waren, und zeigte sich nicht überrascht, als die anderen im Team, denen er sie weitergab, daran scheiterten. Als letzte Möglichkeit stellte er sie in ein beliebtes Internetforum für Passwortknacker ein – Hashkiller.com. Innerhalb weniger Stunden hatten zufällig eingeloggte anonyme Freiwillige alle drei geknackt. Das Ergebnis für eines davon sah so aus:

4036d5fe575fb46f48ffcd5d7aeeb5af:kibafo33

Hinter der verschlüsselten Zeichenfolge erschien Aaron Barrs Passwort. Als das Team versuchte, mit kibafo33 die auf GoogleApps gespeicherten Firmen-E-Mails von HBGary Federal abzurufen, gelang das problemlos. Die Hacker wollten ihren Augen nicht trauen. Am Freitagabend konnten sie schon live mitverfolgen, wie der ahnungslose Barr fröhliche E-Mails mit seinen Kollegen über den Artikel in der *Financial Times* wechselte.

Nur mal so, weil es einen Versuch wert war, probierten sie kibafo33 auch bei Barrs anderen Accounts aus. Unglaublicherweise hatte Barr, immerhin ein Internetsicherheitsexperte, der es mit Anonymous aufnehmen wollte, bei fast allen dasselbe leicht zu entschlüsselnde Passwort verwendet – Twitter, Yahoo, Flickr, Facebook, sogar bei World of Warcraft. Das hieß, dass sich jetzt die Gelegenheit für reines, ungehindertes »Lulz« bot.

Lulz ist eine Variante der Abkürzung lol – laughing out loud, lautes Auflachen –, die seit Jahren zur Sprache der Internetforen gehört. Lulz ist neuer und bezeichnet im Wesentlichen Schadenfreude. Telefonstreiche beim FBI waren lol. Das FBI anzurufen und ein Überfallkommando zu Aaron Barr nach Hause zu schicken war Lulz.

Die Gruppe beschloss, an diesem Tag noch nicht gegen Barr loszuschlagen, auch nicht am nächsten. Sie wollten sich das Wochenende über Zeit nehmen und alle E-Mails herunterladen, die er während seiner Tätigkeit für HBGary Federal je gesendet oder empfangen hatte. Beim Lesen merkten sie allerdings, dass es doch ein bisschen dringender war: Schon am Montag hatte Barr einen Termin beim FBI. Als das Team alles mitgenommen hatte, was es finden konnte, wurde entschieden, dass der Anstoß des Super-Bowl-Spiels am Sonntag das Signal zum Losschlagen sein sollte. Das war in 60 Stunden.

Es war ein ganz normaler Samstag für Barr. Er war zu Hause bei seiner Familie, genoss seine Freizeit und sendete und empfing beim Frühstück einige E-Mails über sein iPhone. Er hatte keine Ahnung, dass ein sieben Mann starkes Anonymous-Team gerade dabei war, seine E-Mails zu durchsuchen, und dass die Hacker ziemlich aufgeregt über das waren, was sie soeben gefunden hatten: Barrs Anonymous-Recherchen. Es handelte sich um ein PDF-Dokument, das mit einer ordentlichen, kurzen Erläuterung begann, worum es sich bei Anonymous handelte. Dann folgten Listen von Webseiten, eine Zeittafel kürzlicher Internetangriffe und jede Menge Spitzna-

men, denen Klarnamen und Adressen zugeordnet waren. Die Namen Sabu, Topiary und Kayla tauchten nicht auf. Am Ende lief das Dokument in hastige Notizen wie »Mmxanon – states ... ghetto« aus; es wirkte unfertig. Langsam wurde den Hackern klar, wie Barr mithilfe von Facebook versucht hatte, Online-Spitznamen und echte Namen miteinander zu verknüpfen. Er hatte offensichtlich keine Ahnung, was er damit anrichten konnte, nämlich völlig Unschuldige anzuschwärzen.

In der Zwischenzeit hatte Tflow Barrs E-Mails auf seinen Server heruntergeladen und etwa fünfzehn Stunden gewartet, bis sie zu einem Torrent kompiliert waren, einer winzigen Datei, die einen Link zu einer großen Datei auf einem anderen Rechner enthielt, in diesem Fall zu dem von HBGary. Torrents wurden Tag für Tag von Millionen Menschen weltweit benutzt, um illegal Software, Musik oder Filme herunterzuladen, und Tflow wollte seine Torrent-Datei auf der beliebtesten aller Torrent-Webseiten einstellen: The Pirate Bay. Das hieß, schon sehr bald würde jeder Interessierte über 40.000 E-Mails von Barr herunterladen und lesen können.

Am Morgen, etwa 30 Stunden vor dem Super-Bowl-Endspiel, überprüfte Barr die Webseite von HBGary und sah, dass sie, genau wie er vorhergesehen hatte, mehr Anfragen als üblich bekam. Es waren keine legitimen Besucher, sondern die Anfänge eines DDoS-Angriffs von Anonymous. Das war nicht das Ende der Welt, aber er loggte sich bei Facebook ein, um unter dem fiktiven Profil eines Julian Goodspeak mit einem seiner Anon-Kontakte zu sprechen, einer anscheinend wichtigen Figur namens CommanderX. Barrs Recherchen und seine Gespräche mit CommanderX ließen ihn vermuten, dass dieser in Wirklichkeit »Benjamin Spock de Vries« heiße, was allerdings nicht stimmte. CommanderX, der nicht wusste, dass eine kleine Gruppe von Hackern sich bereits Zugang zu Barrs E-Mails verschafft hatte, antwortete auf Barrs höfliche Anfrage, ob CommanderX nicht etwas gegen die Überlastung seiner Webseite tun könne. »Meine Recherchen sind abgeschlossen. Ich habe nichts gegen euch«, erklärte Barr. »Ich befasse mich mit den Schwachstellen sozialer Netzwerke.« Barr meinte damit, seine Recherchen sollten nur zeigen, wie man Organisationen infiltrieren könne, indem man in den Profilen ihrer Mitglieder bei Facebook, Twitter und LinkedIn herumschnüffelte.

»Ich habe damit nichts zu tun«, schrieb CommanderX berechtigterweise zurück. Er hatte sich die Webseite von HBGary Federal angesehen und

wies Barr jetzt darauf hin, dass sie angreifbar aussah. »Ich hoffe, Sie werden für diesen Auftrag gut bezahlt.«

Am Sonntagmorgen, etwa elf Stunden vor dem Anstoß, hatte Tflow die Arbeit an den E-Mails von Barr, Vera und Wallisch abgeschlossen; die Torrent-Datei war fertig zur Veröffentlichung. Jetzt kam das große Vergnügen, Barr zu sagen, was ihm bevorstand. Natürlich würden ihm die Hacker nicht alles sofort sagen. Mehr Lulz brachte es, wenn man zuerst ein bisschen mit ihm herumspielte. Inzwischen wussten sie, dass Barr unter dem Spitznamen CogAnon in Anonymous-Chatrooms zu finden war und dass er in Washington, D. C., lebte. »Wir haben alles von seiner Sozialversicherungsnummer über seine Militärakten bis zu seinen Sicherheitseinstufungen«, schrieb Sabu an die anderen. »Wir wissen sogar, wie oft er am Tag aufs Klo geht.«

Gegen acht Uhr morgens Ostküstenzeit am Sonntagmorgen beschlossen sie, ihm schon mal ein bisschen Angst zu machen. Als Barr sich als CogAnon in das AnonOps-Chatnetzwerk einloggte, schickte Topiary ihm eine private Nachricht. »Hallo«, begann Topiary. »Hi«, schrieb CogAnon zurück. In einem zweiten Chatroom-Browserfenster gab Topiary einen laufenden Kommentar für die anderen Anons ab, die sich darüber totlachten. »Schreib ihm, du suchst Freiwillige für eine neue Mission«, schrieb Sabu. »Aber Vorsicht«, mahnte ein anderer. »Er könnte Verdacht schöpfen.«

Topiary kehrte zu seiner Unterhaltung mit dem Sicherheitsspezialisten zurück. Er gab immer noch vor, CogAnon für einen echten Unterstützer von Anonymous zu halten. »Wir suchen Freiwillige für einen Einsatz im Bereich Washington. Interessiert?« Barr ließ 20 Sekunden verstreichen, dann antwortete er: »Vielleicht. Hängt davon ab, worum es geht.« Topiary kopierte die Antwort zum Mitlesen in den anderen Chatroom. »Hahahahaa«, schrieb Sabu. »Schaut euch an, wie die Schwuchtel mir die Info entlocken will, richtige psychologische Kriegsführung«, schrieb Topiary. »Schwuchtel« wurde in Anonymous-Chatrooms so inflationär gebraucht, dass es nicht einmal mehr als Beleidigung galt.

»Ich sehe an deinem Hostserver, dass du in der Nähe unseres Ziels wohnst«, schrieb Topiary an Barr. In Washington, D. C., stockte Barr der Atem. »Ist das Ziel konkret oder virtuell?«, tippte er. Er wusste natürlich, dass es nur um ein virtuelles Ziel gehen konnte, aber ihm fiel nichts anderes ein. »Ich bin in der Nähe, stimmt ...« Wie genau hatten sie heraus-

gefunden, dass er in D. C. wohnte?»Virtuell«, antwortete Topiary. »Alles an Ort und Stelle.« Dann lies er die Anons wieder mitlesen. »Es wäre zum Totlachen, wenn er jetzt eine E-Mail darüber schreibt«, kommentierte er. Sie konnten gar nicht glauben, was da stand. »DIESER TYP IST EIN SOLCHER IDIOT«, meinte Sabu. »Ich würde ihn am liebsten von hinten vergewaltigen«, entgegnete Topiary. Einen Server zu »vergewaltigen« war eine häufige Umschreibung dafür, sich gewaltsam Zugang zu seinem Netzwerk zu verschaffen. Tflow richtete einen neuen Chatroom namens #ophbgary im Anonymous-Chatnetzwerk ein und lud Topiary ein.

»Hört mal«, meldete sich ein Hacker namens AVunit. »Ist das alles echt? Klingt nämlich richtig toll.« In seinem Chat mit Topiary versuchte Barr derweil, hilfsbereit zu klingen. »Ich brauche nur ein paar Stunden bis in die Stadt ... hängt vom Verkehr ab, lol.« Topiary wollte ihm noch etwas mehr Angst einjagen: »Unser Ziel ist ein Sicherheitsdienstleister«, schrieb er. Barr wurde flau im Magen. Das hieß also, dass Anonymous es wirklich auf HBGary Federal abgesehen hatte. Er öffnete sein E-Mail-Programm und schrieb eine hastige Mail an andere HBGary-Manager, unter anderem an Hoglund und Penny Leavy.

»Jetzt werden wir direkt bedroht«, schrieb er. »Ich werde das morgen mit dem FBI besprechen.« Sabu und die anderen sahen ruhig zu, wie er die E-Mail abschickte. Er klickte sich in den Chat mit Topiary zurück. »O. K., lass mich wissen, was ich tun kann«, schrieb er. »Hängt davon ab«, antwortete Topiary. »Was kannst du denn alles? Wir brauchen Hilfe, um an Info über Ligatt.com zu kommen.« Barr atmete tief durch. Er war erleichtert. Ligatt war eine Sicherheitsfirma, die ähnlich wie HBGary arbeitete; es sah also so aus, als ob seine Firma (zumindest vorläufig) noch verschont bleiben würde. »Ahhhh, O. K.; ich schau mal, was ich finde«, schrieb Barr fast dankbar zurück. »Habe sie mir schon eine Weile nicht mehr angesehen. Sucht ihr was Bestimmtes?« Er schien zu allem bereit, um HBGary aus der Schusslinie zu halten, auch wenn er nur zum Schein mitspielte. Keine Antwort. Er tippte: »Ich wusste gar nicht, dass die in D. C. sitzen.« Eine Minute später fügte er hinzu: »Mann, ich weiß gar nicht mehr, warum die vor einer Weile so beliebt waren. Es gab auch ziemlich viel Ärger wegen ihnen, oder?« Nichts. »Bist du noch dran?«

Topiary hatte zu tun. Er saß mit den anderen an der Planung der Attacke. Es war nicht mehr viel Zeit, und er musste noch die offizielle Anonymous-

Botschaft schreiben, durch die sie die Homepage von HBGaryFederal.com ersetzen würden. Erst eine Dreiviertelstunde später meldete er sich wieder: »Sorry wegen der Unterbrechung – bleib dran!« »O. K.«, schrieb Barr zurück.

Einige Stunden später, gegen Mittag und etwa sechs Stunden vor dem Super-Bowl-Anstoß, saß Barr dann in seinem Wohnzimmer und starrte entsetzt auf das Display seines Telefons, nachdem er begriffen hatte, dass er gerade aus seinem E-Mail-Account ausgesperrt worden war.

Er rief Greg Hoglund Penny Leavy an, um sie zu informieren, was gerade passierte. Dann rief er seine IT-Administratoren an. Die wollten sich mit Google in Verbindung setzen und versuchen, die Kontrolle über die Webseite von HBGary Federal zurückzugewinnen. Wegen der gestohlenen E-Mails könne man aber nichts mehr machen. Um Viertel vor drei Uhr kam eine weitere Nachricht von Topiary: »Also, heute Abend passiert noch was. Hast du schon was vor?« Es waren nur noch wenige Stunden, und er wollte sichergehen, dass Barr auch wirklich von Anfang bis Ende mitbekam, wie seine Karriere zerstört wurde.

Als es an der Ostküste der USA langsam Abend wurde, machten sich die Anons in allen möglichen Zeitzonen rund um die Welt zum Zuschlagen bereit. Das Stadion der Cowboys in Arlington, Texas füllte sich mit Zuschauern. Die Black Eyed Peas spielten einige Songs, Christina Aguilera verhunzte den Text der Nationalhymne, dann endlich der Münzwurf, einer der Green Bay Packers kickte die Schweinsblase mit der Ferse übers Feld, und das Spiel lief.

Auf der anderen Seite des Atlantiks sah Topiary auf seinem Laptop zu, wie der Football über den Himmel zog. Er saß in seinem schwarzen Ledersessel, den er zum Spielen benutzte, riesige Kopfhörer übergestülpt. Er öffnete ein neues Fenster und loggte sich in Barrs Twitter-Account ein. Vor sechs Stunden hatte er Barr mit dem Passwort kibafo33 ausgesperrt. Jetzt, pünktlich zum Anstoß, begann er zu posten. Er fühlte keine Hemmungen gegenüber diesem Mann, er wollte es ihm richtig heimzahlen. »O. K., meine teuren Anonymous-Mitschwuchteln«, schrieb er von Barrs Twitter-Account aus, »wir arbeiten gerade daran, euch die besten Lulz überhaupt zu bringen. Bleibt dran!« Dann: »Hallo, ihr Arschlöcher, ich bin der CEO einer beschissenen kleinen Firma und krieche den Medien so tief in den Arsch,