

Anonymous: Fluch oder Segen?

Aktivisten der Anonymous-Bewegung sorgten in der Vergangenheit für Furore: So führten sie Angriffe gegen Unternehmen und Institutionen wie CIA, Mastercard oder Sony durch und pressten erfolgreich ein Mitglied frei. Doch sind ihre Aktionen sehr umstritten. Der CDU-Politiker und Autor Stephan Eisel hält die Methoden von Anonymous für inakzeptabel. Der IT-Anwalt Emanuel Schach hebt positive Aspekte der auf Aufmerksamkeit und Transparenz zielenden Aktionen hervor.

In dieser Woche erschien das von den Journalisten Ole Reißmann, Christian Stöcker und Konrad Lischka herausgegebene Sachbuch „We are Anonymous“. [In einer Rezension](#) schreibt Patrick Beuth von Zeit Online dazu: „Anonymous und seine zahlreichen Teil-, Splitter- und Trittbrettfahrergruppen, das betonen die Autoren immer wieder, wollen oft vor allem eines: sogenannte lulz. Sie wollen Spaß haben. Sie tun dafür Dinge, die man fragwürdig bis böse finden kann und die auf keinen Fall mit der Hackerethik vereinbar sind.“ Ist diese Hacker-Bewegung nun Fluch oder Segen? Die Wahrheit liegt wohl irgendwo in der Mitte.

Was aber spricht für oder gegen Anonymous?

Der CDU-Politiker Dr. Stephan Eisel kritisiert, dass sich die Anonymous-Bewegung eines digitalen Faustrechts und des größten Feindes der Freiheit bediene: der Angst. Ihre Methoden seien in einer Demokratie inakzeptabel. Dagegen hält der Anwalt Emanuel Schach die Aktionen von Anonymous für eine Form des politischen Protests und eine Art virtuelles Pendant zu den Demonstrationen auf der Straße, die sich gegen Regulierung und Kontrolle der Datenströme im Netz richten.

UPDATE vom 24.2.2012:

In einem Gespräch hat mich Emanuel Schach darauf hingewiesen, dass ihn die Beschäftigung mit dem Thema zu weiteren Überlegungen befeuert hat. Diese können in seinem Blog nachgelesen werden:

<http://emanuelschach.wordpress.com/2012/02/23/anonymous> Und hier zwei weitere lesenswerte Beiträge, die sich mit Anonymous auseinandersetzen:

<http://www.taz.de/Aus-Le-Monde-diplomatique/!87859> &

<http://blog.zdf.de/hyperland/2012/02/zehn-dinge-die-man-ueber-anonymous-wisse>

[n-sollte](#)

Pro-Standpunkt Emanuel Schach

Anonymous ist keine Gruppe im klassischen Sinn, sie hat keine feste Struktur, keine festen Mitglieder. Anonymous ist ein Phänomen, das zugleich seine eigene Lebensvoraussetzung beschreibt: ein freies, unkontrolliertes und unzensiertes Netz. Klassische Anonymous-Aktionen richten sich vor allem gegen Institutionen oder Gruppierungen, die versuchen, eine Regulierung und Kontrolle der Datenströme im Netz zu erreichen. Aber auch gegen rechtsradikale Gruppierungen oder Foren von Pädophilen geht Anonymous vor. Mit diesen Aktionen zielt Anonymous vor allem auf Aufmerksamkeit und Transparenz. Zumeist erreichen sie dieses Ziel auch. Kritiker werfen ihnen regelmäßig vor, letztlich nichts anderes zu sein als kriminelle Hacker, die sich hinter der Anonymität ihrer (virtuellen) Masken verstecken, um Straftaten zu begehen. Verkannt wird dabei allerdings der politische Charakter, der den Aktionen dieser Idee bzw. Bewegung häufig beikommt. Anonymous ist Protest, eine Art virtuelles Pendant zu den Demonstrationen auf den Straßen unserer Städte. Und ebenso wie diese Demonstrationen etwa den Straßenverkehr behindern, behindert Anonymous mit seinen Aktionen den Datenverkehr: vorübergehend und ohne bleibende Schäden für die Betroffenen. Bei Straßen-Demonstrationen ist allgemein anerkannt: Je mehr Menschen damit konfrontiert werden, je zentraler und öffentlicher sie stattfinden, umso effektiver sind sie. Nicht trotz, sondern wegen der damit einhergehenden temporären Behinderung für die nicht teilnehmende Umwelt. Ein DDoS-„Angriff“ auf eine Webseite, die letztlich nur dazu führt, dass diese temporär von außen nicht erreicht werden kann, ist kein Hack, weil nicht in das EDV-System eingegriffen wird. Es ist eine Art virtuelle Sitzblockade, die sich zudem ohne Zutun von Polizei oder sonstigen Ordnungskräften wieder auflöst. Und die zum Ziel hat, Missstände bei dem Betroffenen aufzuzeigen. Was nicht heißt, Anonymous-Aktionen seien generell gutzuheißen. „Einbrüche“ in Datenbanken mit Veröffentlichung so gewonnener Daten gehen weit über das hinaus, was hingenommen werden kann. Umgekehrt erlauben uns solche Fälle nicht, alle anderen Aktionen zu verurteilen. Vielmehr sollte „Anonymous“ Anlass sein, über die Berechtigung und eventuell auch Regeln eines solchen Protests, solcher digitaler Demonstrationen zu diskutieren. Nicht über deren generelles Verbot. Protest ist Teil und Ausdruck einer vitalen Demokratie. Auch im Netz.

Contra-Standpunkt Dr. Stephan Eisel

Man kann die Ziele des Internet-Kollektivs „Anonymous“ teilen oder auch nicht, aber seine Methoden sind in der Demokratie inakzeptabel. Die Bewegung nimmt nämlich für sich in Anspruch: Der Zweck heiligt die Mittel. Dieser machiavellistische Grundsatz ist das Gegenteil von freiheitlicher Demokratie. Anonymous kämpft gegen Internetzensur mit den Mitteln der Zensur, indem durch Hackerangriffe systematisch Internetangebote unliebsamer Anbieter lahmgelegt werden. Man ist gegen „Netzsperrern“, um selbst nach Gutdünken im Internet zu sperren, was nicht behagt. Anonymous propagiert nicht nur, sondern lebt das digitale Faustrecht im Internet. Auf der deutschen Anonymous-Homepage finden sich Slogans wie: „Da niemand weiß, was richtig ist, kann niemand beurteilen, was falsch ist.“ Oder „Alles ist erlaubt!“ Angeblich um die Freiheit des Internets zu schützen, bedient sich Anonymous des größten Feindes der Freiheit: der Angst. Aus dem Lehrbuch des Totalitarismus könnten Anonymous-Slogans stammen wie: „Identität ist unwichtig, wenn du weißt, dass es uns gibt.“ oder „Wir sind viele, aber Du weißt nicht wer; wir sind überall, doch du weißt nicht wo.“ In Diktaturen schützt Anonymität vor Verfolgung, in der Demokratie gehört sie zur Grundausstattung der Gegner der Freiheit: Rechts- und Linksextremisten ver mummen sich, religiöse Fundamentalisten agieren aus dem subversiven Untergrund. Wer im Schutz der Anonymität nicht nur Internetseiten lahmgelegt, sondern auch Kreditkartendaten stiehlt oder persönliche Daten veröffentlicht, bedient sich der gleichen Methoden. Der Glaube an die Überzeugungskraft eigener Argumente kommt darin jedenfalls nicht zum Ausdruck, eher die Feigheit dafür einzustehen. Die Anonymous-Bewegung ist so widersprüchlich wie die grinsende Maske von Guy Fawkes, hinter der sich ihre Anhänger gerne verstecken. Fawkes wollte 1605 mit mehr als zwei Tonnen Schwarzpulver das englische Parlament in die Luft sprengen. 2008 machte der Film „V wie Vendetta“ nach der gleichnamigen Comicserie das Gesicht des gescheiterten Terroristen bekannt, weil es der anarchistische Titelheld bei seinen Anschlägen als Maske trug. Die Rechte an Comic und Film liegen beim Medienkonzern Time Warner, einem der Feindbilder der Anonymous-Bewegung. Die von ihr benutzte Fawkes-Maske gehört zu den Merchandise-Produkten des Konzerns. So verdient der internationale Medienkonzern an jeder Maske, die seine Gegner im Kampf gegen ihn tragen...

Dieser Beitrag wurde von mir auf politik-digital.de am 23.2.2012 unter

Gute oder böse Hacker?

Die Hackergruppe Lulzsec [erklärt den Regierungen](#) und den sogenannten „Whitehat-Sicherheits-Terroristen“ den Krieg und das Hackerkollektiv Anonymous zu ihrem Verbündeten. Welche Bedrohung geht von ihnen aus? Kämpfen sie für eine gute Sache? Ich sprach dazu mit dem IT-Sicherheitsexperten Ralph Langner.

Angeblich griffen heute Mitglieder der beiden Hackergruppen Anonymous und Lulzsec in einer ersten konzertierten Aktion Internet-Präsenzen der brasilianischen Regierung an. So sollen für mehrere Stunden im Rahmen der Operation Anti-Security (#AntiSec) die Webseiten des Präsidenten, der Regierung und des Finanzministeriums mittels etwa zwei Milliarden Datenanfragen per DDoS-Attacke innerhalb kurzer Zeit lahmgelegt worden sein. Meldungen dieser Art werden zurzeit fast täglich verbreitet. [Mutmaßliches Hauptziel](#) der neuerdings verbrüdeten Hackerbewegungen soll es jedoch in Zukunft sein, Informationen von Regierungen, Großkonzernen oder Banken zu stehlen und offenzulegen, die aufzeigen, was hinter dem Rücken der Bürger so getrieben werde. Auf ihrem [Twitter-Kanal](#), dem immerhin schon mehr als 250.000 Nutzer folgen, [kündigte Lulzsec für den morgigen Tag](#) die Operation Anti-Security Payload #1 an.

Video von Anonymous zur Operation AntiSec:

[Hier klicken, um das Video auf YouTube anzusehen...](#)

Beide Gruppen hatten in der Vergangenheit bereits erfolgreich Hacker-Angriffe

auf Institutionen und Unternehmen wie CIA, Mastercard, Visa, Sony, GEMA, GVV oder die türkische Telekommunikationsbehörde TIB durchgeführt. Laut dem [IT-Sicherheitsexperten Ralph Langner](#) geht es Anonymous und Lulzsec in erster Linie darum, Aufmerksamkeit zu erzeugen. Die Ankündigung des Zusammenschlusses liege ebenso wie die intendierte Dramatik ganz auf dieser Linie. Er rechnet beide Gruppen den sogenannten Hacktivisten, also Hackern mit einer weltanschaulichen Agenda, zu. Ernst zu nehmen seien sie, weil einige ihrer Akteure über sehr gute technische Fähigkeiten verfügten. „Wir erwarten ein weiteres Anwachsen solcher Gruppierungen, da es für den normalen Freizeit-Hacker offenbar attraktiver ist, sich einer derartigen Gruppe anzuschließen, als zu versuchen, alleine in die immer stärker gesicherten IT-Systeme potenzieller Opfer einzudringen“, so Langner. Aus seiner Sicht tragen die Aktionen der Hackergruppen zwar dazu bei, dass die Öffentlichkeit für die Gefahren von Cyber-Angriffen sensibilisiert wird, das Vorgehen sei jedoch zu verurteilen: „Zugespitzt könnte man sagen: Hacker sind Teil des Problems, dessen Lösung sie vorgeben zu sein“, bringt er es auf den Punkt. Nicht nur vor diesem Hintergrund begrüßt Langner grundsätzlich die Errichtung von staatlichen Cyber-Abwehrzentren [wie in der vergangenen Woche in Deutschland](#): „Das Cyber-Abwehrzentrum war überfällig. In der jetzigen Form ist es allerdings eher ein Feigenblatt, wo eigentlich ein warmer Pullover gebraucht würde. Wenn das Abwehrzentrum einmal eine dreistellige Personalbasis hat, kann man beginnen, es Ernst zu nehmen. Die Aufgaben sollten in der Prävention massiver Cyber-Angriffe auf die deutsche Industrie und Infrastruktur liegen. Zum gegenwärtigen Zeitpunkt sind wir gegen ernsthafte Angriffe völlig unzureichend geschützt.“ Derzeit wäre es einem Angreifer möglich, Deutschlands Wirtschaft für Tage bis Wochen in weiten Teilen lahmzulegen. Hierzu könnten Cyber-Angriffe auf Kraftwerke, Wasserversorgung, Straßenverkehr (Ampelanlagen), Flugsicherung usw. zählen, ebenso gegen Schlüsselindustrien wie Autobau und Chemie. Darüber hinaus geht der IT-Sicherheitsexperte auch davon aus, dass Attacken in nationalen und internationalen politischen Auseinandersetzungen in Zukunft eine Cyber-Komponente haben werden.

So war beispielsweise [das stark vernetzte Estland](#) im Jahre 2007 das Ziel mehrwöchiger DDoS-Angriffe durch die Jugendorganisation des Kreml. Im Rahmen der Attacke gelang es den Hackern, Server der estnischen Regierung sowie von Banken, Medien und Unternehmen über längere Zeit lahmzulegen. Daraufhin hatten die Esten eine Freiwilligen-Armee aus IT-Experten zur Cyber-

Abwehr ins Leben gerufen, um zukünftig besser gewappnet zu sein. Birgit Johansmeier [berichtete in einem Beitrag bei DRadio Wissen](#) gar von Überlegungen zur Einführung einer Cyber-Wehrpflicht in dem baltischen Staat. Auf die Frage, ob öffentlichkeitswirksame Cyber-Attacken wie die von Lulzsec und Anonymous dazu beitragen könnten, dass Staaten und Unternehmen mit Verweis auf die Abwehr von vermeintlichem Cyber-Terrorismus bestimmte Zensur-Maßnahmen bzw. Netz-Einschränkungen rechtfertigen, antwortete Langner, dass in der Politik natürlich vieles möglich sei, man aber damit das Symptom anstelle der Krankheit bekämpfen würde. „Es ist ja keineswegs so, dass es unmöglich wäre, Cyber-Systeme sicher zu betreiben. Darum hat man sich in der Vergangenheit leider nicht ausreichend gekümmert, weil Sicherheit Geld kostet. Was wir heute sehen, war insofern vorhersehbar.“

Neben Lulzsec und Anonymous gibt es noch viele weitere Hackergruppen, doch erhalten beide durch ihre öffentlichkeitswirksamen Aktionen derzeit [besonders großes mediales Interesse](#). Zumal sie daran interessiert sind, ihr Handeln öffentlich anzukündigen und zu erklären. Auf der anderen Seite gibt es unzählige Cyber-Angriffe durch Hacker, die im Verborgenen stattfinden: sei es auf eine Infrastruktur wie mittels des Computerwurms Stuxnet, zur eigenen finanziellen Bereicherung oder für einen vermeintlich guten Zweck. Doch egal von welcher Tragweite, politischer Motivation und weltanschaulicher Gesinnung solche Cyber-Angriffe auch sein mögen: [Eine simple Trennung zwischen guten und bösen Hackern](#) ist nur schwer möglich, da die Grenzen häufig fließend sind. Und letztlich ist es immer auch eine Frage des Standpunkts!

Dieser Beitrag wurde von mir auf [politik-digital.de](#) am 23.6.2011 unter der Creative Commons Lizenz [CC BY-NC-SA 3.0](#) erstveröffentlicht.