Have Script, Will destroy
Ein Interview mit der Hackerin Clara G.Sopht

1. Februar 2000, Berlin

F: Clara, würdest du dich selbst als ‘Hackerin’ bezeichnen?

A: Nein. Das ist immer wieder die gleiche dumme Frage. Ich schätze mal, es gibt einige Hacker, die mich als ‘Hackerin’ bezeichnen, andere würden mich eher als ‘Crackerin’ bezeichnen oder als “lazy-assed destroyer” (stinkfaule, zerstörungswütige Schlampe). Es gibt jede Menge Schimpfwörter für Leute wie mich, aber das ist mir letztendlich ziemlich gleichgültig.

F: Aber ‚Hacker’ und ‚Cracker’ hat doch bereits ganz unterschiedliche Bedeutungen. Gibt es eigentlich genaue Definitionen dafür, und falls ja, mit welcher möchtest du identifiziert werden?

A: Es gibt das ‚Jargon File’, so eine Art Lexikon für alles, was mit hacken zu tun hat. Da findet man alles, was wichtig ist. Es wurde von verschiedenen Leuten der Hackerszene zusammengestellt und wird seit den 70er Jahren immer wieder ergänzt.

Um deine Frage zu beantworten: Nachdem der Begriff ‚Hacker’ durch die Medien einen sehr schlechten Ruf bekommen hat, ist die Idee entstanden zwischen guten [nicht-kriminellen] und bösen [kriminellen] Hackern zu unterscheiden. Die letzteren wurden dann ‚Cracker’ genannt. Ich weiss nicht, ob das eine gute Idee war, jedenfalls hat sie nicht funktioniert. Die Unterscheidung wird nur innerhalb der Szene selbst getroffen. Die Medien sprechen weiterhin nur von ‚Hackern’. Aber es hat zumindest dazu beigetragen, dass sich einige besser fühlen, weil sie die ‚Guten’ sind. Ich bin gut und böse gleichzeitig, deshalb passen alle diese Bezeichnungen für mich - oder keine. Kommt frauf an.

F: Du bist zum Chaos Communication Congress nach Berlin gekommen. Wie fandest du ihn?

A: Es lohnt sich eigentlich immer, zu solchen Veranstaltungen zu gehen. Man trifft ein paar gute Leute, und die eine oder andere heisse Information springt auch dabei raus. Und ein paar Sachen im Programm fand ich auch spannend wie z.B. ‚Information Warfare’ bzw. ‚Information Operations’ und Infos über ‚Echelon’, das Teil des Projektes 415 ist.

F: Aus dem, was du über das Hackertreffen erzählst, schliesse ich, dass du hauptsächlich an den politischen Aspekten der Informationstechnologie interessiert bist. Stimmt das?

A: Jeder Aspekt von Informationstechnologie hat auch eine politische Komponente. Und es stimmt auf jeden Fall, dass ich mich ganz besonders für die Idee von politischem Widerstand und Aktivismus im Internet interessiere - den elektronischen Untergrund. Hacker bilden die Speerspitze einer neuen Form von Widerstand. Sie besitzen ein ungeheures politisches Potential, obwohl sich viele darüber gar nicht ganz im klaren sind. Und darüber hinaus gibt es Politaktivisten, die für Ziele ausserhalb des Netzes kämpfen und das Netz aber als Mittel für ihren Kampf einsetzen.

F: Welche Formen politischen Widerstandes gibt es denn heute?

A: Hm, das ist nicht leicht zu beantworten. Letztendlich sind es gar nicht so viele, und die diejenigen Formen, die es gibt, sind auch noch sehr umstritten. Ich gebe mal ein Beispiel, um das zu verdeutlichen: Mitte der 90er Jahre hat die Gruppe 'Critical Art Ensemble' ihr Buch 'Electronic Civil Disobedience' (Elektronischer Ziviler Ungehor-sam) veröffentlicht. Die Grundthese des Buches ist, dass sich Macht und Repäsentationsformen von Macht aus der realen Welt in die elektronischen Netze verlagern. Deswegen hätte jeglicher effektiver Widerstand gegen diese Macht ebenfalls im Netz stattzufinden. CAE haben ein theoretisches Modell entwickelt, das die Idee des zivilen Ungehorsams aus dem realen Leben in die virtuelle Welt verschiebt und nannten es 'elektronischen zivilen Ungehorsam'. Es geht dabei vielmehr um das Blockieren eines Informationsflusses, als um das Blockieren von Warentransporten oder Menschen, aber diese 'virtuellen' Blockaden können ebenfalls an den Orten militärischer, kommerzieller oder Regierungseinrichtungen erfolgen. Die Grundannahme von CAE wird einfach durch die Tatsache bestätigt, wie diese Einrichtungen gesichert werden und daran, wie hart Eindringlinge bestraft werden. Je mehr Aufwand für die Verteidigung und Bestrafung betrieben wird, umso grösser sind natürlich die Machtinteressen, die dahinter stehen. Und wie du sicherlich weisst, sind Hacker verhältnismässig hohen Starfen ausgesetzt. Aber das bedeutet einfach, dass sie an den richtigen Orten operieren.

F: Du erwähntest vorhin, dass diese Methoden sehr umstritten sind. Wo genau liegt der Streitpunkt?

A: Der Streit fing an, als es die ersten Vesuche gab, das theoretische Modell von CAE in die Praxis umzusetzen. Man bezeichnet diese Art von hacking als 'Denial of Service'-Angriff (Service-Verweigerung), DoS. Das bedeutet hauptsächlich, über das Netz Computer ausser Betrieb zu setzen, indem man sie mit so vielen Anfragen überhäuft, dass sie unter dem Ansturm zusammenbrechen. Damit kann man jedes Netzwerk lahmlegen, ganz unabhängig davon, wie gross es ist und wieviel Bandbreite es besitzt. In nur wenigen Minuten kann der Rechner nicht mehr antworten, weil die Leitungen durch die Flut der Anfragen blockiert sind. Um die Aktion zu automatisieren, bedarf es nur relativ einfacher Scripts [kleine Computerprogramme], die die Anfragen immer wieder automatisch stellen. Natürlich sind nicht alle DoS-Angriffe politisch motiviert oder haben etwas mit den Ideen von CAE zu tun. Oft wird das auch nur aus Neugier, Spieltrieb oder auch blinder Zerstörungswut betrieben. Und genau das löst dann die Miss-verständnisse aus und führt dazu, dass alle Angriffe in einen Topf geworfen werden und diese Möglichkeit des Aktivismus grundsätzlich in Frage gestellt wird.

F: Ich nehme an, dass fast jede/r von den Angriffen auf die e-commerce Sites von eBay, amazon, yahoo und noch anderen im Februar dieses Jahres gehört hat. Sie wurden mit den gleichen Mitteln ausgeführt. Mir erscheint das doch eine sehr zielgerichtete Angriffsmethode zu sein. Warum genau ist sie so umstritten?

A: Erst einmal gibt es ja ganz unterschiedliche Arten von Dos-Angriffen, die alle etwas unterschiedlich funktionieren und jeweils andere Scrips verwenden. Im Moment sind alle Dos-Angriffe eigentlich Ddos-Angriffe, was für ‚distributed denial of service' steht. D.h. sie werden von mehreren Servern gleichzeitig gestartet, benutzen ausspionierte [spoofed] IP-Nummern als Absender und arbeiten mit Millionen von Datenpaketen. Solche Angriffe belegen nicht nur die ganze Bandbreite des angepeilten Netzwerkes, sondern verursachen auch für andere Nutzer der gleichen Leitungen Probleme. Man kann also nie genau sagen, wer alles mitbetroffen sein wird, weswegen die Methode als unelegant gilt. Und anstatt den freien Informationsfluss zu gewährleisten, was ein Grundprinzip der Hacker-Ethik ist, wird genau das Gegenteil erreicht. Das sind die eher rationalen Argumente, die gegen DoS vorgebracht werden, aber es gibt noch jede Menge irrationale. Leute, die mit DoS operieren wird vorgeworfen, kindisch und technisch unfähig zu sein, und dass sie nur niedere Beweggründe hätten. Die Angriffe selbst werden als vollkommen sinnlos eingestuft.

F: Und was hältst du persönlich von dieser Art des hackens?

A: Naja, erst einmal möchte ich grundsätzlich festhalten, dass man sich schon allein durch den Besitz eines Computers ganz schön viel Macht aneignet. Kommen dann noch ein paar spezielle Kenntnisse dazu, kann es richtig interessant werden. Das Computernetz bietet ja jede Menge Angriffsflächen. Irgendwie, aus Versehen, haben jetzt plötzlich unheimlich viele Menschen einen Computer. Das hat zwar ein paar wenige reich gemacht hat, aber die halbe Welt ist jetzt mit diesen ‚Waffen' ausgestattet. Das hatte offensichtlich niemand so recht bedacht, denn das letzte, was Regierungen gebrauchen können, ist ein schlagkräftig bewaffnetes Volk.

Aber um noch einmal auf Dos zurückzukommen: Die meisten Leute, die ich kenne und die solche Attacken ausführen, sind gute Hacker, die wissen, was sie tun. Und sie machen sich darüber Gedanken, warum sie wen angreifen. Es sind also nicht nur dumme, kleine Script-kiddies*. Für diese Leute ist Dos eine Form von Widerstand unter anderen. Sie praktizieren durchaus auch andere Formen, wie z.B. Websites zu hacken und Inhalte zu manipulieren. Aber viele Formen sind einfach nicht besonders spektakulär, z.B. sich um Verschlüsselung und Datensicherheit zu kümmern, kostenlose, gut arbeitende Software zu schreiben oder einfach wichtige, von der Industrie zurückgehaltene Informationen zu veröffentlichen (reverse engineering). Ach, und es gibt noch ein paar Beispiele für Hackergruppen, die durch die Kombination verschiedener Methoden, ziemlich effektive Startegien entwickelt haben, wie zum Beispiel R™ark (www.rtmark.com). Sie arbeiten sehr effektiv und öffentlichkeitswirksam, was die Kampagne genen ‚eToys' 1999 deutlich bewiesen hat. Sie haben es tatsächlich geschafft, dass die kleine Künstergruppe ‚etoy' ihren Domainnamen gegen den Konzern ‚eToys' verteidigen konnte. Das war ein legendärer Erfolg, der beweist,

dass sich kommerzielle Interessen im Netz nicht immer durchsetzen können. Die ‘Electrohippies’ (www.gn.apc.org/pmhp/ehippies/) wären ein weiteres Beispiel. Sie betreiben gerade mit unterschiedlichsten Formen im Netz, u.a. DoS, Widerstand gegen Genmanipulationen. (www.resistanceisfertile.com)

Es geht mir hier nicht darum, Dos als Mittel der Wahl anzupreisen, aber was die Öffentlichkeitswirksamkeit anbelangt, kenne ich im Moment keine bessere Methode. Wir müssen einfach noch viel experimentieren, um Erfahrungen zu sammeln und auch von unseren Irrtümern lernen. Gut an DoS ist in jedem Fall, dass es jede Menge Aufmerksamkeit verursacht, was man jüngst an dem Angriff auf MPAA (Motion Picture Association of America) gesehen hat, oder noch viel deutlicher im Februar dieses Jahres, als die e-commerce Websites yahoo.com, eBay.com und amazon.com und noch einige anderen geschlossen werden mussten, nach dem sie mit TFN (TribeFloodNet) und trin00 Scripts angegriffen worden waren. Das hat fast eine Massenhysterie ausgelöst, als plötzlich klar wurde, wie verletzlich und instabil der grosse Hoffnungsträger ‘Internet’ eigentlich ist. Aber es hat auch gezeigt, welche Interessen dahinter stehen und wo sich Macht akkumuliert im Netz. Ganz zu schweigen von einem wirklich grossen Vorzug dieser Methode, nämlich, dass es kaum eine Chance gibt, die ‘Täter’ zu erwischen. Wenn man sich nicht allzu blöd anstellt, ist es eine recht sichere Methode. Und den Informationsfluss zu behindern, ist immer noch die beste Methode, um das reibungslose Funktionieren einer Institution zu stören - auch wenn die Hackerethik davon ausgeht, dass der “freie Fluss von Information”, oberstes Gebot sei…

F: Lass uns noch einmal auf die Angriff vom Februar zurückkommen.

A: Bestimmte Dinge scheinen sich einfach zu wiederholen. Jedenfalls gibt es Ähnlichkeiten zu den ersten erfolgreichen Angriffen mit DdoS, die 1994 oder so stattgefunden haben. Das war vom ‘Electronic Disturbance Theatre’ organisiert und gegen die mexikanische Regierung gerichtet. Und technisch gesehen, waren die Angriffe wirklich keine Überraschung, zumindest nicht, wenn man ein bisschen Ahnung hat. Alles was man braucht, um solche Angriffe auszuführen, existiert seit längerem und es war nur eine Frage der Zeit, bis jemand einen Grossangriff starten würde. Und da es sehr erfolgreich war, kann ich mir vorstellen, dass es bald mehr davon geben wird.

Interessanterweise fanden die Angriffe ein paar Tage nach Clintons Vorschlag statt, das Budget für die Verfolgung elektronischer Kriminalität extrem zu erhöhen. Das war für einige Schlaumeier der sichere Beweis, dass der Secret Service selbst hinter den Angriffen steckte, um Panik auszulösen und so grössere Chancen bestünden das Budget zu verabschieden. Aber es war genau anders herum. Wenn die Regierung andauernd ‚Alternativ-Kriege’ und ‚Cyberterrosrismus’ heraufbeschwört, dann sollten wir ihnen den Gefallen tun. Die ‚neue und tödliche Gefahr’ hat sie ereilt. Und das alles ist erst der Anfang.

Nein, ganz im ernst. So wie die technische Infrastruktur heute funktioniert, aber auch wie mit Sicherheitsmängeln umgegangen wird, kann in keinster Weise die Stabilität des Internet gewährleisten. Und der Knackpunkt ist, dass die tatsächliche Zuverlässigkeit des Internet in

keiner Relation steht, zu den gigantischen Werten, die darauf projiziert werden. Es tut ganz gut, ein bisschen Verwirrung und Panik auszulösen und ein paar Seifenblasen platzen zu lassen. Der Cyberspace ist nicht sicher und wird es niemals sein! Ausserdem habe ich grundsätzlich was gegen Glaubenssysteme - auch wenn sie uns den Glauben an die Technologie verkaufen wollen.

F: Ich würde noch gern einen anderen Aspekt ansprechen, Clara. Du bewegst dich ja in einem männlich dominierten Feld. Hast du Probleme damit? Musst da dafür kämpfen, dich als Frau durchzusetzen? Bist du Feministin?

A: Naja, jedenfalls ist meine Erfahrung, dass die meisten Hacker Feministinnen hassen. Das ist schon Grund genug, mich 'Feministin' zu nennen, obwohl ich im allgemeinen keine grosse Freundin von Ismen aller Art bin - wie z.B. Hackismus J - aber wir sind in der Tat weit davon entfernt, als Männer und Frauen gleichwertig behandelt zu werden. Es ist nur nicht so einfach heutzutage gute Strategien zu entwickeln, damit umzugehen. Wir haben zwar immer noch mit struktureller Diskriminierung zu kämpfen, nur haben sich die Bedingungen sehr verändert. Ein intentionales Politikverständnis wie es die 70er-Jahre-Feministinnen noch hatten greift einfach nicht mehr: Es fehlen allgemeingültige Ansatzpunkte und gemeinsame Ziele. Deshalb kämpft jede mehr oder weniger alleine vor sich hin. Anstatt Subjekte zu sein, die klare Rechte einfordern, können wir uns nur noch damit beschäftigen, unsere Identitäten zu konstruieren.

F: Was hältst du vom Cyberfeminismus?

A: Naja, Cyberfeminismus - das ist so komisches Zeug. Die sind zwar ganz aufgeweckt und erfrischend, die Mädels, aber ich würde ihnen raten, sich ein bisschen mehr die Hände mit der Technik schmutzig zu machen. Wenn sie anstatt ihrer rhetorischen Strategien technologische Attacken fahren würden, könnten sie echt tödlich werden.

F: Hast du eine Vision? Was treibt dich in deiner Arbeit an?

A: Das weiss ich gar nicht so genau. Manchmal fängt man plötzlich an die Dinge zu hassen, die man zuvor am meisten geliebt hat. Und dann stelle ich mir vor, das ganze Internet ausser Betrieb zu setzen - natürlich nicht ganz alleine, sondern zusammen mit ein paar FreundInnen - und dann würde ich wohl Musikerin und Tänzerin werden…

· Script-kiddies: Jugendliche, die zum Eindringen in Computer(netze) nicht selbst geschriebene Programme verwenden, sondern bereits fertige Scripts, die sie vom Netz herunterladen. Problematisch daran ist vor allem, dass die Jugendlichen aufgrund mangelnder Erfahrung das Potential der Scripts nicht genau einschätzen können und deshalb gar nicht wissen, was diese u.U. auslösen können.

Veröffentlicht in:

UFO Strategien, Hrsg. Helene von Oldenburg, Isensee Verlag, 2000

Cross Female, Ausstellungskatalog, Berlin, 2000

Dieser Text isz Teil des Projectes Women Hackers:
http://artwarez.org/projects/womenhackers