Netzpiraten
Die Kultur des elektronischen Verbrechens

Armin Medosch, Janko Röttgers (Hrsg.)

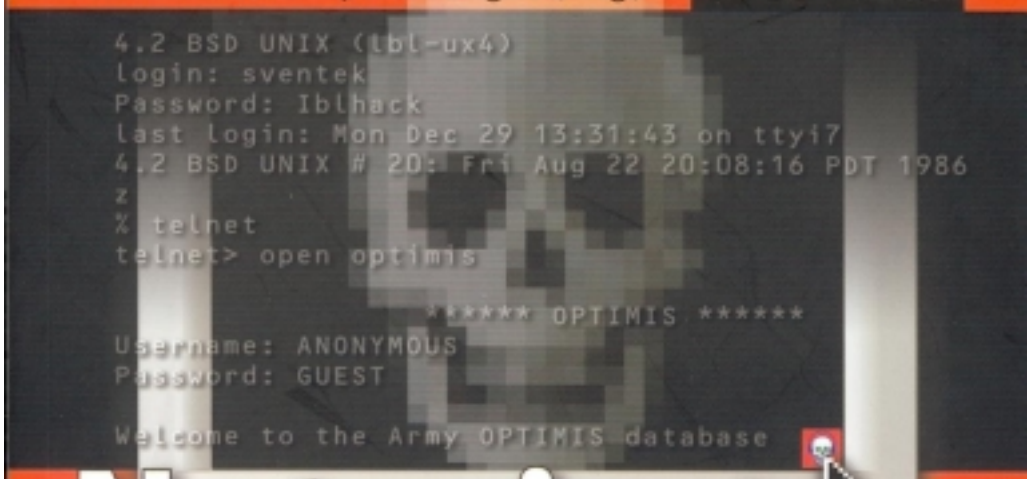
Gescannt von ***Jacopo***

Gewidmet der Cosmo Connor Community,
und Isabel R., die so ein Buch niemals lesen würde ;-)

Version 01, 18.02.2002

Armin Medosch • Janko Röttgers (Hrsg.)

TELEPOLIS



Netzpiraten

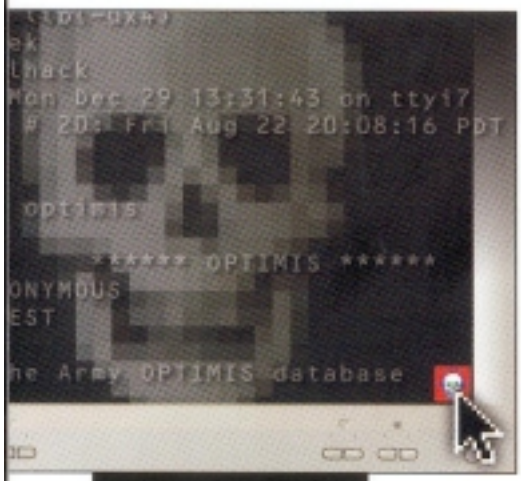
Die Kultur des elektronischen Verbrechens

HEISE

Armin Medosch, Janko Röttgers (Hrsg.)

Netzpiraten

Die Kultur des elektronischen Verbrechens



Hacker, Cracker und Raubkopierer, Virenprogrammierer und Cyber-Terroristen werden gerne als dunkle Seite des Netzes gehandelt, als technisch hochgerüstete Bösewichte, die den Stoff liefern für reißerische Bedrohungsszenarien. Politiker lassen sich von ihnen zu Law-and-Order-Parolen hinreißen, Strafverfolger und Geheimdienste begründen mit ihnen eine zunehmende Überwachung der neuen Kommunikationswege. Doch wie gefährlich ist das viel zitierte elektronische Verbrechen wirklich?

In diesem TELEPOLIS-Band wagen ausgesuchte Experten einen vorurteilsfreien Blick auf all jene Subkulturen, um die viele Menschen normalerweise lieber einen großen Bogen machen.

Was motiviert jemanden, einen Virus zu programmieren? Was hat es mit dem vielbeschworenen Info-Krieg auf sich? Wie organisieren sich Software-Raubkopierer? Wie rechtfertigen sie ihr Handeln, welche Beziehungen pflegen sie zu Sicherheitsfirmen und surfenden Strafverfolgern?

«Netzpiraten» widmet sich diesen Fragen detailliert und stellt sie in den Kontext einer Diskussion um Sicherheit und kulturelle Freiräume in den Datennetzen.

TELEPOLIS

Die Telepolis-Bücher zur Netzkultur bauen auf den thematischen Stärken und dem internationalen Autorenkreis des Online-Magazins Telepolis auf. Die Reihe konzentriert sich in ihren Bänden auf jeweils ein Thema mit speziell in Auftrag gegebenen Artikeln anerkannter Fachjournalisten und Wissenschaftler. In Zusammenarbeit mit Gastherausgebern erarbeitet, bieten die Telepolis-Bücher anspruchsvolle Lektüre zu relevanten Themen unserer Zeit.

Telepolis finden Sie im Web unter
www.telepolis.de

ISBN 3-88229-188-5

DM 29,00
Euro 15,00 (D) (ab 1.1.2002)
Euro 15,50 (A) (ab 1.1.2002)

9 783882 291889

Das Online-Magazin Telepolis wurde 1996 gegründet und begleitet seither die Entwicklung der Netzkultur in allen Facetten: Politik und Gesetzgebung, Zensur und Informationsfreiheit, Schutz der Privatsphäre, wissenschaftliche Innovationen, Entwicklungen digitaler Kultur in Musik, Film, bildender Kunst und Literatur, sind die Kernthemen des Online-Magazins, welche ihm eine treue Leserschaft verschafft haben. Doch Telepolis hat auch immer schon über den Rand des Bildschirms hinausgesehen: Die Kreuzungspunkte zwischen realer und virtueller Welt, die »Globalisierung« und die Entwicklung der urbanen Kultur, Weltraum und Biotechnologie bilden einige der weiteren Themenfelder. Als reines Online-Magazin ohne Druckausgabe nimmt Telepolis damit eine einzigartige Stellung im deutschsprachigen Raum ein und bildet durch seine englischsprachige Ausgabe und seinen internationalen Autorenkreis eine wichtige Vermittlungsposition über sprachliche, geografische und kulturelle Grenzen hinweg.

www.telepolis.de

Armin Medosch ist Mitbegründer und Redakteur des Online-Magazins Telepolis und lebt in London.

Janko Röttgers lebt und arbeitet als freier Journalist und Autor in Berlin. Seine Texte erscheinen u.a. in Telepolis, De:Bug und der Berliner Zeitung. Weitere Infos: www.lowpass.de.

Armin Medosch, Janko Röttgers (Hrsg.)

Netzpiraten

Die Kultur des elektronischen Verbrechens

Verlag Heinz Heise

Armin Medosch
E-Mail: ame@tp.heise.de

Janko Röttgers
E-Mail: roettgers@lowpass.de

Copy-Editing: Susanne Rudi
Lektorat: Dr. Michael Barabas
Satz und Herstellung: Verlagsservice Hegele, Dossenheim
Umschlaggestaltung: Helmut Kraus, Düsseldorf
Druck und Bindung: Koninklijke Wöhrmann B.V., Zutphen, Niederlande

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Netzpiraten : die Kultur des elektronischen Verbrechens/Armin Medosch ; Janko Röttgers (Hrsg.). - 1. Aufl. - Hannover : Heise, 2001
(Telepolis)
ISBN 3-88229-188-5

1. Auflage 2001

Inhalt

Netzpiraten

Ein Vorwort

»Sollen wir uns vielleicht eine verdammte Website zulegen?« fragt Robert De Niro in der Mafia-Komödie »Reine Nervensache« gereizt, als seine Jungs von ihm Reformen verlangen. De Niro, der über Jahrzehnte so etwas war wie unser Mann bei der Mafia, bekommt in diesem Film von 1999 plötzlich Muffensausen. Die Zeiten haben sich geändert, die alterprobten Strukturen der Familienclans wirken antiquiert vor der sich vernetzenden Gesellschaft.

Auch jenseits der Leinwand hat sich längst die Erkenntnis durchgesetzt, dass das Verbrechen im 21. Jahrhundert zunehmend im Netz stattfindet. Dabei geht es natürlich nicht um Mafia-Familien mit eigenen Websites. Doch allzu oft bedient sich die sensationslüsterne und auf wenig Sachkenntnis aufbauende Berichterstattung der traditionellen Medienlandschaft ähnlicher Klischeebilder wie die Traumfabriken Hollywoods. Anstelle des organisierten Verbrechens sind als universelles Feindbild mehr und mehr genialische Einzeltäter getreten, gerne auch pauschal als Hacker bezeichnet.

Statt diesen schon viel zu arg strapazierten Begriff weiter zu bemühen, möchte dieses Buch sich detailliert den Subkulturen des elektronischen Verbrechens widmen, die im Rummel um die großen Hacks oft in Vergessenheit zu geraten drohen: Den Virenprogrammierern, Raubkopierern, Kopierschutz-Knackern und Script-Kiddies dieser Welt. Was treibt sie zu ihrem Handeln an? Wie rechtfertigen sie ihr Tun? Welches Verhältnis pflegen sie zur Gegenseite, zu den Herstellern von Antiviren-Software, zu Kopierschutz-Programmierern und zu surfenden Strafverfolgern? Und welchen Einfluss hat ihr Handeln auf die Entwicklung des Internets, auf die Mainstream-Netzkultur? Zur Beantwortung dieser Fragen haben wir für »Netzpiraten - Die Kultur des elektronischen Verbrechens« eine ganze Reihe Fachkenner gebeten, sich einer spezifischen Subkultur zu widmen.

Wohlgemerkt geht es dabei nicht darum, Gesetzesverstöße zu rechtfertigen. Dass aber die Grenzen zwischen Illegalität und kultureller Innovation hauchdünn sind, zeigt nicht zuletzt die Musik-Tauschbörse Napster. Sie entwickelte sich aus den Tausch-Strukturen der Musikpiraten in Chaträumen und BBS-Systemen, wird aber mittlerweile auch von Intel-Entwicklern als Blaupause für die Zukunft des Internets begriffen. Bernhard Günther zeichnet diese Entwicklung in seinem Text eindrucksvoll nach und zeigt dabei, dass Piraten auch früher schon in vielen Dingen ihrer Zeit voraus waren. David McCandless berichtet uns dazu vom Rausch, den die Verbreiter raubkopierter Software bei ihrem Tun empfinden und von ihrem Katz- und Maus-Spiel mit den privaten Ermittlern der großen Softwarekonzerne.

Die Underdogs des elektronischen Verbrechens, von denen dieses Buch handelt, haben allerdings nicht nur mit der Strafverfolgung zu kämpfen. Auch von der etablierten Hackergemeinde ernten sie oft nur böse Worte. Boris Gröndahl widmet sich deshalb der Hacker-Ethik und zeigt, dass diese Abgrenzung schon immer eine willkürliche Konstruktion

war. Bewegung in die verhärteten begrifflichen Fronten könnten auch die Auseinandersetzungen um DeCSS und SDMI bringen - treten hier doch Universitätsprofessoren als Cracker im klassischen Sinne auf, die mit ihren Hacks gleichzeitig auch das Recht auf freie Meinungsäußerung verteidigen. Grund genug, diese Entwicklung mit einigen Telepolis-Artikeln der letzten Monate zu dokumentieren.

Das Recht auf freie Meinungsäußerung reklamieren auch Virenprogrammierer für ihr Handeln. Janko Röttgers dokumentiert diese widersprüchliche Szene und gibt dabei einen Überblick über die Geschichte der Computerviren. Peter Mühlbauer beschreibt die Rezeption der viralen Epidemien aus dem Cyberspace und zieht Parallelen zur Aids-Debatte und zu der Angst vor kultureller Unterwanderung. Armin Medosch geht dem Phänomen nach, dass falsche Virenwarnungen selbst zu einer Art Virus werden können und ein Hoax oft weit mehr ist als nur ein schlechter Scherz. Florian Schneider hat schon oft unerwünschte Post gekommen und nimmt das zum Anlass, einmal genauer über Geschichte und Urheber der alltäglichen Flut von Spam-E-Mails zu berichten.

Einer ganz anderen Subkultur nimmt sich Ralf Bendrath in seinem Beitrag über den Info-War an. Jenseits aller Öffentlichen Warnungen vor Cyber-Terroristen findet vor allen Dingen bei den US-Streitkräften ein heimliches Aufrüsten statt, dessen Grenzen zum elektronischen Verbrechen fließend sind. Dagegen nehmen sich die oft bereits als Info-Krieg bezeichneten Taten der Script-Kiddies und Web-Graffiti-Gruppen recht harmlos aus, wie Armin Medosch in seinem Text über jugendliche Hacker aufzeigt.

Trotzdem schlagen die Mafiaboys und Coolios der Cracker-Welt in Presse und Politik mit schöner Regelmäßigkeit hohe Wellen. Schnell ist dann vom »rechtsfreien Raum Internet« die Rede. Unter der Annahme, dass in diesem unkontrollierten Freiraum endlich aufgeräumt werden müsse, werden drakonische Gesetze entworfen und Gerichtsfälle ausgefochten, die das Rad der Zeit zurückdrehen möchten und im Internet verbieten wollen, was in der wirklichen Welt eine allgemein akzeptierte Freiheit ist. Christiane Schulzki-Haddouti wagt sich deshalb in die digitalen Freihäfen, in Zonen unzensierter und nicht überwachbarer Kommunikation, die von engagierten freiheitsliebenden Programmierern geschaffen wurden. Schon heute operieren diese Programmierer oftmals in juristischen Grauzonen. Sollte sich der Trend zu einer flächendeckenden Überwachung des Netzes fortsetzen, könnten sie auch hierzulande bald zum elektronischen Verbrechen gehören.

Um dies zu verhindern, brauchen wir zuallererst eine sachliche, informierte Debatte über die tatsächlichen Gefahren der Vernetzung unserer Gesellschaft. Telepolis hat sich als Magazin der Netzkultur der Aufgabe verschrieben, zu dieser informierten Debatte beizutragen, indem ein vorurteilsloser Blick auf die so genannten »dunklen Seiten« des Internets geworfen wird.

Armin Medosch und **Janko Röttgers**
Berlin/London Juni 2001

1. Piraten im Reich der Daten

Vom Gold der Inkas bis zum geistigen Eigentum.
Die Geschichte einer verwegenen Metapher.

Piraten

Bernhard Günther

Sie sind unsichtbar. Sie sind überall. Sie verändern die Welt.

So klängen die Werbeslogans, wäre die folgende Piratengeschichte für das Kinopublikum produziert worden. Aber das einzige, was sich die Traumfabrikanten an dieser Geschichte ausgesucht haben, ist der Titel: »Piraterie«, ein verstaubtes Zauberwort aus Hollywoods Klamottenkiste, soll einem ungleichen Duell zu etwas mehr Anschaulichkeit verhelfen. In der Rolle der Guten sehen sich in dieser Geschichte die Vorstandsvorsitzenden, Pressesprecherinnen und Rechtsanwälte der »Copyright Industries« - allen voran Plattenlabels, Filmstudios und Softwareschmieden. Die Rolle der Bösen - mit dieser Besetzung hatten selbst die erfahrenen Studiobosse nicht gerechnet - geht an das Publikum. Und der Plot scheint für die Unterhaltungsindustrie ein ziemlicher Horrortrip zu sein.

Für den Kampf gegen die eigene Zielgruppe haben sich die Copyright Industries auf die »Verteufelung der Piraten« eingeschossen. Bis auf weiteres scheint diese Medienstrategie gut zu funktionieren; vom Feuilleton bis zum Tabloid finden sich mit der größten Selbstverständlichkeit Schlagzeilen à la »Record Moguls Take On Pirates« [1] oder Wie der Geist zur Beute wird« [2]. Doch ein etwas genauerer Blick in das eigene Filmarchiv hatte die Copyright-Industrie davor warnen sollen, ausgerechnet die Helden der ehemaligen Kassenschlager zum Feindbild zu erklären.

Die Rebellen der Leinwand

Von den Anfängen des Kinos bis in die 1950er Jahre war der Piratenfilm eines der präsentesten Genres. Die segelnden Outlaws gehörten jahrzehntelang zu den größten Sympathieträgern und »Quotenbringern« der Filmindustrie. Sea Hawk, der Herr der Sieben Meere, der Rote Korsar, Captain Blood, die Piratenkönigin und wie sie alle hießen trafen mit ihren Piratengeschichten verlässlich den Nerv des Publikums. Als Schreckbild funktionierten Piraten allerdings eher im Kinderprogramm -und nicht einmal dort wirklich: Der schneidige Kapitän Hook, der im Disney-Zeichentrickfilm Peter Pan von 1951 so gerne Cembalo spielt, ist zur Dämonisierung kaum geeignet. Noch knapp fünfzig Jahre später wird er sich viel besser gehalten haben als Peter Pan selbst. Denn der Junge, der nicht erwachsen werden wollte, ist in der Steven-Spielberg-Verfilmung mit Dustin Hoffman und Robin Williams (1991) zum alternden Rechtsanwalt mit Magenkrämpfen aufgestiegen und gewinnt seinen letzten Kampf gegen den Titelhelden Hook nur mit Hilfe von vielen special

effects. Das Piratenlied aus der Disney-Verfilmung bringt die anziehende Ambivalenz des Piratenbildes auf den Punkt:

> A pirate's life is a wonderful life
> You'll find adventure and sport
> But live every minute
> For all that is in it
> The life of a pirate is short. [3]

Im Abendprogramm standen Hollywoods Piraten dann mit aller Deutlichkeit auf der richtigen Seite: Wagemutige Freibeuter nehmen korrupten Spaniern im 15. und 16. Jahrhundert die Piaster und Dublonen ab, die diese den Indios abgepresst haben; edelmütige Korsaren bringen der unmenschlichen Navy der Engländer im 18. und frühen 19. Jahrhundert bessere Umgangsformen bei; tollkühne Volkshelden verpassen der Festung des habgierigen Unterdrückers endlich die verdiente Breitseite. Das Schema des klassischen Piratenfilms ist klar: Die Identifikationsfiguren sind Erroll Flynn und Burt Lancaster im Kampf gegen die Mächtigen - und keinesfalls die spanischen Kapitäne, Gouverneure und Kerkerwachen.

Helden im Ruhestand

Es lohnt sich, einen Blick auf das Ende der Piratenfilm-Ära zu werfen. In den späten 1950er Jahren schien das Genre allmählich Überholt zu sein - Piraten landeten neben den Musketieren der Mantel-und-Degen-Filme im Archiv der Filmgeschichte; die Cowboys ritten noch eine Weile weiter, und Geheimdienstagenten, Marsmännchen & Co. übernahmen allmählich die Leinwand. Das ist kein Zufall. Es war eine wirkliche Ausnahme, als 1958 eine Horde Piraten mit dem Überfall auf eine amerikanische Luxusyacht für Schlagzeilen sorgte (ironischerweise verdiente der Besitzer der vor den Galapagosinseln geenterten Yacht sein Geld ausgerechnet als Rechtsanwalt der Filmindustrie). Doch ansonsten schaute die Welt nach oben: Die Boeing 707 hatte ihre ersten Flüge absolviert und degradierte die mächtigen Ozeane zum schrumpfenden Zwischenraum zwischen den Kontinenten. Vor allem aber war soeben der Sputnik über New York geflogen. Auch das UNO-Abkommen über die Hohe See - ebenfalls 1958 - musste, um up-to-date zu sein, Piraterie bereits auf Flugzeuge ausdehnen. Dort heißt es:

> »Piraterie ist jeder ungesetzliche Akt der Gewalttätigkeit, Freiheitsberaubung oder Plünderung, der zu privaten Zwecken von der Besatzung oder den Fahrgästen eines privaten Schiffes oder privaten Flugzeuges gegen ein anderes Schiff oder Flugzeug oder dort an Bord befindliche Personen oder Güter begangen wird: a) auf offenem Meere, b) an einem außerhalb der Hoheitsgewalt eines Staates gelegenen Orte.« [4]

Der letzte Satz wirkt geradezu prophetisch. Zumal der Sputnik bekanntlich ein Nachspiel hatte: Als der erste Schreck der Amerikaner verflogen war, wurde entschlossen an Plänen zur Errichtung eines neuartigen militärischen Kommunikationsnetzes gefeilt. In der Kategorie »außerhalb staatlicher Hoheitsgewalt« bahnte sich für Weltmeere, Luftraum und Weltraum folgerichtig jener Mitbewerber an, der heute für Piratenromantik zuständig ist: das Internet.

Vom Kassenmagnet zum Feindbild

Statt Werbetexten für das spektakuläre Comeback der Rebellen im »anarchischen« Internet sind von den Rechteinhabern drastische Warnungen zu vernehmen. »Piraterie« ist das marketingstrategische Schlüsselwort, mit dem die Copyright-Industrie die Leichtigkeit, mit dem im Internet digital kopiert, verbreitet und getauscht werden kann, als Gefährdung für Fortschritt und Kultur brandmarkt. Dabei ist zwar nicht direkt von der »Gewalttätigkeit, Freiheitsberaubung oder Plünderung« aus der UNO-Definition die Rede, aber ansonsten wird nicht eben dünn aufgetragen. Schließlich gehört sich das nicht für ordentliche Piratengeschichten. Schon um 1700 spritzte bei Reinhard Keisers Seeräuberoper Störtebecker das Blut aus prall gefüllten Schweinsblasen auf die Bretter der Hamburger Bühnen. [5] Und was altdeutsche Opernkomponisten können, kann die heutige Unterhaltungsindustrie erst recht. Professionelle, weltweit operierende Lobbying-Verbände wie die Motion Picture Association (MPA), die Recording Industry Association of America (RIAA), die International Federation of the Phonographic Industry (IFPI), die Business Software Alliance (BSA) und etliche mehr haben sich explizit dem »Kampf gegen die Piraterie« verschrieben. Eine Leseprobe von der Homepage der RIAA, der Interessenvertretung der amerikanischen Tonträgerindustrie, zeigt, mit welcher Eindeutigkeit dem Piratentum inzwischen allein dämonisierende Assoziationen beigemessen werden - keine Spur mehr vom schwungvollen Rebellentum der alten Seeräuberfilme:

> »Keine schwarzen Flaggen mit Totenkopf und gekreuzten Knochen/ keine Entermesser/ Kanonen oder Dolche kennzeichnen die Piraten von heute. Man sieht sie nicht kommen; es gibt keine Warnschüsse vor den Bug. Aber seien Sie versichert, dass die Piraten da sind - weil es heute jede Menge Gold zu holen gibt (und Platin und Diamanten). Die Piraten von heute operieren nicht auf hoher See, sondern im Internet, in illegalen CD-Presswerken, in Vertriebszentren und auf der Straße. Das Credo der Piraten ist noch immer dasselbe: Warum bezahlen, wenn man so einfach stehlen kann? Das Credo ist so falsch wie es schon immer gewesen ist. Diebstahl ist ungesetzlich, unethisch und im heutigen digitalen Zeitalter leider nur allzu verbreitet. Und deswegen kämpft die RIAA weiter gegen Musik-Piraterie.« [6]

Ein wenig nüchterner erklärt die International Federation of the Phonographic Industry, kurz; IFPI, was Piraterie für sie bedeutet:

> »Der Ausdruck Piraterie bezeichnet im Allgemeinen eine absichtliche Verletzung des Urheberrechts in kommerziellem Ausmaß. Mit Bezug auf die Musikindustrie bezieht er sich auf unerlaubtes Kopieren.« [7]

Gegen das Kopieren rückt die Unterhaltungsindustrie, deren Geschäftsmodell auf dem Kopieren basiert, sehr entschieden zu Felde. Schon zu Zeiten der Musikkassette war die Weltuntergangsstimmung in der Plattenindustrie nicht zu überhören. Im Kampf gegen das Kopieren ist bis heute in alter Hollywood-Manier die Rede vom Kampf der Guten gegen die Bösen. Jay Berman, Chairman der IFPI, ist da wenig zimperlich:

> »Den Diebstahl geistigen Eigentums unterstützen Verbrecherorganisationen. Er nährt den Drogenhandel und andere Schwerverbrechern« [8]

Nur damit jetzt keine Verwechslung aufkommt: Die Internetadressen von Napster, MP3.com und sonstigen von der Musikindustrie verklagten Firmen enden mit .com für

»Commercial« - und nicht mit .co für Kolumbien. Aber weiter im Text des Vorsitzenden der International Federation of the Phonographic Industry:

> »Der heutige Kampf gegen Musikpiraterie ist ein Kampf gegen ein riesiges, organisiertes, illegales internationales Geschäft. Unsere Industrie widmet diesem Kampf große Ressourcen, aber wir brauchen, dringender als alles andere, die Unterstützung von Regierungen. Wir brauchen strengere Gesetze und deren effektive Durchsetzung. Auf dem heutigen globalen Markt kann es sich keine Regierung leisten, einfach zuzuschauen, wie Piraterie ihre Wirtschaft untergräbt, ihre Kultur ausplündert und ihrem internationalen Ansehen schadet.« [9]

Edgar Bronfman, der oberste Manager von Universal und damit Herr über eines der größten Copyright-Imperien der Welt, erklärt den Gesetzgebern dieselbe Gefahr auf seine Art:

> »Im Unterschied zu den Geschenken Gottes und der Natur ist das, was frei ist, nur deswegen frei, weil jemand anders dafür bezahlt hat. Fairness und Gerechtigkeit haben es unserer zivilisierten Gesellschaft ermöglicht, zu überleben und zu gedeihen; während die unseres Alliierten, der Sowjetunion, zersprungen, zerrissen und zerstört ist, weil sie versucht hat, eine Gesellschaftsordnung aufrechtzuerhalten, die zutiefst ungerecht und unfair war.« [10]

Die Geschichte der Public Enemies

Skrupellosigkeit und Goldgier sind klassische Bestandteile des Schwarz-Weiß-Bildes von Piraterie. Beide beschreiben zu Zeiten der historischen Seeräuber aber zunächst einmal die Vorgehensweise der offiziellen Machthaber. »Gold ist etwas Hervorragendes. Mit Gold macht man alles, was man auf dieser Welt wünscht. Mit Gold bringt man sogar die Seelen ins Paradies« [11] - so schreibt kein geringerer als Christoph Kolumbus in einem Brief an seine spanischen Herrscher. Mit anderen Worten: Wäre es nur um Geld gegangen, hätte man sich wohl ganz gut auch andere Titelhelden als Piraten suchen können. Aber der Vergleich der Seeräuber mit den Mächtigen führt geradewegs in die Ursprünge der Piraterie.

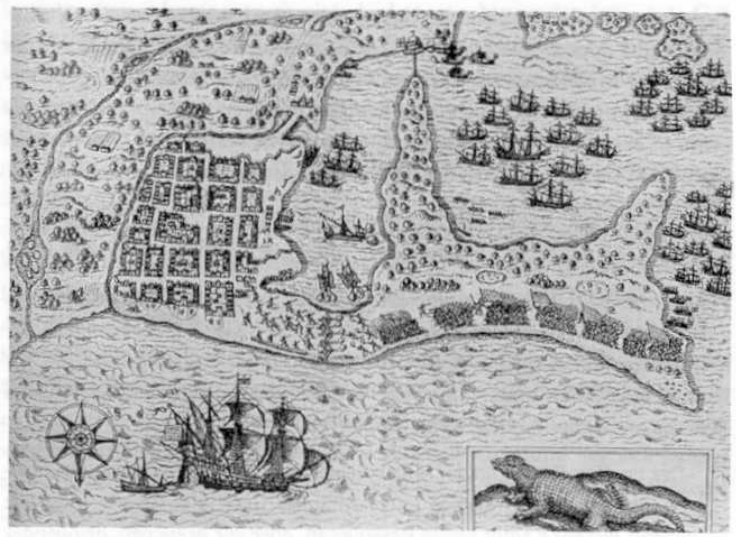
Die Weltmeere wurden zunächst als exklusives Eigentum der mächtigsten Staaten genutzt. Als bekannt wurde, dass Kolumbus 1492 Land im Westen des Atlantiks ausfindig gemacht hatte, einigten sich die beiden großen Seemächte der damaligen Zeit - unter Vermittlung des Papstes - rasch auf eine Aufteilung: Die nicht-christlichen Länder westlich einer Demarkationslinie im Atlantik (ca. 311 Längengrad) sollten Spanien gehören, Östlich davon Portugal. Diesem Vertrag von Tordesillas (1494) folgte 1529 in Saragossa die entsprechende Aufteilung des Pazifischen Ozeans - wiederum als Eigentum von Spanien und Portugal. Beide Staaten bauten zügig ihre Handelsmacht aus: Portugal monopolisierte den Handel zwischen Indien und Europa; die spanischen Conquistadoren fielen brutal in Mittel- und großteils auch Südamerika ein und machten die dortigen Goldbestände zum Motor der spanischen Wirtschaft.

Alle anderen Regierungen ließen das Monopoly-Spiel der beiden römisch-katholischen Weltmächte zunächst unangetastet. Der erste, der aufhörte, die Monopolisierung einfach staunend hinzunehmen, war ein privater Unternehmer: Der französische Kaufmann und Reedereibesitzer Jean Ango schickte mehrere Segler auf die Suche nach den legendären Goldtransportschiffen; der Pirat Jean Fleury schaffte es daraufhin, Kaiser Karl V. ein paar spanische Goldschiffe abzujagen und den Schatz der Azteken 1522 nach Dieppe

umzuleiten. Die Freude in Frankreich war groß, und allmählich regte sich auch auf Ebene der europäischen Regierungen Widerstand gegen die spanisch-portugiesische Weltaufteilung. Der französische König brüskierte schon bald nach Angos Privatinitiative höchst offiziell einen spanischen Gesandten:

> »Die Sonne scheint für mich genauso wie für alle anderen. Ich würde gerne die Klausel im Testament Adams sehen, nach der ich von der Teilung der Welt ausgeschlossen bin.« [12]

50 Jahre später. Halb privat, halb mit dem Segen seiner Königin überfällt der britische Seefahrer Francis Drake das von den Spaniern besetzte Panama. Ein Freibeuter aus dem eher unbedeutenden Inselreich wird 1572 und 1573 zum Schreckgespenst für die spanische Regierung - und zum Nationalhelden für das aufstrebende England. Mit zwei kleinen Segelschiffen und rund 70 Männern macht Drake die Küsten der dominierenden Großmacht seiner Zeit monatelang unsicher. Zum Vergleich: Als 15 Jahre darauf Spanien gegen das immer lästiger werdende England vorrückt, geschieht das mit 130 Schiffen und 30.000 Mann. Die Spanier haben ihre ehrfurchtgebietende Armada: riesige Kahne mit hohen Aufbauten, Hunderte Tonnen schwer, so imposant wie schwerfällig. Die Engländer haben schnelle Segler, die sich leicht steuern lassen und mit weit reichenden Kanonen bestückt sind.



Francis Drake im Kampf gegen die Spanier

Lope de Vega, als junger Dichter Augenzeuge der Vernichtung der Armada durch die englische Flotte (1588), schildert Drake aus spanischer Perspektive als den Drachen der Apokalypse. Zeitgenössische englische Berichte haben dagegen mit Drakes Kampf gegen die mächtigen Staaten keine Probleme, ganz im Gegenteil:

> »Wie es eine Rachegöttin gibt, die insgeheim die Übeltäter verfolgt und : dafür sorgt, dass diese, obwohl von niemandem unter Anklage gestellt, ihrer gerechten Strafe nicht entgehen, so gibt es eine Art Empörung, die tief in der Brust all derer sitzt, denen Unrecht widerfahren ist; und diese werden mit allen ihnen zur Verfügung stehenden Mitteln versuchen, das erlittene Unrecht zu rächen. Insofern scheinen all die großen und mächtigen Leute, die durch außerordentlichen Besitz zur Selbstanmaßung verführt, ihren Untergebenen Unrecht tun und

sie deshalb auch noch verachten, einen sehr gefährlichen Kurs für ihre Sicherheit und ihre Ruhe zu steuern.« [13]

Auf der Seite der Macht

Zur Erinnerung: Aus ökonomischer Sicht ist gerade die heutige Musikindustrie ein Musterbeispiel für Macht. Zumal die Tonträgerbranche mit mehreren spektakulären Musterprozessen innerhalb der Copyright Industries im Internet die Rolle des Pfadfinders übernommen hat, konzentriert sich die folgende Betrachtung auf diesen Bereich. Ökonomisches Kennzeichen Nummer eins: eine ungewöhnliche oligopolistische Marktkonzentration. Gerade einmal fünf Unternehmen - die seit längerem verhandeln, um sich per Merger auf vier zu reduzieren - beherrschen rund 80 % des Weltmarktes für Tonträger. Kennzeichen zwei: eine sehr hohe »vertikale Integration«. Vom vertraglich lizenzierten Copyright über die Aufnahmestudios, die Presswerke, die Marketingabteilungen und die Vertriebsnetze bis zu den CD-Megastores landet im Extremfall die gesamte Wertschöpfung - die Differenz zwischen den wenigen Pfennigen Materialkosten plus den ein bis zwei DM für die Musiker und dem Ladenverkaufspreis der CD abzüglich der Mehrwertsteuer - in den Kassen eines einzigen Unternehmens. Eine ehrfurchtgebietende Wertschöpfungskette. Riesige Kähne mit hohen Aufbauten, Hunderte Tonnen schwer, so imposant wie schwerfällig. Die Newcomer dagegen haben schnelle Segler, die sich leicht steuern lassen und mit weit reichenden Kanonen bestückt sind. Und die Unterhaltungsindustrie schildert aus ihrer Perspektive das Internet als den Drachen der Apokalypse.

Die Musikindustrie reagiert auf die neue Herausforderung

Von der solide gefügten Festung der auf Copyright basierenden Industrien aus werden Angriffe aller Art seit langem gut beobachtet. »Produktpiraterie«, das Nachmachen marken-, patent- oder urheberrechtlich geschützter Handelswaren, ist eine altbekannte Straftat. Das Spektrum reicht von rührend falsch geschriebenen Markennamen auf spottbilligen chinesischen Jogginganzügen bis zur beschlagnahmten Wagenladung gefälschter Rolex-Uhren, die unter einer von Pressefotografen umringten Schweizer Dampfwalze demonstrativ plattgewalzt wird.

Auch »Piratensender« sind ein alter Kampf begriff im Wortschatz von Rechteinhabern. In diesem Fall sind auf Seiten der »Piraten« deutlich (positiv interpretierte) Motive der »klassischen« Piraterie abzulesen - wie die Nichtakzeptanz bestehender Machtverhältnisse oder die Versorgung mit Gütern oder Leistungen unabhängig von der bisher üblichen Kontrolle. Die »Piratenhymne« der britischen Piratensenderszene der 1980er Jahre drückt die Überzeugung und Ausdauer aus, mit der die Betreiber von Piratensendern es teilweise bis zum lizenzierten freien Radio brachten. Verdeutlicht wird auch jenes Merkmal der »Piraten-Szene«, das dafür verantwortlich war, dass viele UKW-Piraten schnell auf das Internet umschwenkten und zu den Pionieren der digitalen Verbreitung von Musik wurden [14]: die Schnelligkeit, mit der sie Lücken im Angebot der bestehenden Distributoren - »trying their best to keep the music down« - erkannten und einen Markt für die entsprechende Musik erreichten, »just because we play what the people want«. Ein paar Ausschnitte, man denke sich dazu einen relaxten Jamaica-Sound:

»Them a call us pirates.
Them a call us illegal broadcasters
Just because we play what the people want.
So them a call us pirates.
Them a call us illegal broadcasters.
DTI try stop us, but they can't.
[...] If they brought down one we build five more strong.
They're passing laws,
They're planning legislation,
Trying their best to keep the music down.
DTI why don't you leave us alone,
We only play the music others want.
One Station, it couldn't run England.
Two Station, they couldn't run England.
Three Station, they could not please the nation.
Everybody want to listen to the free Station.« [15]

»Musikpiraterie« wurde auch schon vor den Zeiten des Internets verfolgt und bezog sich auf das illegale Kopieren von urheberrechtlich geschützter Musik in unterschiedlichen Größenordnungen - von der »Schulhofpiraterie« - ein Ausdruck für das Austauschen von individuell bespielten Musikkassetten unter Klassenkameraden - über eine Hand voll zusammengeschalteter Tapedecks in einem winzigen Studio bis hin zum zwar großindustriellen, jedoch nicht vertraglich lizenzierten CD-Presswerk in einem der »Piratennester« in Fernost. Die aktuelle Medienberühmtheit der alten Seeräuber-Metapher kam trotz dieser Übung im Umgang mit Piraterie aller Arten jedoch unerwartet.

Das Internet wurde bis in die Mitte der 1990er Jahre als Nischenmedium für Freaks abgetan beziehungsweise ignoriert. Für selbstsichere Einschätzungen seitens der Musikbranche sorgten unter anderem die langsamen Dial-up-Verbindungen der frühen Jahre und die so gar nicht mit der bunten Marketingwelt der großen Labels in Einklang zu bringende Nüchternheit von Song-Listen auf FTP-Servern und sonstigen »Piraten-Sites«. Als das Interesse für Musik im Internet unübersehbar wurde, zahlten die Rechteinhaber zunächst einiges Lehrgeld beim Versuch, Musik im Internet kurz und bündig zu verbieten.

In Folge wurde daraus das erklärte Ziel, die Arbeit der Piraten technisch und rechtlich bedeutend zu erschweren. Mit Suchmaschinen - etwa der eher unbescheiden »MP3-Wolf« benannten Software in Verwendung der deutschen Verwertungsgesellschaft GEMA [16] - sollten die Rechtsverletzungen ausfindig gemacht und anschließend rechtlich verfolgt werden. Der nächste Schritt - wir befinden uns ungefähr im Winter 1998/1999 - war die Einsicht, dass es ohne ein eigenes, legitimes Angebot von Musik im Internet nicht gehen würde. Auf Anfang 2000 datiert der Versuch, unter dem wohlklingenden Titel »Rights Protection System« einen Internetfilter um ganz Deutschland zu legen; nach Vorstellungen der deutschen IFPI sollte eine von der Zollbehörde verwaltete Datenbank bestimmen, welche Internetadressen von Deutschland aus abrufbar wären.

Zusätzlich folgten PR-Offensiven, die auf das Schuld- oder Problembewusstsein der Musikhörer abzielten. Zeitgleich warb die Initiative »Copy Kills Music« der deutschen IFPI mit dem keinen Analysen standhaltenden Spruch »10.000 kopierte CDs vernichten eine Nachwuchsband«. Nach wenigen Monaten war die bespöttelte Internetseite dazu wieder offline. Die so genannten Konsumenten redeten offensichtlich lieber über Musik und zeigten nicht besonders viel Verständnis für die Schwierigkeiten der Konzerne. Deren nächster Ansprechpartner war der Gesetzgeber. Insbesondere rund um die Entstehung des Digital Millennium Copyright Act (DMCA) in den USA und der »Richtlinie zur

Harmonisierung des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft« der Europäischen Union (1997-2001) wurde erheblicher Lobbying-Aufwand betrieben, um die Perspektiven der betroffenen Industriezweige möglichst weitgehend in die neue Gesetzgebung einfließen zu lassen. 1999/2000 begann eine neue Größenordnung einschlägiger Gerichtsprozesse in den USA; mehrere Unternehmen der Musikindustrie forderten spektakuläre Summen von den neuen »Music Service Providern« MP3.com und Napster.

Es waren letztlich erst diese Musterprozesse, die den Fall »Musikindustrie versus Piraten« zu einem Dauerthema der Schlagzeilen werden ließen. Im Frühjahr 2001 ist die mediale Übersensibilisierung so weit fortgeschritten, dass selbst die routinemäßige Bekanntgabe relativ normaler Jahresergebnisse der Tonträgerbranche zu Hunderten von Schlagzeilen ä la »Napster drückt CD-Verkäufe« führt. Als Anfang 1999 die CD-Verkäufe um 8 % nach oben gegangen waren, hatten sich die Sprecher von RIAA und IFPI noch beeilt, die Aussagekraft von Zahlen im Allgemeinen zu relativieren. [17] Ein anderes Beispiel für die überhitzte Poker-Atmosphäre des Jahres 2001: Mobilfunk ist einer der wenigen Bereiche der neuen Kommunikationsnetze, in dem immer noch optimistische Umsatzerwartungen formuliert werden - doch statt attraktiver Musikangebote für Handy-Kunden werden weitere Milchmädchenrechnungen bekannt gegeben: »Handy-Klingeltöne kosten Musikindustrie 1 Million Dollar pro Tag.« [18]

Weitere Elemente der üblichen Anti-Piraten-Rhetorik: Das komplexe Ineinandergreifen sämtlicher Interessen im Umfeld des Urheberrechts wird schematisch auf den Showdown zweier Gegner reduziert. Die kleine, schwache Copyright-Industrie auf der einen Seite, die große und gefräßige Telekom-Industrie auf der Gegenseite. Einerseits gibt es zum Verhältnis dieser beiden Marktteilnehmer allerdings bereits weniger reißerische Analysen à la »Content is not king« [19], andererseits gilt die 38,5 Milliarden Dollar pro Jahr umsetzende Tonträgerbranche nicht gerade als Waisenkind. Um so mehr Energie verwendet die Unterhaltungsindustrie daher auf die Darstellung der eigenen Uneigennützigkeit. Eine typische Formulierung dieser Argumentationsstrategie aus dem Mund von Thomas Stein als Manager der Bertelsmann Music Group: »Man kann ja leicht sagen, so große Firmen können schon mal auf ein paar Mark verzichten, weit gefehlt! Der Punkt ist, dass der Künstler letzten Endes am schlimmsten dran ist, weil er kein Geld verdient.« [20]

Unter den Künstlern, die sich gegen die Vereinnahmung als Feigenblatt wehren, befinden sich immerhin Prince und Courtney Love. Es gibt jedoch durchaus Stars, die das Internet genauso sehen wie ihre Labels das tun, die Petitionen unterzeichnen oder gar Rechtsanwälte im Internet auf die Suche nach Piraten schicken - beispielsweise Jean-Michel Jarre, Smudo von den Fantastischen Vier, die Hardrockband Metallica und die Wiener Philharmoniker. Bemerkenswert ist dabei, warum gerade Stars sich für eine starke Kontrolle des Internets einsetzen - anders ausgedrückt, für welch geringen Prozentsatz der Künstler die aus dem Urheberrecht resultierenden Einnahmen überhaupt eine nennenswerte Größenordnung erreichen. Die »Hit-Lotterie« der Musikindustrie hat kaum mehr als zwei bis drei Prozent Gewinner. Die meisten veröffentlichten Alben machen Verlust (beziehungsweise dienen als Visitenkarte), der Rest wird zunächst einmal dazu verwendet, die enormen Marketingkosten einzuspielen. Den Künstlern bleibt infolge der in der Regel ungünstigen Verträge sehr wenig; finanzielle Gewinne aus dem Tonträgergeschäft sind für den Großteil der Musiker vollkommen unrealistisch; viele zahlen drauf. Die von der Industrie verteidigten Gewinne aus dem Urheberrecht sind für die meisten Urheber daher genauso unerheblich wie es den Inkas egal sein konnte, ob der

ihnen von den Spaniern abgenommene Schatz in Madrid, in Dieppe oder auf dem Meeresboden landete.

Die Copyright-Industrie unter Beschuss

»Piraterie ist, wenn man das Werk eines Künstlers stiehlt ohne die Absicht, dafür zu bezahlen. Ich spreche hier nicht über irgendeine Software ä la Napster. Ich spreche über die Plattenverträge von Major Labels.« [21] Die Sängerin Courtney Love gehört keineswegs zu denjenigen, die das Urheberrecht für überflüssig halten würden. Sie rechnet vielmehr detailliert vor, wie weit die selbst stilisierten Piratenjäger und Wächter des Urheberrechts von einer fairen Entlohnung der Urheber entfernt sind.

Hovell Davies

Künstler schließen sich zur Recording Artists Coalition zusammen, um endlich bessere Vertragsbedingungen zu erhalten. [22] 28 Bundesstaaten der USA reichen eine Klage gegen die Musikindustrie wegen illegaler Preisabsprachen bei überteuerten CDs ein. [23] Die EU-Kommission setzt erste Schritte in Richtung eines Kartellverfahrens gegen die Musikindustrie. [24] Die Familien mehrerer Opfer des Columbine-Massakers reichen gegen 25 Firmen der Unterhaltungsindustrie (darunter Nintendo, Sega, Sony und Time Warner) eine Klage über 5 Milliarden Dollar ein; der Vorwurf lautet, dass ohne die Geschäftemacherei mit Gewalt und Sex der Amoklauf der beiden Videogamer nicht stattgefunden härte. [25] Fast zeitgleich rügt eine von der US-Regierung beauftragte Studie die Plattenlabels für Geschäftemachern mit Gewalt in Lyrics. [26] Wie gesagt, klassische Bestandteile des Schwarz-Weiß-Bildes von Piraterie sind Goldgier und

Skrupellosigkeit. Und beide werden zu einem recht dauerhaften Teil des Images der heutigen Piratenjäger.

Die Fortschrittlichkeit der historischen Piraten

Vom Piratenkapitän Hovell Davies ist aus dem frühen 18. Jahrhundert überliefert, dass er seine Mannschaft nach einer Streiterei zur Vernunft ruft: Sie seien nicht aus Rauflust Piraten geworden, sondern um sich an blutsaugerischen Kaufleuten und an grausamen Schiffsführern zu rächen. [27] Kapitän Samuel Bellamy (mit dem Beinamen »der Redner«) versucht 1716 den Kapitän eines geenterten Handelsschiffs zur Mitarbeit auf Seiten der Piraten zu überreden. Es kommt zu keiner Einigung, und Bellamy hält eine Rede:

> »Ich bedaure, dass sie Euch Eure Schaluppe nicht wiedergeben wollen; ich halte nichts davon, irgendjemandem Schaden zuzufügen, wenn ich davon keinen Vorteil haben kann; zum Teufel mit der Schaluppe, wir müssen sie versenken, und sie hätte Euch nützlich sein können. Trotzdem: Ihr seid ein schleicherischer Hund, und ebenso alle, die es hinnehmen, von Gesetzen regiert zu werden, die reiche Männer zu ihrem eigenen Schutz gemacht haben - weil diese feigen Hunde nicht den Mut haben, auf andere Weise zu verteidigen, was sie in ihrer Unehrlichkeit zusammengetragen haben; aber sie seien alle miteinander verflucht: Meinen Fluch über dieses Pack verschlagener Luder, und über Euch, die Ihr Ihnen als ein Posten hühnerherziger Dummköpfe zu Diensten steht. Sie machen uns schlecht, ohne die geringste Zurückhaltung, und dabei ist der einzige Unterschied: Sie berauben die Armen unter dem Mantel des Gesetzes, so, und wir nehmen's von den Reichen unter dem Schutz unserer eigenen Courage. Ist es nicht besser, Ihr seid einer von uns, anstatt diesen Betrügern für eine Anstellung hinterherzulaufen?«

Als der Kapitän darauf antwortet, sein Gewissen erlaube ihm nicht, die Gesetze Gottes und der Menschen zu brechen, setzt Bellamy fort:

> »Ihr seid ein verfluchtes Gewissens-Luder, ich bin ein freier Prinz, und es steht mir genauso zu, der ganzen Welt den Krieg zu erklären, wie es irgendjemandem zusteht, der hundert Schiffe auf See und hunderttausend Männer auf dem Feld hat; und das sagt mir mein Gewissen; ach, was gibt es zu diskutieren mit so weinerlichen Hündchen, die es irgendwelchen Vorgesetzten erlauben, sie nach Belieben übers Deck zu scheuchen.« [28]

Die »Piratenrepubliken« als Vorläufer des Sozialstaats

Mitte des 17. Jahrhunderts. Die staatlichen Justizsysteme basierten auf Folter und Todesstrafe. Die Ordnung im Militär, in Staaten und in Unternehmen war extrem hierarchisch, bei Bestrafungen wurde wenig zimperlich verfahren. Kriege waren an der Tagesordnung.

Zur gleichen Zeit gab es bei den Piraten in Westindien - auf Haiti und Tortuga - geregelte Versicherungsansprüche, ein ausgeprägtes Rechtssystem und eine Herrschaftsform, die um vieles demokratischer aufgebaut war als die der damaligen Regierungen. Es gab eine gemeinsame Kasse für Krankenversicherung und Sozialversicherung. Die Beute wurde unter allen (einschließlich Kapitän) gerecht aufgeteilt.

Zum Vergleich: Die staatliche Navy requirierte ihr Personal nicht selten per Kidnapping und zahlte einfachen Matrosen meistens nichts. Auf Fluchtversuche folgten unmenschliche Strafen. Auch auf Handelsschiffen war die Heuer immer noch

verschwindend gering und die Disziplin unerbittlich. Bei den Korsaren, die sich im Unterschied zu eindeutigen Piratenschiffen immerhin durch einen Kaperbrief als politisch legitimierte Eingreiftruppe ausweisen konnten, behielt der Kapitän von der Beute den vierzigfachen Anteil seiner Mannschaftsmitglieder. Die unabhängigen Piraten schließlich hatten zur gleichen Zeit ein deutlich anderes Geschäftsmodell. Der Kapitän eines Flibustierschiffs erhielt höchstens zweimal so viel wie seine Kampfgefährten. Die Rechte und Pflichten aller waren durch Verträge geregelt. [28]

Der Historiker Clive Senior resümiert: »Im Vergleich zum Dogmatismus ihrer Zeit muss man den Pragmatismus der Piraten einfach begrüßen.« [29] Also noch einmal: Was macht Piraten zu Sympathieträgern? In die Metapher von der Piraterie hat sich durch verschiedene Jahrhunderte eine Idee davon eingeprägt, dass ein menschliches Gemeinwesen nicht immer auf die bestmögliche Art funktioniert - und dass man dem etwas entgegensetzen kann.

Von welcher Position aus operieren »Piraten« heute?

Die Versuche von IFPI, RIAA etc., die »Piraten« begrifflich in der Nähe organisierter Kriminalität dingfest zu machen, haben einen Haken. Sie halten den Eindruck aufrecht, die Industrie habe das Internet noch immer nicht begriffen. Das Internet, das Silicon Valley und die New Economy als untergehendes Sowjetimperium? Die zig Millionen Napster-User als Drogenmafia? Es fällt schwer, über den dramatischen Vergleichen von Jay Berman und Kollegen (s. o.) den entscheidenden Qualitätssprung hin zur heutigen »Piraterie« als Massenphänomen nicht zu vergessen. Nicht, dass es keine industrielle »Piraterie« im großen Stil gäbe; die seit langem von der Industrie bekämpften illegalen CD-Presswerke sind keineswegs aus der Welt. Aber die heutige Ausgangslage von »Internet-Piraterie« ist doch wohl eher umgekehrt: Der ernüchternde Eindruck, dass es im klassischen Musikgeschäft nur noch um Geld geht, [30] wird für eine kritische Masse von Musikfans zum Auslöser für »Piraterie im kleinen Stil«. Die Triumphe der Copyright-Industrie im Gerichtssaal haben ihre Kehrseite im Reißen des Fadens zwischen den Rechteverwertern und ihren Kunden. Welcher Musikfan hat Verständnis dafür, dass das Major Label Universal für jede einzelne CD, die auf der my.MP3.com-Website zugänglich war, 25.000 Dollar Schadenersatz von MP3.com erhalten soll - zumal, wenn Peter Gabriel auf die Frage, wie viel von der Millionensumme denn an ihn als Musiker gegangen sei, nur antworten kann: »Mir ist bislang kein Künstler begegnet, der davon etwas bekommen hätte. Solange Künstler nicht klug genug sind, um sich zusammenzutun und gemeinsam zu handeln, steigen sie nur wieder schlecht aus.« [31] Die von Napster den Labels zur Versöhnung angebotene Dollarmilliarde wird - mit dem Verweis auf den Branchenumsatz von 38,5 Milliarden Dollar pro Jahr - von der Copyright-Industrie als Scherz abgetan. Kurz: der »legale« Teil des Musikgeschäfts scheint sich nur noch um Kommerz zu drehen - und zugleich wird durch eine hemmungslose Schlammschlacht mit Rechtsansprüchen, Millionenforderungen und Milchmädchenrechnungen Geld zu Spielgeld abgewertet. Für viele Fans eine willkommene Gelegenheit, es einmal ohne Geld zu versuchen.

Die Entwicklung von »Musikpiraterie« im Internet

Noch scheint »Filmpiraterie« im Internet aufgrund der großen Datenmengen unrealistisch zu sein. Heiß umkämpft wird der Bereich jedoch spätestens, seit 1999 eine Hand voll Hacker die CSS-Verschlüsselung der DVD-Filme knackte. Um die digitalen Filmscheiben nicht nur auf den von der Unterhaltungsindustrie unterstützten Apple- und PC-Betriebssystemen, sondern auch auf der Open-Source-Plattform Linux abspielen zu können, wurde der industrieeigene Kopierschutz außer Kraft gesetzt. Seitdem tobt ein erbitterter Streit - unter anderem darüber, wie weit es hier um (in vielen Staaten zulässiges) Reverse Engineering oder um schlichte Urheberrechtsverletzung ging. [32]

Eine etwas längere Tradition hat der Kampf gegen »Softwarepiraterie«. Die Business Software Alliance (BSA) gibt auf ihrer österreichischen Homepage 1996 als Beginn des Kampfs gegen die Piraten an, [33] die deutsche BSA konstatiert trotz ihrer Angst-Kampagne (»Sie haben allen Grund, nervös zu sein«) 2001 einen Boom der Internet-Piraterie und verzeichnet 533 stillgelegte Sites. [34] Die über weite Strecken nicht von Kommerz, sondern von Leidenschaft getriebene Warez-Szene verweist auf jenen Bereich, der die Internet-Piraten zu Medienstars gemacht hat und gegen den Film- und Softwarepiraterie geradezu wie Bagatellen wirken: die Musikfans im Internet.

Mit Beginn der 1980er Jahre stellte die Musikindustrie in einer groß angelegten Aktion das Konsumentengeschäft auf digitale Formate um. Die CD (Compact Disc) als Nachfolger der LP war immer noch an physische Datenträger gebunden und ebenso wenig kopiergeschützt wie die analogen Vinyl-Scheiben. Zeitgleich entwickelten Wissenschaftler an der Friedrich-Alexander-Universität Erlangen, ab 1987 dann am dortigen Fraunhofer-Institut für Integrierte Schaltungen (IIS-A) die Komprimierung digitalisierter Klänge. Das Erlanger Team wurde innerhalb der Moving Pictures Expert Group (MPEG) federführend für die Entwicklung des »MPEG Audio Layer-3«, kurz: MP3, in internationalen Standardisierungsgremien. Der ursprüngliche Encoder war klein und wenig benutzerfreundlich - und verbreitete sich explosionsartig. Weitere Programme, die sehr bald als Shareware kursierten, waren CD-Ripper, die Audiodaten vom Tonträger auf die Festplatte kopierten. Als nächstes entfiel mit der billigen Verfügbarkeit von CD-Brennern und beschreibbaren CD-Rs die technische Barriere, die das identische Vervielfältigen digitaler Tonträger ohne Qualitätsverlust als Breitenphänomen verhindert hatte. Vor allem aber ermöglichte das Internet., die so entstehenden Sammlungen von Files aller Art auch ohne den Transport physischer Daten- respektive Tonträger zusammenzuschließen. Es gibt immer mehr Programme, die es Musikfans ermöglichen, via Internet an Musik zu kommen.

Eine gigantische Community, die nicht länger auf den Schulhof angewiesen war, um Kassetten zu tauschen, begann im Internet eine lebhafte Diskussion über Musik. Bald stellten lokale UKW-Piratensender auf Real Audio Stream um. Seit spätestens 1996 gab es Internet Relay Chat Groups (IRC), die sich der Verbreitung von MP3-Files verschrieben. Die Musik fand rasch den Weg vom Usenet zum WWW, vom Textbefehl zur grafischen Benutzeroberfläche, vom Spezialwissen zum Massenphänomen. Immer mehr Browser-ähnliche Programme boten Zugriff auf Musik; inspiriert von IRC und MP3-Suchmaschinen brachte der junge Student Shawn Fanning im Januar 1999 eine wirkliche »Killer Application« ins Spiel. Als die Betaversion seiner Software Napster auf Download.com sofort durchstartete, gründete er im Mai 1999 Napster.com und gab den Anstoß zur steilen Karriere von Peer-to-peer (P2P) Filesharing.

Die Musikindustrie brauchte Monate, um die Neuerung auch nur zu bemerken. Um so schneller reagierten die Hörer: Nach einer Studie der Firma PC Pitstop war im Herbst 2000

die (nicht übermäßig ausgereifte) Software bereits auf fast jedem dritten ans Internet angeschlossenen PC installiert. Laut Firmenangaben greifen auf Napster bis zu einer Million User gleichzeitig zu. Zum Vergleich: Auch AOL als größter Internet Service Provider der Welt hat in Spitzenzeiten kaum mehr als 1,5 Millionen User gleichzeitig im Netz. [35] Vor dem Hintergrund der stark zentralisierten, objektorientierten Tonträgerbranche und des immer noch überaus mäßigen legalen Musikangebots im Netz schössen weitere P2P-Plattformen wie die Pilze aus dem Boden - Gnutella, Scour, Mojo Nation & Co. Und die nächste Überraschung kommt bestimmt.

If you can't beat them ...

»Das Internet verändert unser Leben, verändert Ladenschlusszeiten, verändert alles. Für die Musikindustrie hat Internet Vorteile und Nachteile zugleich, einerseits ist die Musik das einzige Medium, neben Bildern, das man sofort konsumieren kann über Internet. Damit ist ein Vorteil und Nachteil gleichermaßen verbunden. MP3 wird für die Musikindustrie ein sehr, sehr angenehmes, wahrscheinlich sehr zukunftsweisendes Instrument werden, unsere Produkte in den Markt zu bringen.« [36]

Noch einmal Thomas Stein von der Bertelsmann Music Group, aus der Frühzeit der positiven Reaktionen im Frühjahr 2000. Ein halbes Jahr später wird bereits ein Schuh daraus. 31. Oktober 2000. Es ist die Zeit der schwebenden Verfahren der Musikindustrie gegen Napster, MP3.com und gegen andere Abkürzungen der alten Vertriebswege, Die Bertelsmann AG, einer der größten Rechteinhaber der Welt, gibt eine Pressekonferenz. Neben den Managern von Bertelsmann sitzen - die Vertreter des Erzfeindes. Shawn Fanning und Hank Berry, der Gründer und der Geschäftsführer von Napster. Man habe sich auf eine strategische Allianz geeinigt, und Bertelsmann wolle größere Anteile an Napster übernehmen:

> »Das Austauschen von Dateien von Person zu Person hat die Vorstellungskraft von Millionen Menschen beflügelt durch seine Einfachheit, die weltweite Auswahlmöglichkeit von Content und durch die ganzen Aspekte einer Community. Napster hat einer neuen Art der Musikdistribution den Weg gewiesen, und wir sehen darin die Grundlage eines wichtigen und aufregenden Geschäftsmodells für die Musikindustrie. Wir laden andere Plattenfirmen und Verlage, Künstler und andere Industrieteilnehmer ein, an der Entwicklung eines sicheren und auf Mitgliedschaft basierenden Services mitzuarbeiten.« [37]

Keine einfache Angelegenheit, die Musikindustrie auf gemeinsamen (Piraten-)Kurs zu bringen, wie die nächsten Monate zeigen sollten. Und wie vertragen sich die Profitinteressen der Industrie und die Wendigkeit der Piraten?

Piraterie als Geschäft

1547. Heinrich der Achte, König von England, erhalt vom Bankhaus Fugger einen Kredit: 400.000 Carolusgulden - ein Vermögen -, verzinst zu 12 %. Andere Bankhäuser beschweren sich. Für diese unglaublichen 48.000 Gulden an Zinsen pro Jahr wäre es schließlich ein Leichtes gewesen, Piratenschiffe auszurüsten, die die Kreditsumme für den König schon bald im Ärmelkanal aufgetrieben hätten. Es ist nicht mehr zu übersehen; Die eigentlichen Piraten sind die großen Handelshäuser. Bankkaufleute im Hintergrund, die

noch nie eine Schiffsplanke betreten haben, arbeiten mit dem kalkulierbaren Gewinn, den die Seeräuberei ihnen als Investoren bringt. Zugleich verdienen natürlich die Versicherungsunternehmen an den enormen Prämien und die Speditionen an den hohen Frachtsätzen.

In Frankreich funktioniert die Aufteilung der piratischen Gewinnmargen bis weit ins 18. Jahrhundert hinein meist ähnlich. Konsortien von Reedern und Investoren, die die Seeräuberei als lohnendes Geschäft entdeckt haben, zahlen dem König ein paar Prozent Steuern, erhalten dafür einen Kaperbrief, der sie ermächtigt, Schiffe aus verfeindeten Ländern zu plündern, und beauftragen dann Piraten, die zusätzlich zur politischen Rückendeckung auch einen kleinen Anteil von der Beute behalten dürfen. Bei Heinrich VIII. resultiert aus dieser Entwicklung das erste Gesetz gegen Piraterie; zusätzlich wird ein verantwortlicher Vizeadmiral zur Eindämmung des Geschäfts mit der Piraterie beauftragt. [38]

Die Nebenwirkungen des Kampfs gegen Piraterie

Zahlreiche Firmen stehen bereit, um an den Forderungen nach Sicherheit, Kopierschutz und Überwachung viel Geld zu verdienen. Die »technischen Maßnahmen« und »Informationen für die Wahrnehmung der Rechte«, die die 2001 verabschiedete EU-Richtlinie inzwischen dezidiert unter rechtlichen Schutz stellt, werden den gewohnten Umgang mit urheberrechtlich geschützten Files - Texten, Tonträgern, Videos - auf neue Beine stellen. Digital Rights Management (DRM) bietet die Möglichkeit, aus dem von der Copyright-Industrie in den schrecklichsten Farben geschilderten Piratenparadies Internet ein Medium der totalen Kontrolle werden zu lassen. Der US-amerikanische Internet- und Verfassungsrechtsexperte Lawrence Lessig warnt vor dem gerade unter den Apologeten des Internets verbreiteten Glauben an die »Natur« der Information oder der Informationstechnologien. Den statischen Optimismus legendärer Sätze wie »Information wants to be free« [39] oder »The net interprets censorship as damage and routes around it« [40] stuft er als naiven »Is-Ism« ein. Es sei riskant, davon auszugehen, dass das Internet »sei, wie es ist« - denn das Internet sei schließlich nichts als eine Hand voll Protokolle, von Menschen geschaffener Code - der zur Zeit massive Veränderungen erfahre. [41]

Sicher, auch die Gesetzgeber sind sich bewusst, dass die Welt nicht nur aus Rechteinhabern besteht. Und es klingt auch nicht besonders wahrscheinlich, dass die Kunden der Unterhaltungsindustrie massenweise bereit sein werden, zum Hören von Musik einen digitalen Waffenschein und einen Dongle vorzuzeigen. Aber wie tiefgreifend der Umbau der digitalen Welt im Zuge des »Kampfs gegen die Piraten« ausfallen könnte, deuten die 2001 durchgesickerten Überlegungen von Intel, IBM, Toshiba und Matsushita, den Kopierschutz gleich auf der Ebene der generischen Hardware einzubauen. [42] Um von Festplatte C auf Festplatte D zu kopieren, zeigen Sie bitte Ihren Legitimationsausweis. Noch bevor sich der Rauch der auf die vermeintlichen Piraten gerichteten Kanonen verzogen hat, ist die Welt zur Goldkammer der Conquistadoren geworden.

Für »Konsumenten« wie für die Copyright-Industrie kann übrigens ein Blick auf die Musik Anregungen für originelle Auswege aus der verfahrenen Situation bieten. Die Erfolgsgeschichte der Band Grateful Dead begann zum Beispiel, als die Musiker aufhörten, ihren Fans das urheberrechtlich »verbotene« Mitschneiden von Konzerten zu verbieten. Deren Texter John Perry Barlow weiß im Übrigen, dass es zumindest im Bereich

künstlerischen Schaffens ohnehin unmöglich ist, kein »Pirat« zu sein: »How many musicians can honestly say they've never used something that was there before?« [43]

Wie angebracht diese Frage ist, bekommen auch die professionellen Gegner des Kopierens zu spüren; der DRM-Anbieter InterTrust verklagte im Frühjahr 2001 die Kollegen von Microsoft wegen Patentverletzung durch die im Windows Media Player eingebaute Kopierschutztechnik, [44] Eine aus Piraten-Perspektive gesehen vielversprechende Rückkoppelung - doch auch angesichts des immer Öfter unter Hard- und Softwareentwicklern ausgetragenen Spiels der gegenseitigen Patentklagen ist es verfrüht zu hoffen, dass die diversen Auswüchse des Urheberrechts Schutzes einander so weit lahmen werden, dass dazwischen noch Luft für ganz normalen Fortschritt bleibt. Auf jeden Fall scheint es dem Grundgedanken des Urheberrechts - der Belohnung und Förderung von Kreativität - fundamental zu widersprechen, wenn Entwicklung und Fortschritt als Aufgabe allein den Piraten überlassen werden.

Ein letzter Blick in die Vergangenheit - verbunden mit der Hoffnung, dass die plumpe Anti-Piraten-Propaganda wieder der erstaunlichen Vielschichtigkeit Platz macht, die mit »Piraterie« vor Jahrtausenden in Europa verbunden war. Das Schlusswort gehört dem Griechisch-Wörterbuch: »peirates: Seeräuber; von peiráomai: versuchen, sich daranmachen, sich bemühen, streben, unternehmen, wagen; etwas versuchen oder erproben, prüfen, untersuchen oder ausforschen; sich oder sein Glück in etwas versuchen; einen Angriff wagen; den Kampf mit jemandem aufnehmen; in Versuchung führen; sich um die Gunst von jemandem bemühen; um eine Geliebte werben; aus Erfahrung lernen.« [45]

Literatur

[1] Metro, 3. April 2001 (17 cm hohe Titelschlagzeile der Londoner U-Bahn-Gratiszeitung)
[2] Die Zeit, 15. März 2001
[3] Oliver Wallace, Peter Pan. A Pirates Life is a wonderful life, © 1951 Walt Disney Music Company (ASCAP)
[4] Artikel 125 des Abkommens über die Hohe See, Seerechtskonferenz der Vereinten Nationen, Genf 1958
[5] Hans Leip, Bordbuch des Satans. Eine Chronik der Freibeuterei vom Altertum bis zur Gegenwart, Berlin/Darmstadt/Wien: Deutsche Buchgemeinschaft, 1961, S. 364
[6] RIAA, »Old as the Barbary Coast - New as the Internet«, http://www.riaa.com/Protect-Campaign-l.cfm, 10/2000
[7] IFPI, »Whatispiracy?«, http://www.ifpi.org/antipiracy/what_is_piracy.html, 2000
[8] Jay Berman, IFPI Chairman, Musikwoche, 10. April 2000, S. 12
[9] Jay Berman, http://www.grayzone.com/ifpi61099.htm
[10] http://www.infoculture.cbc.ca/ai-chives/newmedia newmedia_05312000_bronfman.phtml
[11] Christoph Kolumbus, zitiert nach Hellmut Diwald, Der Kampf um die Weltmeere, München/Zürich: Droemer Knaur, 1980, S. 131
[12] ebenda, S. 200
[13] Philip Nichols u. a., Sir Francis Drake revived: Calling upon this Dull or Effeminate Age, to folowe his noble Steps for Golde & Silver, London: printed by E.A. for Nicholas Borne dwelling at the South Entrance of the Royall Exchange, 1626 [Ms. von ca. 1592], zitiert nach: Sir Francis Drake. Pirat im Dienst der Queen. Berichte, Dokumente und Zeugnisse des Seehelden und seiner Zeitgenossen 1567-1596,

hrsg. von John Hampden, aus dem Englischen übertragen von Günter Thimm, Tübingen: Horst Erdmann Verlag, 1977, S. 64
[14] Home T, Cocoa Tea, Shabba Ranks, »Pirates Anthem«, Greensleeves Records, 1989; vgl. http://website.lineone.net/~anthonypage/PirAnt.htm
[15] Vgl. GEMA-Mitarbeiter Alexander Wolf; nicht verbunden mit http://mp3-wolf.de/
[16] Brad King, »Despite > Piracyy CD Sales Up«, Wired News, 24. 4. 2000, http://wired.com/news/business/0,1367/35848,00.html
[17] Tim Richardson, »Ringtones cost music industry $1m a day«, The Register 23, 4. 2001, http://www.theregister.co.uk/content/7/18441.html
[18] Des - im Übrigen vom Telekom-Unternehmen AT&T beschäftigten - Andrew Odlyzko, vgl. http://www.firstmonday.dk/issues/issue6_2/odlyzko/
[19] Aus einem Interview mit Thomas Stein (als Managing Director BMG Ariola), http://www.iface.at, aus der Fernsehsendung »Interface 02«, ORF, 30. 3. 2000
[20] Courtney Love in einer Rede bei der Digital Hollywood Online Entertainment Conference, New York, 16. 5. 2000, zitiert nach Salon.com, »Courtney Love does the math«, http://salon.com/tech/feature/2000/06/14/love/index.html
[21] http://www.recordingartistscoalition.com/
[22] http://www.heise.de/tp/deutsch/inhalt/musik/8514/1.html
[23] http://www.spiegel.de/wirtschaft/maerkte/0,1518,114227,00.hlml
[24] Associated Press, 24. 4. 2001
[25] http://www.msnbc.com/news/563947.asp
[26] Leip, a. a. O., S. 413
[27] Capt. C. Johnson: A General History of the Robberies and Murders of the Most Notorious Pirates, Eondon 1724, Kapitel XXVIII. Vgl. Peter Lamborn Wilson: Pirate Utopias, Moorish Corsairs & European Renegadoes. Brooklyn/NY: Autonomedia, 1995, S. 52 f.
[28] Vgl. Leip, a. a. O., S. 277 f. + 242; Peter Eamborn Wilson, a. a. O., S. 145
[29] Clive M. Senior, A nation of pirates: English Piracy in its heyday, New York: Crane Russack, 1976, S. 94. Zitiert nach Peter Lamborn Wilson, a. a. O., S. 68
[30] Vgl. Peter Rantasa, »Alles Napster oder was?«, Profil 13/01, 26, 3. 2001
[31] Auf der Midemnet Konferenz im Januar 2001, http://www.miaminewtimes.com/issues/2001-02-15/music2.html
[32] Vgl. http://www.quintessenz.at
[33] http://www.bsa.or.at/rechtundpolitik/urheberrecht.phtml
[34] http://www.bsa.de
[35] vgl. http://www.heise.de/tp/deutsch/inhalt/musik/3583/1.html
[36] Aus einem Interview mit Thomas Stein (als Managing Director BMG Ariola), http://www.iface.at, aus der Fernsehsendung »Interface 02«, ORF, 30. 3. 2000
[37] Thomas Middelhoff, Bertelsmann, zitiert nach der Presseaussendung der BMG vom 31.10.2000
[38] Vgl. Leip, a. a. O., S. 155, 372, 612
[39] Whole Earth Catalog-Gründer Steward Brand 1984, vgl. http://www.yaie.edu/yup/qyd/media.html
[40] John Gilmore
[41] Lawrence Lessig, Code and other laws of Cyberspace, New York: Basic Books, 1999, S. 24 ff.
[42] CPRM Content Protection for Recordable Media; vgl. »4C retreats in Copy Protection Storm", theregister.co.uk, 4. 1. 2001,

http://www.theregister.co.uk/content/2/15797.html, und »Stealth plan puts copy protection into every hard drive«, theregister.co.uk, 20. 12. 2000, http://www.theregister.co.uk/content/2/15620.html
[43] John Perry Barlow in seiner Keynote Address »The Abolition Of Property In Cyberspace« auf der DDMI Europe in London, 3. 4. 2001, http://www.ddmiglobal.com; vgl. http://www.eff.org/~barlow/barlow.html
[44] John Borland, »Anti-piracy firm sues Microsoft«, CNET News 26. April 2001, http://news.cnet.com/news/0-1005-200-5744735.html?tag=mn_hd
[45] Langenscheidt Griechisch-Deutsch, 1913/1964 (gekürzt)

Bernhard Günther ist Kurator des mica - music information center austria (mit den Schwerpunkten Internet, Urheberrecht, neue Musik, Musikwissenschaft) sowie freiberuflicher Autor für verschiedene Festivals, Verlage und Medien.

Warez World

David McCandless

Du kommst an einem HiFi-Laden vorbei. Im Schaufenster siehst du eine Anlage. Schick, aber teuer. Weit außerhalb deiner finanziellen Möglichkeiten. Unter normalen Umständen würdest du dich nicht weiter dafür interessieren, aber dieser Laden ist ungewöhnlich. Seine Fenster haben keine Scheiben, es gibt keine Alarmanlage. Wenn du die HiFi-Anlage mitnimmst, bedeutet das für den Besitzer keinen Verlust, weil sofort eine andere am selben Platz erscheint. Und was noch viel besser ist: Du kannst die Anlage klemmen und keiner hält dich auf. Denn niemand sieht dich. Niemand wird dir folgen. Niemand wird je erfahren, dass du die Anlage hast. Du wirst nie erwischt. Jetzt mal ehrlich: Würdest du die Anlage mitnehmen?

Das Internet wurde ausschließlich zu einem Zweck geschaffen - zum freien Austausch von Informationen. Information jedoch ist eine einzigartige Ware. Du kannst sie verschicken und eine Kopie für dich behalten. Falls die Information jedoch in der realen Welt einen Wert hat, einen konkreten Preis wie etwa Computersoftware oder kommerzielle Musik im MP3-Format, dann hast du ein Problem. Ein riesiges Problem.

Ein Krieg zweier Welten

Wenn man sich die Versuche der Softwareindustrie betrachtet, das durch das Internet geschaffene Copyright-Leck zu stopfen, und als Gegenstück dazu die Anstrengungen des Undergrounds, seine ausgeklügelten Piraterie-Netzwerke zu erhalten, dann gibt es bei dieser Geschichte zwei ganz gegensätzliche Sichtweisen, zwei unterschiedliche, sich jedoch überschneidende Welten. Auf der einen Seite steht die Welt des Geschäfts, bekannt und langweilig. Die Welt der 15 Milliarden Dollar schweren Softwareindustrie mit all ihren Entwicklungskosten, Marketingabteilungen, Gewinn- und Verlustrechnungen, Rechtsanwälten und Polizisten.

Dem gegenüber steht die Warez World, die bunte, technisch hochgerüstete Unterwelt, in der erfahrene Cracker, plündernde Piratengruppen und fleißige Kuriere die Technologie des Netzes untergraben, um so rund um den Globus elektronische Daten auszutauschen. Diese Welt ist eine Welt der Spannung, des Prestiges, der Paranoia und der Angst. Eine Welt, in der ausgebuffte Cracker die Schutzfunktionen teurer Software knacken, um schon wenige Stunden nach Markteinführung die ersten Kopien ins Netz zu laden. Eine Welt der Möchtegerne und der besessenen Sammler, die ihre Festplatten - ähnlich wie Briefmarkenalben - mit illegalen Programmen vollstopfen, die sie nie benutzen.

Das ist die Welt von Mad Hatter. Sonntagmorgen, irgendwo in Florida. Der 44jährige ehemalige Drag-Race-Fahrer nippt an einem Glas Seagrams Ginger Ale. Er checkt seinen Computer, auf dem die ganze Nacht hindurch automatisierte Scripts liefen. Mad Hatter ist der Rädelsführer einer Gruppe von Softwarepiraten, die sich Inner Circle nennt.

Mad findet keine Fehler, also liest er seine E-Mail. Es sind so um die 30 neue Nachrichten: ein wenig persönlicher Kram, etwas Fanpost, ein paar interessante Informationen, zwei Flames, vier Anfragen. Mad hat einen Shell Account auf einem FTP-Server in Schweden geöffnet. Während sein IRC-Programm pausenlos in einem Fenster läuft, inspiziert er den Inhalt einiger privater Server. Er tippt schnell, legt dabei Verzeichnisse an, wählt Filter aus und verschickt Files von einem Server zum anderen. Während er mit seiner Familie frühstückt, setzt eine neue Welle automatisierter Scripts ein. Mads ISDN-Verbindung erwacht summend zum Leben. Ein unaufhörlicher Strom an Informationen verlässt den Rechner und verschwindet im Äther. Am Ende des Tages wird Mad 100 Megabytes illegaler Warez ins Internet eingespeist haben.

«Die meisten der Produkte, die du im Laden kaufst, kannst du, wenn du mit ihnen nicht zufrieden bist, wieder zurückgeben«, sagt Mad Hatter. »Bei Software geht das nicht.« Warez ist eine Möglichkeit, Programme vor dem Erwerb erst einmal zu bewerten«, ergänzt TAG. TAG (The Analogue Guy) ist Computeranimator und ein weiteres führendes Mitglied des Inner Circle. Wenn du die Software dann wirklich magst und sie häufig nutzt, dann sind wir dafür, dass du sie auch kaufst.«

Auf der anderen Seite der Welt erscheint Kyle an seinem Arbeitsplatz. Das fünfgeschossige Hauptquartier des Netzwerk-Riesen Novell im englischen Bracknell ist eine prächtige Erscheinung. In Kyles Büro hingegen regiert das Chaos. In den Regalen stapeln sich die Computer: schimmernde Desktops, ausgeschlachtete Mini-Tower und ramponierte Server, alle Anschlüsse mit DAT-Recordern und CD-ROM-Brennern belegt, jede Erweiterung mit zusätzlichen Festplatten zugeknallt. In der Ecke steht ein Metallregal, vollgepfropft mit Monitoren, Video-Equipment und Ersatz-Keyboards.

In Schlips und Anzug mag der 24-jährige Ingenieur für Netzwerksysteme wie jeder x-beliebige Desk-Jockey aussehen, sein Job jedoch ist einzigartig und hoch spezialisiert. »Ich spiele den ganzen Tag im Netz«, erzählt Kyle, »und werde dafür auch noch bezahlt.«

Kyle ist ein Undercover-Internet-Detektiv und als solcher ein wichtiges Mitglied in Novells Internet Piracy Unit (IPU), einer weltweit operierenden Gruppe von »technischen Ermittlern«, die rund um die Uhr das Netz durchkämmen. Immer auf der Suche nach Leuten wie Mad Hatter, die mit unlizenzierter Software handeln - um diese letztlich auffliegen zu lassen, Kyle verbringt seine Arbeitswoche damit, die Warez World zu infiltrieren, Beweise zu sammeln. Dabei gibt er sich als alles Mögliche aus: als Trader (jemand, der Software hin- und herschiebt), Kurier, Cracker, Newbie (Neuling), Lamer (jemand, der keine echte Ahnung hat), Lurker (der nur passiv im Hintergrund abhängt und beobachtet) oder Leecher (der nur Warez zieht, der Szene aber selbst nichts zurückgibt).

Napster hat der Welt gezeigt, dass es im Internet ein riesiges Copyright-Leck gibt. Dabei bedeutet diese neue Welle von Filesharing-Technologien wie Napster nur eine neue Dimension in der inzwischen uralten Schlacht zwischen Software Industrie auf der einen Seite und Softwarepiraten auf der anderen. Eine Schlacht, die mit den Bulletin Boards und Modems der frühen 90er begann, dann das Internet erfasste und heute auch die Profit-Piraten und Fälscher in Osteuropa und Fernost einschließt.

Napster gab der bis dato jungfräulichen und selbstgefälligen Musikindustrie einen ersten Eindruck davon, wie die Kehrseite der Informationsrevolution aussehen kann. Ein böses Erwachen, wie schon zuvor für Microsoft, Novell & Co., die allesamt feststellen mussten,

dass die meisten Gesetze nichts mehr wert sind, sobald sie mit dem Netz in Berührung kommen. Und dass, wenn die Möglichkeit existiert, Sachen unentgeltlich aus dem Netz zu ziehen, ohne dabei erwischt zu werden, die Leute diese auch nutzen.

In Kyles Welt sind die Regeln klar. Software ist eine wertvolle Ware. Software ist Geld. Anwendungen wie AutoCad, 3D Studio Max, Microsofts Server-Lösungen oder Novell Netware kosten Tausende von Dollar das Stück. Piraterie ist daher Diebstahl. Die Industrie behauptet, durch Piraterie jedes Jahr 15 Milliarden Dollar zu verlieren, wobei der Großteil des Verlustes dem Einsatz unlizenzierter Kopien in Firmennetzwerken sowie der organisierten Fälscherei in Osteuropa und Fernost angelastet wird. Fünf Milliarden jedoch versickern durch das Internet, fünf Millionen pro Tag allein durch die Warez World.

In Mad Hatters Welt lacht man über diese Zahlen. Preise und verlorene Einnahmen bedeuten hier nichts. Wenn die kopierte Software solche ist, die man sich nie gekauft hätte oder die man sich nie hätte leisten können, wie kann diese dann als »entgangene Verkäufe« aufgerechnet werden?

Das Usenet: Der Ort für Gelegenheitspiraten

An den Ausläufern der Warez World befindet sich, ähnlich einer großen Schleuse, die sich ins Meer ergießt, das Usenet. Von den Zehntausenden Diskussionsgruppen des Usenet befassen sich ca. 100 mit Piraterie. In alt.binaries.warez.ibm-pic werden Dateien zum Download angeboten - unentgeltlich und für jedermann. Ohne jedes Problem. Du musst nur deinen Newsreader anwerfen, ihn auf das entsprechende Forum ausrichten, und schon erscheint auf deinem Bildschirm eine Liste der neuesten Software, die sich liest wie ein Homeshopping-Katalog. Du brauchst nur noch runterzuladen. Wenn dir die Atmosphäre gefällt, kannst du der Community beitreten und selber Sachen beisteuern.

Die Warez im Usenet sind alt, vielleicht ein paar Tage oder ein paar Wochen. Den neuesten Kram findest du in den hektischen Trade Rooms des Internet Relay Chats (IRC). Allerdings bietet das Usenet einen guten Einstieg, vor allem für Newbies und Gelegenheitspiraten - oder auch für jeden, der eine ganz spezielle Software sucht. In einer typischen Woche werden Adobe Photoshop, Microsoft Office, 3D Studio Max angeboten, außerdem die neuesten Versionen von Microsofts Windows. Darüber hinaus gibt es Alpha- und Beta-Versionen, alle unglaublich früh vor dem eigentlichen Veröffentlichungsdatum, sowie Web Tools, Netzprogramme, Spiele und Utilities. Eben alles, was sich der fortschrittliche Computernutzer wünscht.

Die Bandbreite der Postings reicht von solchen mit einigen Bytes (für den Crack eines Kopierschutzes etwa) bis hin zu Hunderten von Megabytes für das komplette ISO-Image einer CD. Früher einmal mussten diese Datenmengen für die Modems in kleine Pakete zerteilt werden. Heute, im Zeitalter von xDSL und Kabel-Modems, fließen hier jeden Tag Gigabytes von gerade erst illegal kopierten Daten durch.

»Ein Spiel für Besessene«

»Wir gehören zum Ende der Warez-Fütterungs-Kette, die damit keinen Profit macht«, behauptet TAG. Die Warez-Cracker, -Händler und -Sammler kopieren Software nicht, um damit Kohle zu machen. Sie tun es, weil sie dazu in der Lage sind. Je ausgefeilter die Kopierschutzprogramme der Hersteller werden, desto mehr Spaß macht es den Piraten,

diese zu knacken. Ist das Diebstahl? Nein, eher ein Spiel, ein verrückter Wettbewerb. Es ist ein Hobby, ein Akt unblutigen digitalen Terrorismus. Es bedeutet: »Fuck You Microsoft!« Es geht darum, als erster zu haben, was andere noch nicht besitzen.

»Es ist ein Spiel für Besessene«, erklärt Mad Hatter. »Mein Computer ist rund um die Uhr online. Als ich aus Krankheitsgründen längere Zeit nicht arbeiten konnte, war es der Kitzel beim Uploaden massiver Datenmengen, der mich motivierte. Ich habe vier Monate hintereinander mindestens 40 Megabyte pro Tag geladen.«

Warezheads können nicht schlafen, bevor sie ihre Schatztruhe nicht mindestens mit einer Anwendung pro Tag angereichert haben. Und der eigentlich Witz dabei ist der, dass sie dieses Java Development Kit oder jenes Photoshop Piug-In eigentlich gar nicht brauchen. Ihr Spaß besteht vielmehr darin, ein neues Unterverzeichnis zu erstellen und dann das gut verpackte Zip-File sauber und ehrfürchtig in ihre Sammlung einzugliedern. Vielleicht installieren sie die Software ja sogar. Um dann, geistig völlig abwesend, ein wenig mit den Toolbars und Paletten herumzuspielen, bevor sie alles verstauen und nie wieder anrühren. Mad Hatter kennt diese Gefühl: Wir erleben das jeden Tag. Leute betteln um etwas, nur um damit > ihre Sammlung zu vervollständigen*. Es gibt ne Menge Lamer da draußen!«

Usenet ist ein Magnet für besagte Lamer. Nach gängigem Netz-Vorurteil (dis)qualifiziert sich jeder, der AOL benutzt, automatisch als ein solcher. Andere Kardinalsünden sind das Uploaden einer Virusverseuchten Datei (schlampig und gefährlich), »Me too«-Postings als Anhängsel an die Bestellung anderer (Verstopfung der Bandbreite), das Verschicken von einzelnen Discs anstatt der ganzen Veröffentlichung (ärgerlich), das Verschicken von OBZs (One Big Zip) anstelle sauber fragmentierter Teildateien (schlechtes Karma für diejenigen, die einen unzuverlässigen Server haben). Als größtes Vergehen gilt in der Szene allerdings die Offenlegung geheimer FTP-Sites oder versteckter Server. Schließlich schauen die Bullen jederzeit zu.

Wir haben schnell mitbekommen, wie gefährlich Suchmaschinen a la Altavista sind«, erklärt TAG. »Bei 75 Prozent der Leute, die Warez verschickt haben, konnte man damit ziemlich einfach die richtigen E-Mail-Adressen rauskriegen.« Da ihn dies beunruhigte, hackte sich TAG in den Programmcode von Forte Agent. Bei diesem handelt es sich um einen sehr gebräuchlichen Newsreader, der zuvor schon gecrackt worden war, um so minderwertiger Shareware auszuweichen. TAG befreite diese Version vom X-Newsreader-Header. Dieser Eingriff garantierte den Postern größere Anonymität. Als Nebeneffekt konnte durch den Patch der Anteil an Spam um zwei Drittel gesenkt werden. »Dieser Hack fand selbst bei Leuten, die mit Warez nichts zu tun haben, so viel Anklang, dass Porte ihn letztlich als Feature in Agent integrierte«, erzählt TAG stolz. »Ich glaube allerdings nicht, dass sie uns dafür würdigen werden.«

Eine Zeit lang machte es sich der Inner Circle zur Aufgabe, die einzelne Warez Groups zu betreuen und zu moderieren. Sie veröffentlichten ihre eigene Warez-FAQ, bei der es drei Regeln gab - gutes Benehmen, gute Nutzung der Bandbreite und gute Warez -, und hofften, dass die Leute sich daran halten würden. Aber bald merkten sie, so wie auch die Software firmen, dass die Einführung einer gewissen Ordnung in einer solchen Wüste der Gesetzlosigkeit schlicht unmöglich war. »Der Versuch, die Massen zu erziehen, hat uns ausgebrannt«, meint Mad Hatten

Statt sich weiter zu verschleißen erstellte der Inner Circle daraufhin die Interesting Parties List (IPL), eine Liste von garantiert hochklassigen, Lamer-freien Newsgroups, in denen ausgewählte Mitglieder ihre mit Pretty Good Privacy (PGP) verschlüsselten Warez verschicken können. Diejenigen, die auf dieser Liste stehen, erhalten monatlich ein neues

Passwort zur Entschlüsselung der Software. Die einzige Voraussetzung, um in eine solche Liste aufgenommen zu werden, ist eine annehmbare Kenntnis hinsichtlich PGP. »Wenn sich schon jemand entscheidet, verschlüsselt zu posten, dann bedeutet das hoffentlich auch, dass derjenige nicht komplett inkompetent ist«, meint TAG. Selbst heute, Jahre nach ihrer Einführung, wird auf der IPL immer noch gehandelt.

IRC: Das Handelszentrum der Warez World

Für die Handelsbedürfnisse eines großen Teils der Warez World sind die verschlüsselten Usenet-Posts inzwischen allerdings zu langsam und unzuverlässig. Sie haben sich stattdessen dem Internet Relay Chat (IRC) zugewandt. Das IRC ist das Handelszentrum der Warez World, eine Art Fusion aus Vollzeit-Devisenbörse und Straßenmarkt.

Im IRC gibt es Hunderte von Chaträumen für Software, bei der die Urheberrechte verletzt wurden - FreeWarez, Warez4Free, WarezSitez, AudioWarez, WarezGamez. In den Zeiten vor Napster war hier der Handelsplatz der MP3-Community. Es gibt private Chatrooms, versteckte Treffpunkte und Piratenparties, bei denen nur geladene Gäste Zutritt haben. Die Community ist eine schaurige Mischung aus realen Menschen und »Bots«. Letztere sind automatisierte Macros mit eigenen Persönlichkeiten und Eigenschaften, ähnlich den animierten Figuren in Computer-Rollenspielen. Du musst nur einen Bot antippen und schon kann es dir passieren, dass du umgehend bei einer FTP-Site irgendwo im Äther landest. Tipp einen anderen an und du erfährst den neuesten Warez-Klatsch. Manche Bots fungieren als Barkeeper, bei denen sich die Teilnehmer gegenseitig virtuelle Drinks bestellen oder sich auf eine Zigarette einladen können.

Im IRC gibt es immer die neuesten und frischesten Releases. Allerdings sollte man sich nicht dem Irrglauben hingeben, dass es sich hier um eine Wohltätigkeitsveranstaltung handelt. Für jedes kleine Stück Software muss bezahlt werden - mit Software. Je aktueller die Anwendung, desto höher der Wert. Die ultimativen Tauschwerte sind die Zero Day Warez - also Software, die innerhalb der letzen 24 Stunden veröffentlicht wurde, bei Bedarf auch gecrackt.

Der Handel mit Zero Day Warez erhöht automatisch deine Reputation in der Szene. Wenn du gute Kontakte und eine schnelle Netzverbindung hast, kannst du damit den Status erwerben, sofort Sachen von einem exklusiven Server zu ziehen. Oder du erhältst die Logins und Passwörter für die Elite-FTP-Sites. Vielleicht wirst du sogar in die Reihen so mächtiger Kartelle wie Razor 1911, Class, Paradigm, Siege, Xforce oder RiSC aufgenommen.

»Zero Day-Sites sind wirklich eine Sache der Elite«, erklärt Inner Circles bekennender Elitevertreter TAG. »Zugang erhalten nur Leute, die mehrere hundert Megabyte pro Tag bewegen können. Meist handelt es sich dabei ausschließlich um geladene Gäste. Dem durchschnittlichen Warez-Händler im IRC bleibt der Zugang verschlossen, es sei denn, er investiert eine Menge Arbeit in die Sache.«

Beim Handel mit Zero Days wird viel betrogen. Der direkte Wettbewerb zwischen den Gruppen führt häufig zur Vernachlässigung der ansonsten in der Szene üblichen Sorgfalt. »Man kriegt zum Beispiel eine Menge von Erstveröffentlichungen, die nur schlecht gecrackt sind«, berichtet TAG. »Einfach, damit jemand diese Erstveröffentlichung für sich verbuchen kann. Zwei Tage später bekommt man dann eine gecrackte Version, die auch funktioniert.«

Ein Stufe tiefer in der Kette finden sich die Drop Sites, wo man im Austausch gegen Uploads frische Warez bekommt. Manche der Drop Sites laufen auf den privaten Rechnern der Trader, andere nutzen gehackte Regierungs- oder Firmen-Großrechner, Shareware Mirror Server und Uni-Netzwerke. Häufig sind diese Drop Sites nur für 24 Stunden oder am Wochenende am Netz, wenn die Administratoren zu Hause sind und niemand die Logs überwacht.

Das IRC organisiert und reguliert sich selbst. Viele der Trader sind befreundet. Der Ton im Chat ist höflich und wohl überlegt. »Grüße. Habe 1,5 Gigs auf anonymer Tl, Zugriff ab jetzt, /msg me for more info. Lamer unerwünscht. Thanx.«

»Keiner, der zur echten Warez-Szene gehört, ist hier aus Profitgründen«, meint ein als Diamond bekannter Trader. »Wir machen das hier aus genau demselben Grund, aus dem andere 70 Meter weite Sprünge mit dem Fahrrad machen. Es geht uns nur ums Prahlen und darum, cool zu sein. Außerdem lernt man in der Szene viele neue Freunde kennen, was für mich das Wichtigste ist!«

»Ein Klima der Angst schaffen»

Wie in jeder anderen Untergrundszene herrscht auch in der Warez World Paranoia. Man muss ständig aufpassen, wer sich als Freund ausgibt. In seinem Büro bei Novell überwacht Kyle jeden Tag die einschlägigen Foren, checkt Usernamen und Dialoge, in der Hoffnung, genug Details und Beweise zu finden, die eine Verhaftung rechtfertigen würden.

Es gab allerdings Zeiten, in der es der BSA (Business Software Alliance, ein Verband der Softwareindustrie zur Bekämpfung von Raubkopien und Softwarepiraterie) eher um die »Ausrottung der Piraterie« ging als um das Fangen einzelner Piraten. Als dieser Plan scheiterte, weil Aufklärung und Appelle ans (Schuld-)Bewusstsein nicht fruchteten, ging man dazu über, die Szene einzuschüchtern und exemplarisch hohe Strafen anzudrohen. »Unsere Strategie ist es, eine kritische Masse an Verurteilungen zu erwirken«, sagt der ehemalige Leiter von Novells Anti-Piraterie-Abteilung, Martin Smith, »Erst greifen wir uns ein paar der Leute, die solches Material downloaden, so genannte Gnats. Dann schnappen wir uns ein paar der größeren Fische, die besser organisiert sind. Was wir wollen, ist ein Klima der Angst zu schaffen!«

Im Resultat bedeutet das pro Jahr zwei bis drei heftige Schläge für die Warez World. In den letzten Jahren verhaftete die BSA mehrere Trader in Kalifornien. Sie haben Studenten hochgenommen, die von ihren College-Servern im MIT operierten. Und mit Hilfe der örtlichen Polizei haben sie in Holland, Südafrika und Chile Türen eingetreten und Wohnungen gestürmt. Kyle war bei ein paar dieser Aktionen dabei. Um sicherzustellen, dass keine Beweismittel auf den Rechnern zerstört werden.

Einer seiner ersten Einsätze fand 1996 in Zürich statt. Für Novell war der Fall damals ein »einschneidender Schlag gegen Personen und Organisationen, die im Internet unlizenzierte Software vertreiben«. Dabei handelte es sich um einen 27jährigen Computertechniker, der sich - hilfreich für die Ermittler - The Pirate nannte. Er hatte eine eigene FTP-Site, die bis zum Platzen mit Warez vollgestopft war, darunter unlizenzierte Software von Novell im Wert von 60.000 US-Dollar, sowie die inzwischen obligatorischen Anleitungen zum Bombenbasteln. »Er war einer dieser neuen Sorte von Warez-Typen, die im Internet Werbung machen«, erzählt Kyle. »Seine Files konnte man per E-Mail anfordern.« Kyle gab sich als Trader aus, unterwanderte die Site, sammelte Beweise und übergab diese schließlich der Schweizer Polizei.

Eine weitere Razzia der Polizei betraf das Hauptquartier einer BBS namens M-E-M-O. Geleitet wurde diese BBS von einem Kollegen des Piraten mit dem Spitznamen The Shadow. Unglücklicherweise befand sich dieser zum Zeitpunkt der Razzia gerade mit seinen Eltern in Urlaub. Als die Familie zwei Wochen später zurückkehrte, fand sie eine eingetretene Wohnungstür vor und musste zusehen, wie der Sohn abgeführt wurde.

Verhaftungen wie diese waren zum damaligen Zeitpunkt typisch für die Vorgehens weise der BSA. Inzwischen gibt es jedoch so viele neue, »unbeherrschbare« Technologien, dass die Ermittler nicht mehr Schritt halten können. »Wir haben zunehmend Probleme mit Auktions-Seiten wie etwa Ebay«, gesteht Matt Thomsett, seines Zeichens neuer Ami Piracy Manager bei Novell. »Unseren Schätzungen zufolge sind in den ca. 90 Prozent aller von Ebay in den Staaten angebotenen Novell-Produkte illegale Kopien.« Microsoft geht mit aller Macht gegen 7500 Postings auf diversen Auktions-Sites vor, in denen gefälschte Software angeboten wurde.

Gleichzeitig erkennen auch Regierungen das Problem des Datenschmuggels. Der Aufschwung von E-Commerce hat mehrere westliche Staaten dazu veranlasst, so genannte Cybercrime Squads (klingt gut, oder?) ins Leben zu rufen, nach der Devise: »Hey, geht uns da etwa Steuerkohle durch die Lappen?!« Allerdings gibt es da immer noch das Problem der »Grauzonen-Staaten«.

Grauzonen und Geheimbünde

»Alles, was man braucht, ist ein Server in einem Land, in dem es keine Gesetze gegen den Diebstahl von Urheberrechten gibt, und davon gibt es reichlich«, erläutert Martin Smith. »Ein solches Land, welches über ein für diese Zwecke ausreichendes Telefonnetz verfügt, reicht, um Hunderte Verhaftungen im Westen zunichte zu machen.«

Nehmen wir ein Beispiel: Ein von einer US-Firma hergestelltes Programm wird über einen Router in Kanada an einen Server in Südafrika geschickt, von wo es von einem aus Deutschland operierenden Norweger - welcher wiederum einen anonymen Remailer in den Staaten benutzt - runtergeladen wird. Danach wird alles in Bulgarien auf CDs gebrannt, die dann in Großbritannien verhökert werden. Wie soll man bei so einem Wirrwarr eine Anklage stellen?«, fragt Smith. »Das alles ist ein juristischer Albtraum!«

Diejenigen, die aus Profitgründen Piraterie betreiben, sind relativ leicht aufzuspüren. Man muss nur den Spuren nachgehen, die bei der Bezahlung mit Kreditkarten im Netz entstehen. Doch bei Tradern vom Schlage des Inner Circle, die nach Robin-Hood-Manier Software frei ins Netz stellen, liegt der Fall anders. »Wenn jemand da draußen ist, der ausreichende Ahnung davon hat, mit welchen technischen Mitteln man ihn lokalisieren kann, dann ist es wohl nicht zu viel behauptet, wenn ich sage, dass dieser sich durchaus erfolgreich > verstecken< oder aber ein System nutzen kann, das sein Aufspüren unmöglich macht«, meint Kyle. »Rein technisch ist es für diese Leute kein Problem, ihre Nachrichten um die ganze Welt > hüpfen* zu lassen, wahrend wir wie angestochen in der Weltgeschichte herumrasen.«

Die erfahrensten und verschwiegensten Piratengruppen sind gleichzeitig auch die mit dem höchsten Prestige: Razor 1911, DOD, Pirates With Attitude (PWA). Diese »Geheimbünde« haben eng verknüpfte Strukturen aufgebaut, die Mitglieder dieser Clubs kennen sich zumeist schon seit Jahren. Sie betrachten sich als gute Freunde, und das, obwohl sich die meisten von ihnen, wenn überhaupt, nur sehr selten treffen. Die wahren Identitäten bleiben selbst untereinander geheim.

Diese Gruppen haben ihre eigene Mythologie, auf inoffiziellen Fanpages feiern sie ihre größten Coups und Siege. Des Weiteren findet man auf diesen Seiten sehr schmeichelhafte Biografien, ellenlange Aufsätze über die Geschichten der Gruppen sowie Nachrufe auf diejenigen, die von den Bullen geschnappt wurden (We feel for ya!«). Mitglied einer solchen Gruppe zu werden ist alles andere als einfach. Positionen werden nur dann frei, wenn ein Mitglied aufhört oder erwischt wird, bei Erweiterung des Operationsfeldes wird abgestimmt. Reputation ist alles! Wenn du nicht schon einen Ruf in der Szene hast, kannst du es vergessen!

Sogar Kyle kann eine gewisse Bewunderung nicht verbergen. »Manche dieser Leute sind unglaublich talentiert«, gesteht er. »Die Logik und die Organisation, die hinter diesen Verbindungen stecken, sind atemberaubend.«

Die Reaktion der Piraten, die auffliegen, spricht dabei Bände. Wenn Kyle mit den Kollegen von der Polizei eine Wohnung stürmt., sieht er keine Angst. Noch nie hat er erlebt, dass ein in die Ecke getriebener Pirat aus dem Fenster springen wollte oder versuchte, seine Festplatte die Toilette runterzuspülen. »Du stürmst da rein und alles, was sie sagen ist: >Oh!<. Sie sind deprimiert, es ist, als ob sie sich ergeben. Sie wissen, dass sie überlistet wurden und dass das Spiel jetzt vorbei ist.«

Auch Dongles bieten keinen Schutz

Die Alternative zu Razzien von Sonderpolizei heißt Einbruchsicherung. Die Entwicklung eines Kopierschutzes, der sich nicht cracken lässt. Aber genau das ist der Milliarden Dollar schweren Software Industrie bisher nicht gelungen - obwohl sie es immer wieder versucht. Vergleichen wir einmal eine Einrichtung in der realen Welt, deren Aufgabe es ist, etwas Wertvolles vor dem Zugriff Unbefugter zu bewahren - eine Bank etwa -, mit der Aufgabe der Programmierer, Einbruchsicherungen für Programme zu entwickeln, dann wird deutlich, das Letztere mit einem ganz entscheidenden Nachteil kämpfen müssen.

Üblicherweise ist es immer nur eine Gruppe von Räubern, die in eine Bank einsteigt, und diese hat auch nur einen Versuch. Nun stelle man sich aber ganze Armeen von Räubern vor, in den verschiedensten Ecken der Welt, und alle greifen zeitgleich ein und dieselbe Bank an. Und das nicht nur einmal, sondern immer und immer wieder. Man stelle sich weiterhin vor, dass diese Einbrecher-Gangs miteinander wetteifern, wer die Bank wohl als erster knackt. Man stelle sich außerdem vor, dass einige der Räuber technisch so beschlagen sind, dass sie die Alarmanlage, den Safe, ja vielleicht sogar die Bank als solche hätten bauen können. Und dass sie vorher schon Hunderte von Banken mit exakt demselben Sicherheitssystem geknackt haben. Und dass sie bei jedem Einbruch etwas dazulernen können, weil sie nie gefasst werden. Kein Sicherheitssystem könnte so einem Ansturm widerstehen.

Die Lösung, mit der die Software Industrie einem effektiven Kopierschutz bis dato am nächsten kommt, ist ein Hardwareschlüssel, auch Dongle genannt. Bei diesem handelt es ich um eine äußerst knifflige Kombination aus Hard- und Software. Anfragen an den Dongle sind in der untersten Ebene in den Code der Software eingebaut. Wenn der Dongle nicht in den Computer gestöpselt wird, läuft auch die Software nicht. Und ohne die Software ist der Dongle allenfalls als Briefbeschwerer zu gebrauchen.

»Der Dongle wird vielleicht alle 150 Mausklicks angewählt, oder jedes Mal, wenn man etwas druckt oder wenn man für den Desktop-Hintergrund eine bestimmte Farbe wählt«, erklärt ein Dongle-Experte. Wenn die Antwort auf die Anfrage falsch ist oder die Anfrage

nicht erwidert wird, dann schaltet sich das Programm automatisch ab. Zur zusätzlichen Sicherung ist der Datenaustausch zwischen Software und Dongle in uncrackbaren Algorithmen verschlüsselt. Außerdem sorgt eine eingebaute Sicherung dafür, dass der Dongle sich beim Versuch, ihn mechanisch zu öffnen, selbst zerstört. Nach Ansicht des Experten müsste man schon ein Elektronenmikroskop benutzen, um den Algorithmus aus dem Wirrwarr herauszufiltern.

Der größte Anbieter auf dem Dongle-Markt ist die Firma Rainbow Technologies, deren Sentinel-Hardwareschlüssel bei 55 Prozent aller geschützten Software eingesetzt wird. Insgesamt gibt es auf der Welt acht Millionen Sentinel-Dongles, die mit acht Millionen Rechnern verbunden sind. Die Firma selbst beschreibt ihr Produkt als Wirkungsvollsten Schutz vor Softwarepiraterie, den es auf der Welt gibt«. Diese Aussage dürfte von der weltweiten Cracker-Gemeinde als Weckruf verstanden werden, falls es eines solchen überhaupt bedurfte.

»Heutzutage ist ein Kopierschutz alles andere als einfach zu knacken«, meint Inner Circles Cracker TAG. »Die Softwareindustrie setzt alles daran, ihre Sachen kopiersicher zu machen. Doch das macht es für die Leute, die einen Ruf in der Szene haben, umso interessanter.« Der logische Ansatz, ein Dongle zu cracken, ist der, eine Art Pseudo-Dongle zu kreieren, einen im Speicher versteckten Code-Klumpen also, der sich als Hardwareschlüssel ausgibt und auf alle Anfragen die korrekte Antwort gibt. Um einen solchen Pseudo-Dongle zu konstruieren, müsste ein Cracker theoretisch alle Informationen, die zwischen Computer und Dongle ausgetauscht werden, überwachen und registrieren, um daraus dann eine unfehlbare Frage/Antwort-Tabelle zu erstellen.

Unglücklicherweise ist es so, dass es auf eine sechs Zeichen lange Anfrage über 280 Billionen mögliche Antworten gibt - um genau zu sein: 281.474.976.710.700. Um diese alle durchzuspielen, brauchte ein moderner Rechner 44.627 Jahre. Bei Rainbows SentinelSuperPro-Dongle (laut Werbetext »der sicherste und flexibelste Kopierschutz, den es gibt«) kann die Anfrage aber bis zu 56 Zeichen lang sein, so dass die Berechnung einer kompletten Tabelle »lediglich« 10 hoch 125 Jahre dauern würde.

Beim SentinelSuperPro-Dongle, der die 3D-Studio-Max-Software von Kinetix schützt, dauerte es allerdings nicht einmal sieben Tage (gerechnet ab Tag der Markteinführung durch ForceKill), dann hatte eine führende Hacker-Gruppe namens DOD (Drink Or Die) den Code gecrackt. Allen anderen teuren High-End-Anwendungen, die den Sentinel-Dongle nutzen - sei es Lightwave von NewTek, Softimage von Microsoft oder auch AutoCAD von Autodesk - ist das gleiche Schicksal widerfahren: Sie wurden gecrackt, neu verpackt und innerhalb weniger Tage nach ihre Veröffentlichung in alle Ecken des Internets verschickt.

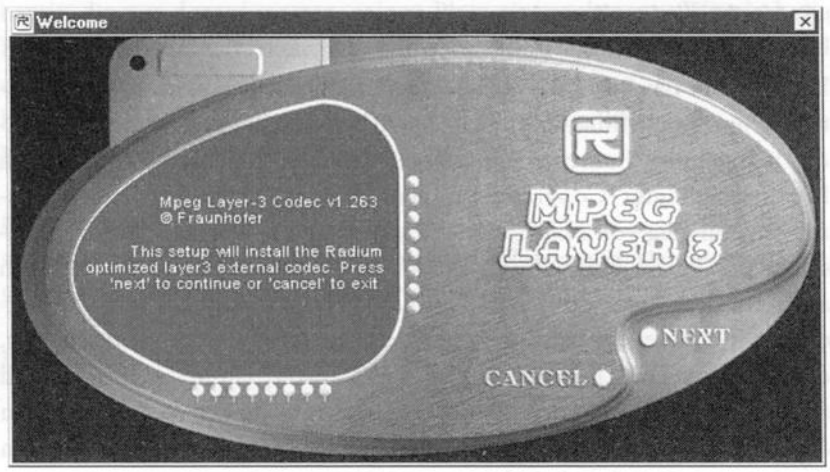
Anstatt zu versuchen, den Dongle zu simulieren, dröseln gerissene Hacker einfach den Programmcode auf, indem sie Zeile für Zeile, Funktion für Funktion, Aufruf für Aufruf die Beziehung entwirren, bis die Anwendung letztlich auch ohne Dongle funktioniert. Es gibt auf der ganzen Welt vermutlich nur acht oder neun Hacker, die in der Lage sind, ein solches Meisterstück abzuliefern. Aber Dank des Internets reicht der Erfolg eines einzelnen Hackers aus, um das Resultat bis in den letzten Winkel der Welt zu verbreiten. Und wenn ein solcher Geniestreich gelingt, dann sorgt die betreffende Crew auch dafür, dass dies bekannt wird, und der Erfolg wird in der gecrackten Software angehängten NFO-Files (Info-Textdateien) ausgiebig gefeiert.

«Total geniale Arbeit des ruhmreichen DOD-Crew-Mitglieds Replicator. Fünf andere Cracker haben vorher schon aufgegeben! Wir haben uns dafür entschieden, kein Crack Patch zu erstellen, weil das Coden zu viel Zeitaufwand bedeutet hatte. Warum? Weil 72 (!!!) EXEs zu patchen wären. Alle Optionen funktionieren jetzt 100%ig.«

Besser als das Original

Diese NFO-Texte sind mehr als nur prahlerische Statements. Sie liefern gleichzeitig die Installationsanweisungen und präsentieren dubiose ASCII-Art-Bilder. Sie sind in der Warez World das Authentizitäts-Zertifikat, Beweis für eine rechtmäßige Veröffentlichung, und die Garantieerklärung für deren Funktionsfähigkeit. Nichts zählt in der Szene mehr als der gute Ruf. Jede Veröffentlichung wird daher vorher aufs Sorgfältigste Beta-getestet. Schließlich betrachten die erfolgreichen Piraten die gecrackte Software jetzt als »ihr Produkt«. Und niemand will schließlich, nach sieben Stunden Download, einen »bad crack« in der Hand haben, der nicht funktioniert.

Im 21. Jahrhundert, nach Jahren des Trainings, erreicht das Können der Cracker jetzt ein neues Niveau, Anstatt nur die Kopierschutzfunktionen von Software zu überlisten, haben sie inzwischen damit begonnen, in die Codes einzutauchen und so die Programme tatsächlich zu verbessern.



Von Crackern optimiert: Der Fraunhofer MP3-Codec

Im Jahre 1996 veröffentlichte das Fraunhofer-Institut eine Kompressions-Technologie, die, im Zusammenhang mit Napster, bald darauf zum Synonym für Copyright-Klau im Internet werden sollte. Der Name dieser Technologie war MPEG Audio Layer 3, oder kurz MP3. Mit ihr konnte man Musik in CD-Qualität zu kleinen Dateien komprimieren, die leicht im Internet zu verschicken waren. Anfangs handelte es sich dabei noch um einen externen Codec. Das heißt, die Kompressionsformeln waren mit jedem Programm anwendbar. Doch dann, nach einer Reihe von Verbesserungen und Weiterentwicklungen, entschlossen sich die Experten bei Fraunhofer, den Codec zu integrieren und damit seinen Einsatz auf offiziell lizenzierte Software zu beschränken.

Die bekannte Audiowarez-Gruppe Radium hatte jedoch etwas gegen den aggressiven Patentschutz der Fraunhofer-Leute und beauftragte ihren Chefhacker IgNorAMUS damit, den Codec wieder extern verfügbar zu machen. Mit anderen Worten: die Reichen zu berauben, um den Armen zu geben. Wahrend besagter IgNorAMUS nach Schleppnetz-Methode Tausende von Zeilen von Assembler Code durcharbeitete, kam er zu einer aufregenden Erkenntnis. Nämlich der, dass er Verbesserungen am Algorithmus

vornehmen konnte. Nach kurzem Einsatz des Debuggers hatte er eine Reihe von Änderungen implementiert, die zu einer Optimierung der Performance führten und letztlich dazu, dass das Programm um 12 Prozent schneller lief. Radium verpackte den MP3-Codec neu und versah ihn stolz mit einem Diagramm, welches die Überlegenheit der Radium-Variante gegenüber dem Original der Fraunhoferschen Konkurrenz verbildlichte. Anschließend verbreitete sich der Radium-Codec mit Netz-Geschwindigkeit in der ganzen Welt und wurde schließlich dazu benutzt, die Millionen kommerzieller MP3s zu komprimieren, die bei Napster getauscht werden.

Die Schlacht wird weitergehen

Napster war das Beste, was der Softwareindustrie je widerfahren ist. Jahrelang hatte sie Millionen für Lobby-Arbeit ausgegeben und dabei ständig mangelndes Interesse und Verständnis der Regierungen bezüglich Internet-bedingter Copyright-Probleme beklagt. Mit dem explosionsartigen Aufstieg von Napster wurden genau diese Themen auf die Titelseiten der Presse katapultiert, direkt in den Mainstream, um letztlich auch auf den Tagesordnungen von EU-Parlament und US-Senat zu landen. In Windeseile werden jetzt harte und strikte Gesetze verabschiedet, die einerseits Tausch-Technologien wie Napster, Gnutella, Freenet und anderen einen Riegel vorschieben und andererseits den Rechteinhabern die Möglichkeit eröffnen sollen, ihre Bücher, Musik und Software im Internet mittels hoher Gebühren zu schützen.

Aber all diese neuen Technologien, Verschlüsselungen und Gesetze werden die Daten-Piraterie nicht beenden. Die Schlacht wird einfach weitergehen. Es liegt in der Natur des Internets, dass es keine Gesetze kennt. Das Netz ist auf den freien Austausch von Informationen ausgerichtet - wobei hier die Betonung auf »frei« liegt. Solange es einen Markt gibt, wird es daneben auch einen Schwarzmarkt geben. Oder, wie das Beispiel von Napster anschaulich gezeigt hat, solange es Informationen mit einem gewissen Wert gibt, wird es auch Leute geben, die diese für lau nutzen. Und angesichts der sich immer wieder selbst auffüllenden Auslagen des anfangs beschriebenen HiFi-Ladens, wo sich jeder bedienen kann und niemand geschädigt oder geschnappt wird, werden sich die Leute auch weiterhin bedienen.

Die BSA und die von ihr repräsentierte Softwareindustrie werden auch in der Zukunft fortfahren, Exempel an einigen wenigen Netzpiraten zu statuieren. Sie werden weiter in Kopierschutzprogramme investieren und auf jede neue Technologie mit Argwohn und Angst reagieren. Aber auch die Warez World wird weiter existieren, sich selbst vervollkommnen und regulieren und dabei neue kreative Wege finden, wie sie die Technologie gegen diejenigen einsetzen kann, die mit ihr Profit machen wollen. Die Netzwerke der Warez World sind zu ausgedehnt, und ihre Mitglieder sind zu sehr auf Draht, als dass die Softwareindustrie sie kontrollieren könnte.

Für jeden Piraten, der der Szene den Rücken kehrt, erwachsen wird, sich für eine Karriere als Schlipsträger entscheidet oder aber von Ermittlern wie Kyle gefasst und angeklagt wird, stehen schon zehn andere bereit, die nur darauf warten, seinen Platz einzunehmen. Wir sind alle Familienmenschen, verheiratet, mit Kindern, normalen Tagesjobs und unzähligen Telefonleitungen«, meint Mad Hatter. »Unsere Kinder haben uns jahrelang über die Schulter geschaut. Sie werden die nächsten Kuriere, die neuen Warez-Götter sein.«

David McCandless lebt und arbeitet als Autor und Musiker in London. Er schreibt seit 15 Jahren über kulturelle Aspekte der Informationstechnologien. Mehr von ihm gibt es auf seiner Website http://www.wakeywakey.com.

Übersetzung: Steve Winkler

2. Eine virale Kultur

Virenprogrammierer,
ihre Geschichte, ihre Communities,
Ihr Katz- und Mausspiel mit der Antivirus-Industrie

Sie lieben uns.txt.vbs

Janko Röttgers

»Sachen zu sammeln ist etwas, was ich immer gern gemacht habe. Als Kind sammelte ich Briefmarken, jetzt sammle ich Computerviren.« Luis ist 27, glücklich verheiratet, arbeitet in einem spanischen IT-Unternehmen und widmet sich in seiner Freizeit mit Vorliebe Programmen, um die andere Computernutzer lieber einen großen Bogen machen.

Virensammler wie Luis gibt es wahrscheinlich ein paar Hunderte. Doch nur wenige nehmen dieses Hobby so ernst wie er, und niemand besitzt eine derart große Sammlung. Wie viele elektronische Schädlinge auf seiner Festplatte schlummern, möchte er nicht sagen. Luis ist in solchen Beziehungen sehr genau. Er weiß, dass viel Unsinn über die Zahl der existierenden Viren geschrieben wird. Er weiß, dass die Hersteller von Antivirus-Software sich gegenseitig mit Zahlen zu überbieten versuchen, die jenseits von Gut und Böse liegen. Luis möchte diese Diskussion nicht noch weiter anstacheln. Er verrät nur so viel: Lediglich drei oder vier der größten Hersteller von Antivirus-Software besäßen eine größere Sammlung als er. Letztlich geht es ihm aber auch gar nicht um die Größe der Sammlung, sondern um jedes einzelne Exemplar. Ein echter Sammler eben.

Seit fast zehn Jahren ist Luis nun schon unter dem Namen Virusbuster Teil einer vitalen Szene des elektronischen Undergrounds, die sich selbst als vXer bezeichnen. Virenprogrammierer, Virensammler und andere Freunde sich selbst vervielfältigender Programme, die sich in kleinen Gruppen zusammenschließen und über ein eng gesponnenes Netzwerk aus Chaträumen, Websites und elektronischen Magazinen austauschen. Luis ist Mitglied der 29a-Gruppe, gegründet 1996 von einem spanischen Programmierer mit dem Pseudonym Mr. Sandman. 29a gilt sowohl unter vXern als auch unter Mitarbeitern von Antivirus-Softwarefirmen - vXer nennen sie gerne AVler - als eine der innovativsten Gruppen der Szene. Der erste Windows-2000-Virus, der erste Gnutella-Wurm, der erste Plattform-übergreifende Virus, der sowohl Windows als auch Linux infiziert - 29a lotet ständig neue Möglichkeiten für elektronische Schädlinge aus. Ständig zwingt sie damit auch die Programmierer von Antivirus-Software, ihre eigenen Programme zu verfeinern und die ihnen zu Grunde liegenden Konzepte zu überdenken. Ein ewiges Katz- und Mausspiel.

Wärmer, Kaninchen und geklonte Elche

Es ist ein Spiel mit Tradition, das Luis und seine Freunde da spielen. Die ersten programmierten Schädlinge tauchen bereits in den Sechzigern auf einigen Großrechnern

auf. Sie vervielfältigen sich selbst im Hauptspeicher der Maschinen, klauen damit anderen Nutzern die zu dieser Zeit noch so kostbare Rechenzeit und werden wegen ihres Vermehrungsdrangs Kaninchen genannt.

Anfang der Siebziger experimentiert dann ein gewisser Bob Thomas mit einem Programm, das sich innerhalb eines Netzwerks von Rechner zu Rechner fortbewegen kann. Thomas arbeitet beim ARPANET-Entwickler Beranek and Newman und ist dort aktiv an der Entwicklung der technischen Grundlagen des heutigen Internets beteiligt. Im wahrsten Sinne des Wortes ein Job mit Zukunft. Einer, den man gerne behalten will. Dummerweise erweist sich sein kleines Experiment - Thomas hat das Programm Creeper getauft - als äußerst erfolgreich. Es pflanzt sich im Tenex-Netzwerk der Firma unkontrolliert von Rechner zu Rechner fort und scheint nicht mehr zu stoppen. Kurzerhand programmiert Thomas ein zweites Programm namens Reeper, das dem Schädling nachjagt und ihn erfolgreich ausschaltet.

Reeper ist damit gewissermaßen die erste Antiviren-Software der Welt. Allerdings würden Antivirus-Experten Creeper aus heutiger Sicht nicht Virus nennen, da das Programm keine anderen Dateien infiziert, sondern sich nur selbst autonom im Netzwerk fortpflanzt. Solche Geschöpfe nennt man heute Wurm - ein Begriff, den John Hupp und John Shoch vom Xerox Palo Alto Research Center 1982 einführen. Die beiden Science Fiktion-begeisterten Forscher lassen sich dabei von John Brunners Kultbuch »Der Schockwellenreiter« inspirieren. Brunner spricht darin schon Mitte der Siebziger von einem »Tape worin« - einem sich selbst vervielfältigenden Programm, mit dem der Held des Romans das Computersystem einer totalitären Regierung lahm legt.

In den Jahren 1981 und 1982 entwickeln einige Computer-begeisterte Jugendliche dann das, was man als erste Computerviren bezeichnen kann. Der fünfzehnjährige College-Freshman Rich Skrenta schreibt ein Programm für den Apple 2 mit dem schönen Namen Elk Cloner. Der sich selbst vervielfältigende Elch infiziert Disketten mit dem Apple Disk Operating System 3.3, ohne dabei Daten zu löschen. Startet man eine solche infizierte Diskette zum fünfzigsten Mal, erscheint ein kleines Gedicht auf dem Bildschirm:

> »It will get on all your disks
> It will Infiltrate your chips
> Yes it's cloner!
>
> It will stick to you like glue
> It will modify RAM too
> Send in the Cloner!« [1]

Später wird Rich Skrenta Mitgründer des Open Directory Projects. Dass er den wohl ersten Virus geschrieben hat, hängt ihm allerdings heute noch nach: »Der dümmste Hack, den ich je programmiert habe, aber er erzeugte am meisten Aufmerksamkeit«, erklärt er dazu Jahre später. [4]

Joe Dellinger studiert zu dieser Zeit an der Texas A&M University und spielt ebenfalls viel mit dem Apple 2 herum. Er schreibt wie Skrenta einige sich selbst vervielfältigende Programme. Ohne groß darüber nachzudenken, nennt er sie Virus1, Virus2 und Virus3 und besetzt damit einen Begriff, der uns bis heute begleitet.

Fred Cohen: Jedes System ist infizierbar

Durchsetzen sollte sich dieser Begriff aber erst, als Fred Cohen 1984 seine Forschungsergebnisse mit sich selbst vervielfältigenden Programmen unter dem Titel »Computer Viruses - Theory and Experiments« veröffentlicht. Cohen definiert hier erstmals, was genau eigentlich ein Computervirus ist: ein sich selbst vervielfältigendes Programm, das andere infizieren kann, indem es ihnen den eigenen Code einverleibt. Cohen liefert in seiner Abschlussarbeit gleich auch einige geringfügig abstrahierte Beispiele für den Aufbau eines solchen Virus mit - ein Schritt, der heute wohl manch einen Professor zum Ablehnen der Arbeit bewegen würde.

Doch 1984 gibt es noch keine bösen Viren, keine Underground-Szene der Virenprogrammierer, keine Antivirus-Industrie und keine sensationsheischenden Zeitungsartikel. Wenn ein Virus Schaden anrichtet, dann allenfalls durch Unachtsamkeit und schlechte Programmierung. Wer in diesen Tagen etwas über Viren lehren oder lernen will, muss ganz zwangsläufig auch welche programmieren. Trotzdem ahnt Cohen bereits, dass man eines Tages Schutz vor Viren und Würmern brauchen wird, dass sie zur Bedrohung werden können.

Er überprüft mögliche Sicherheitskonzepte auf ihre Wirksamkeit, stellt aber bald fest: Vollkommene Sicherheit verspricht nur ein komplett abgeschlossenes System. Eines, das ohne Code von außen auskommt, nicht vernetzt ist und möglichst auch gar keine Eingaben zulässt. Sicher nicht das, was man von einem Computer erwartet. Alle anderen Systeme seien für Viren anfällig, so Cohen. Dies gelte auch für noch zu entwickelnde Systeme, denn: »Die vorgestellten Ergebnisse sind nicht Betriebssystems- oder Implementations-spezifisch, sondern basieren auf den grundlegenden Eigenschaften von Systemen.« [3] Mit anderen Worten: Es gibt keinen absoluten Schutz vor Viren. Jeder Rechner, jedes System kann infiziert werden.

Die ersten Viren mit Impressum

Einige Systeme allerdings leichter als andere, wie sich bald zeigen wird. Im März 1982 erscheint die erste Version von Microsofts MS DOS. Dank eines geschickt ausgehandelten Vertrags mit IBM legt Firmengründer Bill Gates den Grundstein dafür, dass dieses System binnen weniger Jahre zum Standard für Desktop-PCs wird. Und dank seiner Architektur, die keinerlei Privilegien und Schutzmechanismen kennt, wird es bald zur wichtigsten Plattform der Virenprogrammierer.

1986 verbreitet sich erstmals ein MS-DOS-Virus um den Erdball. Die beiden Brüder Basit und Amjad Farooq Alvi besitzen eine kleine Softwarefirma namens Brain Computer Services in Pakistans Hauptstadt Labore. Um gegen die immense Raubkopiererei in ihrem Land vorzugehen, programmieren sie den ganz und gar harmlosen Brain-Virus. Überrascht müssen sie allerdings feststellen, dass schon kurze Zeit später auf der ganzen Welt Disketten verbreitet werden, in deren Boot-Sektor sich ihr Virus findet - und mit ihm die gültige Adresse und Telefonnummer der beiden.

Ebenfalls ganz brav mit seinem echten Namen und seiner Telefonnummer kennzeichnet der deutsche Programmierer Ralf Burger seine ersten Viren. Mit seinem Virdem-Virus im Gepäck besucht er 1986 den Chaos Communication Congress, den der Chaos Computer Club jährlich organisiert. Viren bilden in diesem Jahr das Schwerpunktthema der Veranstaltung. Erstmals kann sich eine breitere interessierte Öffentlichkeit über das

Phänomen informieren. Angeblich beteiligen sich bis zu 20 aktive Virenprogrammierer an den angebotenen Workshops. Die Szene formiert sich.

Ab etwa 1987 tauchen immer mehr Viren für MS-DOS-Rechner auf. Den Programmierern geht es längst nicht mehr nur um das reine Selbst-Vervielfältigen. Ihre Geschöpfe mit Namen wie Cascade-Virus, Vienna-Virus oder Jerusalem-Virus unterscheiden sich auch in dem, was sie mit dem befallenen Rechner anrichten - den so genannten Payloads. Burgers Virdem-Virus fordert den Benutzer irgendwann auf, eine Zahl zu raten. Nur wer richtig Hegt, darf weiterarbeiten. Der Stoned-Virus wird dadurch berühmt, dass er verkündet: »Your PC is stoned!« Doch einige Programmierer bedienen sich auch nur der bereits verbreiteten Viren-Quellcodes, um mit gefährlichen Payloads ihrer destruktiven Energie freien Lauf zu lassen. Eine Variante von Burgers Virdem-Virus etwa formatiert am Freitag dem Dreizehnten die befallene Festplatte. Neben solch bösen Überraschungen entwickeln die Virenprogrammierer auch erste Techniken zur Verschleierung ihrer Aktivitäten. Der Cascade-Virus beispielsweise setzt auf Verschlüsselung - ein klares Tribut an die noch junge Antivirus-Industrie.

Mit Ghostbuster-Attitüde gegen elektronische Schädlinge

Eine der schillerndsten Gestalten dieser Branche ist zu dieser Zeit John McAfee, Chef der Firma Interpath und später Gründer von McAfee Associates. 1988 gründet er den Branchenverb and »Computer Virus Industry Association«. Zahlreiche Antivirus-Firmen wollen jedoch nicht beitreten, weil sie McAfee bezichtigen, als Gründer des National Bulletin Board Society-Netzwerks selbst Viren zu verbreiten. Auch wenn ihm dieser Vorwurf unter Experten noch über Jahre nachhängt, schafft McAfee es, in den Augen der Öffentlichkeit zum prominentesten aller Virenjäger zu werden.

Der für seine Utility-Sammlung bekannte Peter Norton soll angeblich zu dieser Zeit noch öffentlich verkündet haben, er glaube nicht an die Existenz von Viren. Das sei doch alles nur eine Legende, vergleichbar mit den Alligatoren in der öffentlichen Kanalisation New Yorks. John McAfee findet dagegen schnell heraus, dass der unbedarfte Computernutzer sehr wohl gerne an unberechenbare Gefahren in diesem ihm unverständlichen Kasten glaubt. 1988 baut er ein Wohnmobil mit Computern aus, tauft es »Virus Bug Buster« und lässt ein Team damit im Silicon Valley von Kunden zu Kunden fahren, um ihnen die Computer zu säubern. Rent to kill meets High Tech Ghost Busters - das sind Metaphern, die bei den Computernutzern besser ankommen als die leiseren Töne der Konkurrenz.

Der Walker-Virus

Zu diesem Zeitpunkt liegt die Zahl der existierenden Viren noch im zwei- bis dreistelligen Bereich. Tatsächlich in freier Wildbahn findet man davon noch sehr viel weniger. Dafür beginnen die Viren jetzt, die Medien zu infizieren. Neben den ersten Horrormeldungen in diversen Tageszeitungen werden auch erstmals Viren im Sourcecode publiziert und einer breiteren Öffentlichkeit zugänglich gemacht. Ralf Burger veröffentlicht 1987 im Data Becker Verlag »Das Große Computer-Virenbuch« mit dem Sourcecode einiger teilweise selbst programmierter

Beispielviren. Ein Jahr später erscheint das Buch auch in englischer Übersetzung.

1990 zieht dann der Amerikaner Mark Ludwig mit seinem »Little Black Book of Computer Viruses« nach, das sogar samt einer Diskette mit Beispielviren ausgeliefert wird. Diese Veröffentlichungen stoßen in der Antivirus-Community auf große Kritik. So wirft der bulgarische Antivirus-Experte Vesselin Bontchev den Autoren vor, Wissenschaftlichkeit nur als Schutzschild Der Walker-Virus zu missbrauchen und Nachahmer zu provozieren. In Bezug auf Ludwigs Buch urteilt er: »Alles, was wir dort zu sehen bekommen, ist ein Haufen unsinniger MS-DOS-Viren, die kaum funktionieren.« [4]

Doch auch die einfachste Beschreibung des Phänomens reicht aus, um weltweit Computerfreaks zu begeistern. In der Septemberausgabe der deutschen Computerzeitschrift Chip erscheint ein Artikel von Chaos-Computer-Club-Mitglied Steffen Wernery unter dem Titel »Computerviren - Die neue Gefahr?«. Die bulgarische Computerzeitschrift »Computer za vas « druckt den Artikel ein halbes Jahr später übersetzt nach und legt damit den Grundstein für eine der vitalsten Virenprogrammierer-Szenen. Innerhalb von drei Jahren erreichen die bulgarischen Viren einen Anteil von zehn Prozent am Gesamt-Weltmarkt.

Das sozialistische Computerparadies

Aber warum gerade Bulgarien? Glaubt man den Überlieferungen des Antivirus-Experten Bontchev, [5] dann ist Bulgarien Ende der Achtziger so etwas wie das sozialistische Computerparadies. Das ZK der bulgarischen Kommunisten entscheidet Anfang des Jahrzehnts, mit der Produktion eigener Microcomputerserien zu beginnen, diese an den gesamten Ostblock zu liefern und so das Exportverbot des Westens zu unterlaufen. Allerdings entwickelt man keine völlig neuen Systeme, sondern spezialisiert sich auf das Klonen bereits existierender Modelle.

Zuerst werden mit dem IMKO und dem Pravetz 82 Systeme entwickelt, die möglichst perfekte Nachbildungen des Apple 2 darstellen. 1984 wird schließlich der Pravetz 8 entwickelt - ein 8-Bit-Mikrocomputer, der auch mit Microsofts DOS 3.3 arbeitet. Eine wichtige Voraussetzung für seinen Erfolg, denn um den Vorsprung des Westens aufzuholen, setzt man hier nicht auf das Entwickeln eigener Software. Stattdessen werden an diesen Maschinen ganze Generationen von Informatikern in Reverse Engineering ausgebildet. Ihre Studienaufgaben müssen ungefähr so ausgesehen haben: Nimm dir etwas Hardware aus dem Westen und bau es möglichst billig nach. Oder nimm dir Microsofts neueste DOS-Version, portier sie auf den Pravetz - aber lass bitte die Bugs weg.

Als dann Wernerys Chip-Artikel in bulgarischer Übersetzung erscheint, sind einige dieser Studenten sofort infiziert. Viren waren ihnen bis dahin unbekannt. Also besorgen sie sich den Vienna-Virus, der auch im Artikel beschrieben wird, und verfahren damit so, wie sie es mit westlicher Software gewohnt sind: disassemblieren, analysieren, optimieren. Weil es in Bulgarien auch keine Antivirus-Industrie gibt, mit der man das Katz- und Maus-Spiel spielen könnte, müssen sie die Katze gleich mit erfinden. Der Programmierer des Jankee-Doodle-Virus schafft sich deshalb sein eigenes Antiviren-Programm namens Vacsina. Daran probiert er seinen Virus aus, verstärkt den Schutz, verbessert den Virus, und so weiter. Einige seiner Viren verbinden sogar beide Techniken und deaktivieren andere Viren, die sich auf dem befallenen System befinden.

1990 entsteht dann in Sofia das erste Virus Exchange (vX) Bulletin Board - ein Mailboxsystem zum Austausch elektronischer Schädlinge, das mit einer Upload/Download-

Ratio arbeitet. Wer sich Viren herunterladen will, muss dafür neue Viren hochladen. Weil bald alle bekannten Viren in das System eingespeist sind, müssen die User wohl oder übel neue programmieren. Bald wird die BBS mit ihren knapp 300 Nutzem weltweit als »virtuelle Virenuniversität« bekannt. Einer der aktivsten Studenten dieser Universität nennt sich Dark Avenger und ist ein höchst talentierter Programmierer aus Sofia. Anfang 1991 kündigt er an, einen Virus mit mehr als 4.000.000 Mutationsmöglichkeiten zu entwickeln.

Unterricht am Pravetz 82

Wir sind die Guten

Etwa zur gleichen Zeit kauft sich in den USA die Sozialarbeiterin Sarah Gordon ihren ersten PC. Nach kurzer Zelt erscheint auf ihrem Bildschirm ein kleiner, umherspringender Ball - ein sicheres Zeichen für den Ping-Pong-Virus. Gordons Interesse ist geweckt. Da sie schon früh Erfahrungen mit Mailboxen gesammelt hat, sucht sie im Fido-Netz nach mehr Informationen und stößt dabei auf die Newsgroups der Virenprogrammierer-Szene.

Ein Name fällt ihr immer wieder auf: Dark Avenger. Er ist der Autor des gleichnamigen Virus, der als extrem gefährlich gilt, weil er sich vor Virenscannern zu verbergen weiß, diese infiziert und damit auch jede überprüfte Datei befällt. Sarah Gordon versucht vergeblich, mit Dark Avenger Kontakt aufzunehmen. Dann probiert sie es mit einem Trick. In einer einschlägigen Newsgroup wünscht sie sich einen Virus, der ihren Name trägt.

Wieder hört sie nichts von Dark Avenger. Bis im Januar 1992 sein lange angekündigter Mutations-Virus erscheint, ein Generator für polymorphe Viren mit Abertausenden von Erscheinungsmöglichkeiten. Erstaunlicherweise erkennen die meisten Antiviren-Programme Dark Avengers »Mutation Engine« schon nach wenigen Tagen. Doch offenbar waren einige Programmierer bei der Anpassung der Scanner zu eifrig. Neben Dark Avengers Mutationen werden jetzt plötzlich auch Tausende von nicht infizierten Dateien als Viren erkannt. Die Antivirus-Industrie hat ein Problem. Und mitten in diesem Problem steht der Satz: »Wir widmen diesen kleinen Virus Sarah Gordon« - als wäre der Mutation Engine nichts weiter als eine nette Neujahrspostkarte.

In der Antivirus-Community heißt der Mutation Engine zunächst nur »Dedicated«, und Sarah Gordon ist mit einem Mal bekannt wie ein bunter Hund. Doch das hält sie nicht davon ab, sich weiter mit dem Thema zu beschäftigen. Anfang der Neunziger sind die Fronten zwischen Virenprogrammierern und Antivirus-Forschern bereits deutlich verhärtet. Viele in der Antivirus-Industrie fordern bereits härtere Strafen für das Verbreiten von Computerviren und bemühen sich redlich, Virenprogrammierer per se als kriminell darzustellen.

Doch Sarah Gordon besitzt als Sozialarbeiterin andere Zugriffsmethoden: »Ich stellte fest, dass es eine echte Diskrepanz zwischen dem, was die Antiviren-Leute über die > Bad Guys< sagten, und meinen Beobachtungen gab.« [6] Gordon beschließt, sich intensiver den »Bad Guys« zu widmen und erstmals systematisch deren Strukturen und Motivationen zu erforschen. Die Szene akzeptiert sie zwar, viele hatten sie aber wiederum für eine von den »Bösen« - schließlich lässt sie sich ihre Forschungsarbeit von Firmen wie IBM und Symantec bezahlen. Sarah Gordon ironisiert diese wechselseitige Schwarzweißmalerei gerne. Ihre private Website firmiert konsequenterweise unter der Adresse www.badguys.org.

Aus Luis wird der Virusbuster

Wie Sarah Gordon kommt auch Luis Anfang der Neunziger zum ersten Mal mit dem Ping-Pong-Virus in Kontakt. Unfreiwillig, versteht sich. »Mein einziges Interesse an dem Virus war, ihn zu killen«, erklärt er dazu heute. Damals sammelt und tauscht er raubkopierte Programme. Auf der Suche nach ein paar neuen Spielen stoßt er auf jemanden, der wie er Warez tauscht, aber auch ein paar ganz besondere Programme im Angebot hat. »Er zeigte mir, dass Viren eine interessante Sache sein können, wenn du mit ihnen umzugehen weißt. Er gab mir seine Virensammlung, ungefähr 40 oder so, und ich begann mit meinen eigenen Experimenten.«

1994 entdeckt Virusbuster das Internet und damit die vX-Szene. Diese Szene hat im Netz seit etwa 1990 feste Strukturen gebildet. Von ganz elementarer Bedeutung sind dabei neben den Mailboxen zwei Internetdienste: Im August 1988 entwickelt der Finne Jarkko Oikarinen das Internet-Relay-Chat-Netzwerk (IRC). 1989 erfindet Tim Berners-Lee das World Wide Web, 1990 entwickelt er den ersten Web-Browser. Das IRC ist noch heute für die vX-Szene das wichtigste Medium zum informellen Austausch. Das World Wide Web hat dabei geholfen, aus diesen informellen Strukturen feste Bünde zu schmieden. Man schließt sich zu einer Gruppe zusammen, gibt sich mit einer Website ein Gesicht, tauscht darüber Viren aus und gründet E-Zines. Im Juni 1991 erscheint die erste Ausgabe des 40hex-Magazins mit einer Mischung aus Viren-Sourcecode und Programmier-Anleitungen. Es dient zahlreichen Magazinen dieser Art als Vorbild.

Erste Verhaftungen

1992 ist ein schlechtes Jahr für die Antivirus-Industrie. Für den sechsten März kündigen einige Firmen Millionen von Computerausfällen durch den Michelangelo-Virus an. Betroffen sind jedoch letztendlich nur etwa 10 000 Rechner weltweit. Gleichzeitig tauchen in diesem Jahr die ersten wirklich einfach bedienbaren Virusgeneratoren auf, mit denen sich jeder Laie seinen eigenen Virus zusammenklicken kann.

Im Gegenzug verstärkt man den Druck auf die vX-Szene. 1993 kommt es zu den ersten Verhaftungen bei Mitgliedern der britischen Association of Really Cruel Viruses (ARCV). Das Antivirus-Lager feiert dies als Erfolg und hofft, dass ähnliche Aktionen weiteren Virenautoren das Leben schwer machen könnten. Doch bei genauerer Betrachtung des Falls stellt sich heraus, dass die ARCV-Mitglieder sich eines anderen Verbrechens schuldig gemacht haben: Sie benutzten Geräte zur Manipulation des Telefonnetzes (so genannte Brown Boxes), um mit kostenlosen Telefonaten Kontakt zu vX-Mailboxen in den Vereinigten Staaten aufzunehmen.

Zu einer ersten Verurteilung eines Virenprogrammierers kommt es erst 1995. Der 26-jährige Brite Chris Pile wird wegen der Verbreitung seiner SMEG-Viren und der eines manipulierten Antivirus-Programms zu 18 Monaten Gefängnis verurteilt. Viele Virenprogrammierer sind von dem Urteil gegen den Black Baron, wie er in der Szene heißt, schockiert. Vom Schreiben eigener Viren lassen sich dadurch aber nur die wenigsten abhalten. Doch viele überlegen es sich seitdem zweimal, ob sie einen Virus in die Wildnis entlassen. Die meisten Viren zirkulieren nur in der Szene, nur ein geringer Prozentsatz infiziert jemals die Rechner Unbeteiligter. Allein das Programmieren von Programmen, die sich selbst vervielfältigen, ist in den meisten Staaten aber nicht verboten.

Wer seine Viren dennoch in die Wildnis entlässt, bleibt gerne vollkommen anonym. »Virenprogrammierer, die ihre Geschöpfe verbreiten, verbinden sich mit dem IRC über Proxy-Server«, erklärt Luis eine der verbreiteteren Vorsichtsmaßnahmen. Er selbst hat nie einen Virus programmiert, würde seine eigenen Kreationen aber auch nicht in die Wildnis entlassen. Ähnlich geht es den meisten seiner Freunde von der 29a-Gruppe. In deren Policy heißt es: Wir programmieren Viren aus Spaß an der Sache, weil es unser Hobby ist, und nicht, um anderen zu schaden.« [7] Distanzieren mochten sie sich von Viren, die in der Wildnis auftauchen, jedoch nicht.

Windows 95: Neuanfang oder Terror?

Für Schlagzeilen sorgen meist nur die Viren, die tatsächlich Infektionen auslösen, unzählige Computersysteme außer Betrieb setzen oder sich besonders eigentümlich verbreiten. Wie etwa der Tremor-Virus, der 1994 als erstes Programm seiner Art über das Fernsehen unters Volk gebracht wird. Zu dieser Zeit nutzt die deutsche Firma Channel Videodat die Austastlücke des Fernsehsenders Pro 7, um mit etwa 15 KBit pro Sekunde Software an Käufer des Videodat-Decoders zu vertreiben. Im Mai 1994 findet auf diesem Weg auch eine infizierte Version des Dekompressions-Programms PkUnzip den Weg auf zahlreiche Festplatten. Drei Monate nach der Infektion werden Tausende von Videodat-Usern damit konfrontiert, dass die Darstellung ihres Monitors wackelt, bevor sich der Rechner ganz aufhängt. In einigen Fällen meldete sich Tremor auch mit dem Front-242-Zitat »Moment of Terror is the Beginning of Life« zu Wort. [8]

Neuanfang oder Terror - diese Frage stellt sich 1995 auch so manch ein Beta-Tester von Windows 95. Microsoft verschickt in einigen Fällen Disketten, die mit dem Form-Virus infiziert sind. Doch diese peinliche Panne ist fast bedeutungslos gegen all die neuen Möglichkeiten, die das System Virenprogrammierern bietet. Anfang 1996 erscheint mit Bizatch der erste Windows-95-spezifische Virus. [9] Schon ein paar Monate vorher taucht mit Concept der erste Word-Macrovirus in freier Wildbahn auf. Beide legen den Grundstein für unzählige Nachfolger. 1996 kommt es zur ersten Windows-Virenepidemie.

Im selben Jahr gründen einige Virenprogrammierer um einen gewissen Mister Sandman die vX-Gruppe 29a, der wenig später auch Luis alias Virusbuster beitritt. Ihr Name ist die hexadezimale Darstellung des satanischen 666, und auch sonst lieben die 29a-Mitglieder kleine Zahlenspielereien. Am Freitag, dem 13. Dezember 1996, um 6 Uhr 66 morgens erscheint die erste Ausgabe ihres Magazins, mit dem die Gruppe sozusagen offiziell ihre Gründung begeht. Es enthält Programmieranleitungen, Viren-Sourcecode und -analysen und ein Dutzend Viren als ausführbare Dateien sowie Tipps zum Umgehen von Antivirus-Schutzmechanismen, die hier »Klingon Tech« genannt werden. Dazu liefern die 29a-Mitglieder einen eigenen Textbetrachter, der als Bildschirmschoner die Payload-Ausgabe des LSD-Virus verwendet. Solche Gimmicks wiederholen sich in den nächsten Ausgaben. Nummer zwei des 29a-Magazins erscheint mit einem animierten Intro, wie man es von Veröffentlichungen der Demo-Szene kennt.

Intern ist die Gruppe gewissermaßen basisdemokratisch organisiert. Es gibt keinen Anführer, lediglich für eine neue Ausgabe ihres Magazins wird eine Art Redakteur bestimmt. Ganz auf die Gruppe ausgerichtet sind auch die Initiationsregeln: Wenn jemand Mitglied bei 29a werden will, muss er uns seine Artikel und Viren schicken, damit wir die Qualität seiner Arbeit beurteilen können. Die Mitglieder Überprüfen dann sein Material und auch ihn als Person. Wenn alle dafür sind, kann er Mitglied werden. Bei nur einer Gegenstimme wird er nicht Mitglied«, erklärt Luis. Andere Entscheidungen werden per Mehrheitsbeschluss gefasst.

Nach Schätzungen von Sarah Gordon gibt es derzeit rund 20 beständig aktive Gruppen wie 29a. Daneben existiert noch eine ganze Zahl von Gruppierungen, die nur kurz auf der Bildfläche erscheinen, sich aber sofort wieder auflösen oder mit einer anderen Gruppe verschmelzen. 29a jedoch beweist Kontinuität - zwar veröffentlichen sie gerade mal ein Magazin pro Jahr, dafür gehen auf das Konto der Gruppenmitglieder einige der innovativsten und kreativsten Viren der letzten Jahre.

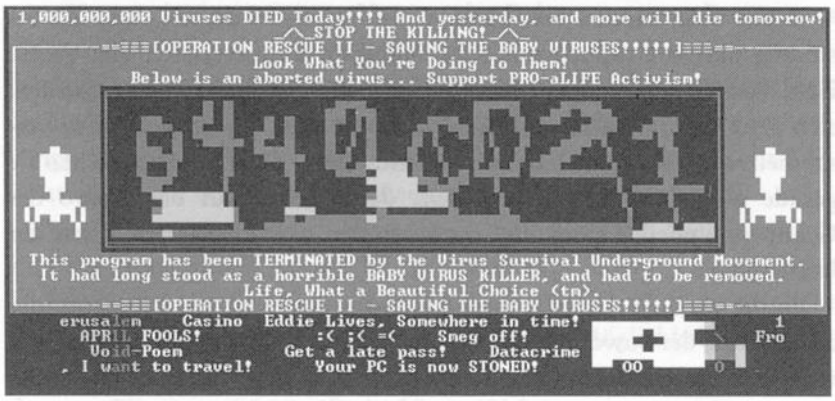
In der zweiten Ausgabe ihres Magazins erscheint mit Esperanto der erste Virus, der sowohl Windows- als auch Macintosh-Rechner infizieren kann. An jedem 26. Juli - dem Tag, an dem 1887 das erste Buch über die Kunstsprache Esperanto erschien - verkündet der Virus:

> Never mind your culture / Ne gravas via kulturo,
> Esperanto will go beyond it/ Esperanto preterpasos gxin;
> never mind the differences / ne gravas la diferencoj,
> Esperanto will overcome them / Esperanto superos ilin.
>
> Never mind your processor / Ne gravas via procesoro,
> Esperanto will work in it / Esperanto funkcios sub gxi;
> never mind your platform / Ne gravas via platformo,
> Esperanto will infect it/ Esperanto infektos gxin. [10]

Von diesem kleinen Sprachkurs abgesehen richtet der von Mr. Sandman programmierte Virus keinen weiteren Schaden an.

Viren: Politik, Forschung, pubertärer Spaß?

Im gleichen Magazin erscheint auch der Anti-ETA-Virus von Griyo, mit dem die Gruppe kollektiv gegen den baskischen Terrorismus Stellung bezieht. Es ist nicht der erste Virus mit einer politischen Botschaft. Aber taugen Viren als Mittel politischer Meinungsäußerung? Heute sehen die 29a-Mitglieder dies selbst eher skeptisch und tun es als eine Art Jugendsünde ab. Griyo hat sich als Autor des Virus mittlerweile von dieser Aktion distanziert, und Luis erklärt: »Das ist eher eine persönliche Leidenschaft einiger Mitglieder der Szene. Die Mehrheit der Virenprogrammierer vermischt Politik und Viren nicht. Ich bezweifle sogar, dass die große Mehrheit der Virenprogrammierer in der Szene sich Überhaupt um so etwas kümmert.« Auch den Versuch, das Programmieren von Viren selbst als politisch, weil ja irgendwie diffus gegen das System gerichtet zu begreifen, blockt er sofort als unzulässige Projektion ab: »Ich sehe im Programmieren eines Virus keinen politischen Akt.«



Bildschirmausgabe des Rescue-Virus

Aber warum machen sie es dann? Mit dieser Frage beschäftigt sich auch Sarah Gordon, seit sie die Szene als ihr Forschungsobjekt entdeckt hat. Eine eindeutige Antwort darauf kann sie bis heute nicht geben, denn Virenprogrammierer »sind so verschieden wie ihre Viren«, so Gordon. [11] Einige handeln aus Spaß an der Sache, andere wollen es in der Szene zu etwas bringen oder genießen es, wenn Antivirus-Firmen ihre Programme rezensieren. Wieder andere üben einfach ihre Programmierkenntnisse an diesen Kreationen oder sie genießen den Kitzel am Illegalen - etwa, wenn sie eine ihrer Kreationen in die Wildnis entlassen. Perikles, ein mit Luis befreundeter Virensammler, begründet seine Leidenschaft im Gespräch scherzhaft so: »Vielleicht bin ich an Viren interessiert, weil ich einen Entomologen-Komplex habe, wie Jünger. Jedenfalls finde ich es interessant, die Schwächen eines Betriebssystems zu erforschen.«

Dieses Forschungsmotiv taucht immer wieder in der Szene auf. Die 29a-Homepage nennt sich »29a Labs«, und deren Mitglied Griyo betreibt nebenbei noch seine private Website unter dem Namen »BiO.net - Virus Research Labs«. Antivirus-Forscher werden dagegen nicht müde zu betonen, dass ohne eine entsprechende Ethik, einen verantwortungsvollen Umgang mit dem Virencode, keine Forschung möglich ist. Doch die vX-Szene ignoriert solche Belehrungen forsch.

Gefängnis oder Job-Offerte?

Am 26. April 1998 entlässt der taiwanesische Wehrdienstleistende Chen Ing-hau seinen CIH-Virus in die Wildnis. Schon nach einer Woche gelangt der Virus über das Internet nach Europa und in die USA, wo er versehentlich mit Promotion-Downloads und kostenlosen CD-ROMs vertrieben wird. CIH wird damit kurzzeitig zu einem der meistverbreiteten Viren, und zu einem der gefährlichsten noch dazu: Am 26. April 1999 löscht er Daten auf dem Wirtscomputer. Auf einigen wenigen Rechnern gelingt es ihm sogar, das BIOS zu überschreiben. Chen Ing-hau wird nach Enthüllung seiner Identität kurzzeitig verhaftet, doch da niemand ihn in Taiwan verklagt, bald ohne Anklage wieder freigelassen. Wenig später wird er vom taiwanesischen Linux-Distributor Wahoo als Sicherheits-Experte eingestellt. Die Antivirus-Industrie reagiert empört.

Ein Jahr später allerdings wird sein Virus wieder aktiv. Diesmal findet sich ein taiwanesischer Student als Kläger, und Chen wird zu drei Jahren Gefängnis verurteilt. Ein Vertreter der Firma Sophos Anti-Virus erklärt: »Dies ist ein deutliches Signal an Virenprogrammierer, dass sie der Strafe für ihre Handlungen nicht entkommen werden.« [12]

Doch das Verhältnis zwischen Antivirus-Experten und der vX-Szene wird nicht allein von solch harten Law-and-Order-Tönen bestimmt. Sarah Gordon beispielsweise beschreibt die 29a-Mitglieder als »sehr nette Leute. Es hat mir immer Spaß gemacht, mich mit ihnen auszutauschen.« Ganz ohne Austausch kommen sie und ihre Kollegen aber auch gar nicht aus, wenn sie wollen, dass ihre Antiviren-Scanprogramme neue Schädlinge möglichst frühzeitig erkennen. Oft bekommen Antivirus-Programmierer diese direkt von den Autoren zugeschickt, die sich über eine kompetente Analyse ihrer Programmierleistung immer freuen. Luis berichtet außerdem, dass er seit Jahren mit Antivirus-Programmierern in Kontakt steht. »Sie benutzen mich als Quelle für ihre Arbeit und ich benutze sie als Quelle für meine Sammlung.« Glaubt man ihm, arbeiten in einigen dieser Firmen ehemalige Virenprogrammierer und sogar aktive Mitglieder der Szene. Ob er sich selbst vorstellen könnte, irgendwann bei solch einer Firma unterzukommen? »Irgendwann? Wenn sie gut genug zahlen schon morgen!«

Überlaufangebote werden allerdings auch an die andere Seite gemacht. Als der tschechische 29a-Programmierer Benny seinen Win98.Millenium-Virus entwickelt, gelangt eine Beta-Version auf unbekannte Weise in die Hände des rumänischen Antivirus-Spezialisten Adrian Marinescu. Marinescu veröffentlicht eine Analyse des Schädlings, und Benny ist voll des Lobs: »Gute Arbeit, Adrian!« Spaßeshalber fordert er ihn in einem Szene-Magazin auf: »Fuck of AV, join 29a!« [13] Adrian Marinescu gehört zu einer jungen Generation von Antivirus-Experten, die schon optisch nicht mehr viel mit den John McAfees und Peter Nortons dieser Welt gemeinsam hat. Er trägt einen Kinnbart, schlabbrige Klamotten und bezeichnet Biertrinken als eines seiner großen Hobbys. Bennys Angebot lehnt er trotzdem dankend ab: »Ich würde nie auf die andere Seite gehen. Für mich ist es kein Spaß, anderen Usern zu schaden. Einige Virenprogrammierer erklären, dass sie nur lehrreiche Viren schreiben, die niemandem schaden. Das ist nicht wahr. Schon weil sie sich selbst vervielfältigen, richten sie Schaden an.« Er selbst gehe Virenprogrammierern nicht aus dem Weg, sondern versuche sie davon zu überzeugen, ihr Hobby aufzugeben. Schließlich weiß er durch seine tägliche Arbeit: »Einige von ihnen sind begabte Programmierer.«

Primitive Makros und autonome Mutanten

Aber zur Umkehr bewegen konnte er noch keinen. Und so geht das Katz- und Mausspiel weiter. Am Freitag, dem 26. März 1999, taucht in der Newsgroup alt.sex erstmals ein Word-Makrovirus namens Melissa auf. Innerhalb weniger Stunden verbreitet er sich über Microsofts Outlook-E-Mail-Client in ganz Nordamerika. Das FBI beginnt mit der Suche nach dem Melissa-Autor. Als am Montag, dem 29.März, in zahlreichen Büros die Desktop-PCs wieder eingeschaltet werden, beschleunigt sich die Melissa-Verbreitung exponentiell. Mehr als 100.000 PCs werden angeblich an diesem Tag infiziert. Am ersten April wird David L. Smith als mutmaßlicher Melissa-Autor festgenommen. Zu seinem Verhängnis wird eine geklaute AOL-Adresse, mit der er den Virus in die Newsgroup eingespeist hat.

Melissa überrascht Antivirus-Hersteller wie Virenprogrammierer gleichermaßen. »Es erwischte uns mit heruntergelassenen Hosen«, erklärt Network-Associates-Forscher John Bloodworth ein Jahr später auf der Virus Bulletin Conference. [14] Durch die Kombination von Word-Macros und Fortpflanzung per E-Mail verbreitet sich der Virus so schnell, dass kaum ein PC ausreichend dagegen geschützt, kaum ein Nutzer darauf vorbereitet ist. Antiviren-Firmen müssen beobachten, wie Tausende von Computerbesitzern sich durch das Öffnen des Melissa-Attachments ins Verderben klicken. Doch auch die vX-Szene hat in den folgenden Wochen unter Melissa zu leiden. Das FBI besucht verschiedene ISPs und Webmaster von vX-Websites. Einige löschen daraufhin vorsichtshalber ihr komplettes Angebot. Auf der Seite des mutmaßlichen Melissa-Autors prangt heute nur noch ein Logo der Antivirus-Software AVP.

Für Schlagzeilen sorgen auch in den kommenden Monaten Melissaähnliche Makroviren wie etwa der I-Love-You-Virus. Doch aus Sicht der Szene sind diese Geschöpfe eher primitiv. Hier bastelt man lieber an möglichst schwer zu entdeckenden Viren wie dem Marburg-Virus oder dem HPS-Virus, die beide auf das Konto von 29a-Mitglied Griyo gehen und versehentlich von PC-Spielemagazinen verbreitet werden. Beide Viren benutzen polymorphe Techniken, um Virenscannern zu entgehen. Mittels zufallsbasierter Verschlüsselung verstecken sie sich in immer neuem Code, so dass sie über einfachen Code-Abgleich nicht mehr auffindbar sind.

Doch damit nicht genug: Noch komplexer wird die Angelegenheit, wenn sich zwei solcher Viren gegenseitig infizieren. Die Chancen, sie dann noch zu entdecken, sinken stark. Wird doch einer gefunden, kann dies noch katastrophalere Folgen haben. Wenn das Antivirenprogramm ihn entfernt und dabei den Code des unentdeckten Virus modifiziert, entsteht unter Umständen als autonome Mutation ein völlig neuer Virus - einer, der nicht entdeckt werden kann, der keinen Autor hat.

Viren im Reich der Pinguine

Im Februar 1997 erscheint dann mit Lin-Bliss der erste Linux-Virus. Viele haben bis dahin das Open-Source-Betriebssystem für immun gehalten, doch sie hatten offenbar noch nie etwas von Fred Cohen gehört. Schließlich hatte der schon 13 Jahre vorher festgestellt: Kein System ist sicher. Der einsetzende Linux-Boom verschärft das Problem noch. Gerade Linux-Anfänger, die sich die ganze Zeit als Systemadministrator (Root) einloggen, sind für Viren wie Lin.Bliss besonders anfällig. Im März 2001 gelingt 29a-Mkglied Benny

schließlich etwas Außergewöhnliches. Er veröffentlicht den ersten Virus, der sowohl Windows- als auch Linux-Rechner infizieren kann.

Viren wie dieser bieten Antivirus-Softwareherstellern zwar die Möglichkeit, ihren Markt auf neues Terrain auszudehnen, bergen aber auch neue Konflikte. Die Linux-Gemeinde ist eine völlig andere Informationspolitik gewöhnt wie AV-Firmen. Taucht unter Linux eine Sicherheitslücke auf, so wird dies auf einschlägigen Mailinglisten und in Weblogs wie Slashdot.org publiziert, damit Administratoren die Lücke auf ihrem System möglichst schnell schließen können. Quellcode und detaillierte Fehlerbeschreibungen gehören dabei geradezu zum guten Ton. Für Antivirus-Experten ist dagegen jede Publikation eines Viren-Sourcecodes unmoralisch. Sie tauschen Viren nur in geschlossenen Zirkeln aus und veröffentlichen lediglich Analysen ohne Sourcecode.

In der Sprache der Open-Source-Gemeinde heißt solch eine Praxis verächtlich »Security by Obscurity«. AV-Forscher argumentieren dagegen, dass man einen Virus nicht mit einer Sicherheitslücke in einer Firewall vergleichen kann. Diese könne mit den regelmäßig veröffentlichten Bug-Fixes schnell gestopft werden, danach sei das System sicher. Ein Virus müsse dagegen nur minimal verändert werden, um wieder ein Sicherheitsrisiko darzustellen. Der Moderator der Bugtraq-Mailingliste Elias Levy will dies nicht gelten lassen: »Darin liegt das Problem der ganzen Antivirus-Community. Der Hersteller hat niemals einen Bugfix veröffentlicht. Ihr seid so dadurch konditioniert, dass der Hersteller nie einen Bugfix veröffentlicht hat, dass ihr glaubt, es gibt keinen Bugfix.« [15]

Ein RFC für Netzwerkviren

Der Hersteller, von dem Levy hier spricht, ist natürlich Microsoft. Und auch wenn sich die Zahl der Linux-Viren sicher noch erhöhen wird, auch wenn mittlerweile schon Viren für Palm Pilots aufgetaucht sind und es bis zum ersten Playstation-2-Virus wohl nur noch eine Frage der Zeit ist, steht doch fest: Windows bleibt das Hauptbetätigungsfeld der Virenprogrammierer. Schon jetzt danken sie in ihren Publikationen gerne mal spaßeshalber Microsoft für die vielen Dinge, die ihnen diese Firma bisher ermöglicht hat. Luis ist sich sicher, dass sich daran auch in Zukunft nichts ändern wird: « Die interessantesten Trends werden weiterhin die sein, die mit Microsoft zusammenhängen. Viren werden, wie schon bisher, sehr davon abhängig sein, was Microsoft tun wird.«

Ein weiterer Trend liegt im Netz. Neben IRC-Würmern und Makroviren der zweiten Generation scheinen sich selbst updatende Viren der letzte Schrei unter Virus-Autoren zu sein. Erfunden hat diese Funktion ironischerweise die Antivirus-Industrie, um Kunden regelmäßig mit neuen Virendefinitionen zu versorgen. Doch schnell haben Virenprogrammierer entdeckt, dass sich auch ihre Geschöpfe neue Komponenten übers Netz besorgen können. Im 29a-Magazin vier veröffentlicht ein Programmierer namens Venca erstmals einen Virus, der sich zusätzliche Module - Venca nennt sie »Plug-Ins« - über eine Webseite herunterladen kann. Eine ähnliche Technik nutzt auch der MTX-Virus, der im Herbst 2000 große Verbreitung findet.

Noch einen Schritt weiter geht der ebenfalls von Venca programmierte Hybris-Wurm: Für ihn existieren bis zu 32 Plug-Ins, die verschlüsselt von einer Website heruntergeladen werden können. Diese ist mittlerweile geschlossen worden, doch Hybris ist damit nicht aus dem Rennen. Zusätzlich kann er sich seine Plug-Ins auch über die Newsgroup alt.comp.virus besorgen - ein Diskussionsforum, das auch von Antivirus-Experten genutzt wird. Andere Viren und Würmer updaten sich selbst über FTP-Server oder loggen sich

automatisch in einen bestimmten IRC-Channel ein, um weitere »Fernwartungskommandos« abzuwarten.

Doch das ist erst der Anfang. Längst feilen die Virenprogrammierer an komplexeren Netzwerk-Nutzungsmöglichkeiten. Ein Testfall dafür könnte der Gnutella-Wurm Gspot von 29a-Mitglied Mandragore gewesen sein. Er breitet sich im Juni 2000 unter Nutzern des Napster-ähnlichen Filesharing-Netzwerks aus, indem er Suchanfragen auswertet und diese pauschal positiv beantwortet. Sucht jemand etwa nach Photoshop, gibt Gspot sich als Photoshop.exe aus. Interessanter als dieser einfache Trick ist jedoch das Netzwerk, dessen sich der Wurm bedient. Was, wenn Viren ein eigenes Peer-to-Peer-Netzwerk aufbauen würden, um über den infizierten Computer unbemerkt Informationen und Updates auszutauschen? Was wie Zukunftsmusik klingt, ist vielleicht gar nicht mehr so weit von der Realität entfernt. Im 29a-Magazin Nummer fünf beschreibt ein gewisser Bumblebee ein Konzept, mit dem sich Viren selbst verschlüsselt über eine eigene Netzwerkstruktur updaten können. Scherzhaft beschließt er seinen Artikel mit der Aufforderung: »Let's start our own RFC!« [16]

Wem das einen kalten Schauer über den Rücken jagt, der sollte sich lieber an die Zukunftsperspektive eines Experten wie Adrian Marinescu halten: »Internet-basierten, selbst-updatenden, metamorphen Viren werden wir in den nächsten Jahren immer häufiger begegnen. Das sind die Techniken der Zukunft - aber ich wette, dass die in der Wildnis vorkommenden Viren im nächsten Jahr genau so albern sein werden wie etwa der I-Love-You-Virus.«

Literatur

[1] Rich Skrentas Virus gibt es mit Sourcecode auf seiner Website http://www.ski-enta.com/cloner/

[2] http://www.skrenta.com/cloner/clone-post.html

[3] Fred Cohen, Computer Viruses. Theory and Experiments, IFIP Conference 1984, online unter http://www.all.net/books/virus/part6.html

[4] http://venus.soci.niu.edu/~cudigest/CUDS5/cud521.txt

[5] Vesselin Bontchev, The Bulgarian and Soviet Virus Factories, Sofia 1991, online z. B. unter http://www.cornplex.is/~bontchev/papers/factory.html. Wie groß die Rolle der Pravetz-Heimcomputer an der bulgarischen Virenproduktion tatsächlich war, ist mittlerweile umstritten. Mehr dazu im Text von Ralf Bendrath in diesem Buch.

[6] Aus Sarah Gordons FAQ, online unter http://www.badguys.org/faq.htm

[7] 29a Magazine Nr. 5, Policies and goals, Online unter http://vx.netlux.org/dat/z001.shtml

[8] Frank Lüdke, Die Geschichte des Tremor-Virus, online unter http://www.outerspace.de/ccn/info-tremor.html

[9] Wie in vielen Fällen gaben Antivirus-Forscher dem Virus einen anderen Namen. In ihren Datenbanken hört er auf den Namen Boza. Um gegen diese »falschen« Namen der Computer Antivirus Research Organisation (CARO) zu protestieren, programmierte 29a-Gründer Mr. Sandman eigens den Anti-CARO-Virus. Entdeckt ein damit infizierter AVP-Virenscanner einen Boza-Virus, meldet er ihn als Bizatch-Virus. Genützt hat es nichts: Antivirus-Datenbanken führen Mr. Sandmans Protestvirus als Anti-AVP.1235.

[10] Mr. Sandman, Esperanto - kommentierter Sourcecode, veröffentlicht im 29a-Magazin Nr. 2, online unter http://vx.netlux.org/dat/z001.shtml

[11] Sarah Gordon, Technologically Enabled Crimc: Shifting Paradigms for the Year 2000, Computers & Security 1994, online unter
http://www.research.ibm.com/antivirus/SciPapers/Gordon/Crime.html
[12] http://www.sophos.com/virusinfo/articles/cihauthor.html
[13] BadByte Magazine Issue 3, online unter
http://www.badsector.org.uk/archives/badbyte/bbyte003.txt
[14] John Bloodworth, The AV Industry, Smug or Smart?, Virus Bulletin Conference 2000, online unter
http://www.virusbtn.com/vb2000/Programme/papers/bloodworth.pdf
{15] Zitiert nach: Sarah Gordon, Richard Ford, When Worlds Collide:
Information Sharing for the Security and Anti-virus Communities, Virus Bulletin Conference 1999, online unter http://www.research.ibrn.com/
antivirus/SciPapers/Gordon/VB99/vb99final.html
[16] RFC = Request for Comment, eine Art Standard für Internetdienste

Janko Röttgers lebt und arbeitet als freier Journalist und Autor in Berlin.
Mehr von ihm gibt es auf der Website www.lowpass.de.

Warum eigentlich Manila?

Peter Mühlbauer

Der Gedanke an Computerprogramme, die Gemeinsamkeiten mit Lebewesen aufweisen, sich fortpflanzen und die sogar gegen den Willen des Benutzers von Computer zu Computer wandern, war Anfang der 1980er Jahre ein aufregendes Betätigungsfeld für Wissenschaftier wie Jürgen Kraus oder Frederick B. Cohen. [1] Mitte des Jahrzehnts entwickelte sich die Wahrnehmung von Computerviren [2] weg von einer Sichtweise als interessantes wissenschaftliches Problem hin zu der einer Bedrohung. , Diese Ansicht hielt sich noch eine Zeit lang mit einer weniger hysterischen Sicht die Waage, doch als es 1987 nach Auftauchen der ersten Computerviren in freier Wildbahn beinahe täglich Meldungen zu Viren in der Tagespresse, in Fernsehen und Radio gab, war das neue Bedrohungsphantasma manifest geworden und die Zeitschrift PM-Computer titelte: »Virenprogramme. Droht uns ein Computer-Aids?« [3]

Die Quellen des Bösen

Der Ursprung der Immunschwäche AIDS wurde in den 1980er Jahren in Afrika ausgemacht. Die Feststellung der Herkunft von Computerviren erwies sich dagegen als nicht ganz so einfach. Ein erster Stolperstein auf dem Weg dahin war die Frage, wie viele Viren es überhaupt gibt. Der An-tivirensoftwarehersteller Sophos gibt die Gesamtzahl der derzeit erkannten Viren zum Stichtag 5. März 2001 mit 61.069 an, die McAfee Virus Information Library [4] nennt zum gleichen Zeitpunkt »mehr als 57.000« und Yun-Sun Wee von Symantec »mehr als 45,000« bekannte Computerviren. Das Problem mit der Anzahl der Viren rührt weniger daher, dass niemand sie zählt, als dass zu viele verschiedene Institute, Firmen, Forscher und Sammler sie zählen und dabei aufgrund der Schwierigkeiten zu unterschiedlichen Ergebnissen kommen. Virus Construction Sets liefern eine Vielzahl von Varianten bereits bekannter Virenkonstruktionen. Wie diese zählen? Sind stilistische Unterschiede belanglos oder machen sie einen neuen Virus aus?

Verwirrung stiftet dabei besonders die unterschiedliche Benennung von Viren. Trotz mehrerer Standardisierungsversuche, unter anderem durch die Computer Anti-Virus Research Organization (CARO) und die WildList Organization, gibt es keine allgemein gültigen Regeln für die Namensgebung. Auf diese Weise erhielt ein und dasselbe Virus oft völlig verschiedene Namen (wie etwa das auch unter dem Namen »Piter« bekannt gewordene 529-Virus). Früher wurden Viren gerne nach ihrer Größe benannt (wie etwa das 1704-Format-Virus), nach der Software, die sie angriffen (etwa beim dBASE-Virus), oder nach einem String im Programm (z.B. beim Brain-Virus). Heute werden Viren häufig nach

dem verwendeten E-Mail-Anhang oder nach der Betreffzeile der E-Mail benannt (z.B. beim ILOVEYOU-Virus). Sehr häufig verdanken Viren aber ihren Namen dem Ort ihrer Entdeckung (wie beim Jerusalem-Virus). Die geografische Ortung ist jedoch nicht immer eindeutig und zuverlässig: Im Juli 1996 tauchte das erste Excel-Virus gleichzeitig in Afrika und in Alaska auf. Auch muss der Ort der Entdeckung keinesfalls der der Herstellung sein: Das Arusiek-Virus beispielsweise wurde in Polen programmiert, aber in Marokko gefunden. [5]

Obwohl viele Viren nach Orten benannt sind, gibt es keinerlei auch nur annähernd aussagekräftiges Material zu den Herkunftsländern der Viren. Das liegt in der Natur der Sache: Ein Posting von John Elsbury in alt.comp.virus legt in ironischer Form die Gründe für die Unmöglichkeit solch einer Statistik dar: »Die Virus Publishers Association hat einen Standard für Länderkennungen definiert, die in der Seriennummer jedes autorisierten Virus enthalten sein müssen. Für gewöhnlich wird diese zusammen mit dem Barcode auf das Virus gestempelt.« [6] Was natürlich genau nicht der Fall ist. Die Programmierer der Viren geben ihre Identität im Allgemeinen nicht bekannt und die weitaus meisten Viren werden anonym verbreitet. Trotzdem existieren - etwa unter den Herstellern von Antivirensoftware - recht konkrete Vorstellungen über die Herkunft von Viren.

Yun-Sun Wee vom Antivirensoftwarehersteller Symantec beispielsweise nennt Osteuropa und Asien als Brutstätte von Viren. Zahlen hierzu kann sie auch auf Nachfrage nicht nennen. [7] Auch Torlav Dirro von Network Associates meint, dass »China, Taiwan und die Philippinen« derzeit die Hauptentstehungsgebiete von Viren seien, kann dies aber ebenso wenig mit statistischem Material belegen.

Dirro erklärt seine Sicht eines geografischen Herkunftsschwerpunkts mit strukturellen Faktoren wie der Verbindung von weit reichendem Zugang zu Computern und einer schlechten Situation auf dem Arbeitsmarkt. Eine Erklärung, die möglicherweise für China und die Philippinen, kaum jedoch für Taiwan gelten kann, dessen Arbeitslosenquote jahrzehntelang unter 2 % lag und die auch nach der Asienkrise 1998 nur auf 2,7 % anstieg. Nicht uneigennützig, aber auch nicht von der Hand zu weisen ist dagegen sein Argument, dass in Ostasien der Einsatz von Antivirensoftware weit weniger verbreitet sei als in Europa oder Nordamerika. Aber will man der Volksrepublik China tatsächlich den Einsatz von Antivirensoftware einer Firma empfehlen, deren CEO und Präsident, George Samenuk, sich auf einer PR-Veranstaltung Anfang 2001 in München damit brüstete, dass ein Großteil der Entwickler über Projekte von der amerikanischen Regierung bezahlt werde und er »sehr eng« mit staatlichen Stellen wie der NSA zusammenarbeite?

Der Mythos Bulgarien

Es gibt also keine verlässlichen Zahlen, wohl aber verlässliche Vorstellungen über Virenbrutstätten. Diese Vorstellungen der Herkunft von Viren sind eng mit zwei Faktoren verknüpft: mit kulturellen Phantasmen und mit politischen Gegensätzen.

»Es ist jetzt allgemein bekannt, dass Bulgarien die Produktion von Computerviren anführt und dass die SU dicht folgt«, schrieb Veselin Boncév [8] 1991 in seinem berühmten Aufsatz »The Bulgarian and Soviet Virus Factories« [9], und Winn Schwartau meinte in Information Warfare: »Viren werden im Allgemeinen einem unaufspürbaren und mythisch brillianten Virenschreiber zugeschrieben oder einfach nur > den Bulgaren.-: « [10] Wenige, aber sehr erfolgreiche Viren prägten das Bild von der bulgarischen Virenwerkstatt im westlichen Ausland. John McAfee zufolge stammten Anfang der 1990er zehn Prozent aller

Infektionen in den USA von bulgarischen Viren, der weitaus größte Anteil davon vom Dark-Avenger-Virus. [11]

Ende der 1980er Jahre stellte der bulgarische Virenforscher Veselin Boncév unter den Viren in seiner Heimat eine Dominanz originell programmierter Exemplare gegenüber Viren von der Stange fest. Seine Berichterstattung darüber spornte die Entwickler neuer Viren an: Einen Monat, nachdem Boncév in einer bulgarischen Computerzeitschrift die Infektion von größeren exe-Dateien als »sehr schwierig« bezeichnet hatte, erschien dort ein Virus mit genau dieser Eigenschaft. [12] Im November 1989 tauchte schließlich ein neues Virus in Bulgarien auf, das seinem Schöpfer einen Namen geben und ihm zu weltweiter Berühmtheit verhelfen sollte: Dark Avenger. Das Ungewöhnliche und Neue an diesem Virus war, dass es Dateien bei deren Öffnung infizierte. Auf diese Weise verbreitete sich das Virus sehr schnell.

Das Virus enthielt einen String, der am Anfang: »Eddie lives ... somewhere in time« und am Ende »This Program was written in the City of Sofia (C) 1988-89 Dark Avenger« enthielt. Ein für Virenprogrammierer ungewöhnlich offener Akt des Lokalpatriotismus verband sich mit einer bekennenden Leidenschaft für Populärkultur. In einem Interview gab der Dark Avenger einen Hinweis auf die Herkunft des Namens: »Der Ausdruck selbst kommt von einem alten Lied [...] und nicht von einem Iron-Maiden-Song, wie manche behaupteten. In vieler Hinsicht, denke ich, könnte man sagen, dass es den Dark Avenger schuf.« [13] Dark Avenger heißt ein Stück des 1982 erschienenen Heavy-Metal-Klassikers Battle Hymns von Manowar. Andere Viren des Dark Avenger wie das Number-of-the-Beast-Virus und das Anthrax-Virus sind ebenfalls als Metal-Zitate interpretierbar. Die Nennung des Iron-Maiden-LP-Titels Somewhere In Time in Verbindung mit dem Iron-Maiden-Monster Eddie im String deutet weiter auf einen Einfluss dieses populärkulturellen Bereichs hin, so dass der Dark Avenger auch in westlichen Viren-Zines wie 40Hex als »Metal-Head« und »Heavy-Metal-Fanatiker« erkannt wurde. [14]

Andere bulgarische Virenerzeuger orientierten sich ebenfalls mehr an internationaler Populärkultur als an östlichen Eigenheiten: W.T. nannte sein berühmtestes Virus nach einer Figur aus der Star-Wars-Reihe »Darth Vader« und in der bulgarischen Virus-eXchange-Mailbox bewegten sich Besucher mit Pseudonymen wie »Ozzy Ozburn« (sie!). Die Verbindungen zwischen Musik- und Computersubkulturen waren in den 1980er und frühen 1990er Jahren nicht nur in Bulgarien sehr eng, wie an zahlreichen Pseudonymen und Botschaften in kopierten Programmen deutlich wurde. Trotzdem erwarb sich nicht die Subkultur Heavy Metal einen Ruf als Brutstätte von Viren, sondern das Land Bulgarien. Das hat zum einen damit zu tun, dass (wie später noch zu sehen sein wird) sich die Nation-Form auch für die Übertragung weltpolitischer Ängste gut eignet (schließlich war Bulgarien einmal Teil des Ostblocks), zum anderen aber damit, dass die Subkultur-Form und die Nation-Form sich nicht konkurrierend, sondern ergänzend gegenüberstehen. Aus einem verstärkten kulturellen Austausch zwischen Nationen entstehen Formen der Populärkultur, die scheinbar unabhängig von Nationalkulturen und -Staaten sind. Dennoch sind solche Identitätsgeber in der Wahrnehmung von außen mit einer Nation-Form verbunden. Wie die Vorstellung von der Slacker-Generation mit Amerika oder die des Otaku mit Japan konnotiert ist, so war es die einer Virenprogrammierer-Subkultur in den 1990er Jahren mit Bulgarien.

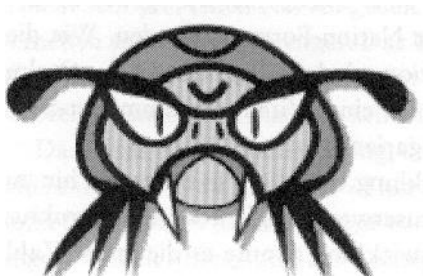
Veselin Boncév stellte die Entwicklung von Viren in Bulgarien hin zu einem Sport dar, der auch zum Statuserwerb tauglich war. An strukturellen Begünstigungen für diese Entwicklung nannte er die große Zahl gut ausgebildeter junger Menschen, die nicht in ökonomische Aktivitäten eingebunden waren. Noch zu Zeiten Shivkovs wurde in Bulgarien

auf die Ausbildung an und mit Computern ein planwirtschaftlicher Schwerpunkt gelegt. Das 8-Millionen-Land sollte zum Silicon Valley des Warschauer Pakts werden. Doch war Bulgarien deshalb noch lange kein Computerschlaraffenland, die Durchdringung mit Computern nicht mit Nordamerika oder Westeuropa vergleichbar. Ein Unterschied zu westlichen Ländern, der die Verbreitung von Viren begünstigte, war, dass es wirkliche »personal« Computer, mit denen nur eine Person arbeitete, kaum gab. Obwohl meist die Verbreitung über getauschte und geteilte Software als Hauptverbreitungsursache für Viren genannt wird, war es vor allem der Einsatz von Rechnern, an denen mehrere Personen arbeiteten, der die Verbreitung von Viren Anfang und Mitte der 1990er Jahre begünstigte - ein Faktor, der auch für andere Ostblockstaaten und für viele Schwellenländer galt. In der ehemaligen Sowjetunion waren die strukturellen Voraussetzungen nicht so günstig wie in Bulgarien: Es gab weniger Computer pro Kopf und die Ausbildung an Computern war weniger verbreitet. Auch lebten die Programmierer weiter voneinander entfernt. Die Entstehung einer Virenprogrammierer-Subkultur setzte hier etwas später ein, verhinderte aber nicht die Entwicklung einer Reputation als Virenschmiede. [15] Bekanntere sowjetische bzw. russische Viren sind zum Beispiel das Beer-, das Leningrad- und das Sverdlov-Virus.

Neben Bulgarien und Russland hat vor allem Asien den Ruf als Brutstätte von Viren. Hervorgerufen wurde diese Vorstellung unter anderem durch einige spektakuläre Viren, die ein großes Medienecho erregten, wie etwa das Tschernobyl- oder CIH-Virus aus Taiwan, das sich durch Spiele-Demo-CDs von Zeitschriften weit verbreitete, oder das ILOVEYOU-Virus aus Pandacan, einer Vorstadt von Manila.

Von Viren und Vampiren

Berühmte Viren führten zur Entstehung und Verfestigung der Vorstellungen über Virenbrutstätten. Aber berühmte Viren gab es auch aus anderen Ländern, von denen keine entsprechenden Vorstellungen existieren: Das Melissa-Virus wurde von einem Amerikaner programmiert, das Tequila-Virus von einem Schweizer Teenager und das Stoned-Virus von einem Studenten der University of Wellington in Neuseeland. Die Vorstellung über die Entstehung von Viren sucht sich trotz fehlender Zahlen und weltweiter Virenproduktion bestimmte Entstehungsschwerpunkte. Das Virus-Symbol der Antivirensoftware von Dr. Solomon vereinigt alle diese populären Vorstellungen der Herkunft von Viren in sich: ein Insekt mit rotem Körper, Leonid-Breschnjew-Augenbrauen, »Schlitzaugen« und Vampirzähnen. Die Nase erinnert zudem an ein chinesisches Schriftzeichen.



Bedrohungen kommen in der öffentlichen Wahrnehmung gerne aus der Fremde, durch ein imaginiertes »Anderes«. Der Balkan (der in solchen Vorstellungen im angloamerikanischen Raum durchaus bis nach Ingolstadt reicht) diente seit dem 19. Jahrhundert als solch ein Ort, in dem sich das Unheimliche und die Bedrohung gut ansiedeln ließen. Bram Stokers Dracula etwa kommt aus Transsilvanien [16] und in F. W. Murnaus Film Nosferatu bringen Ratten die Pest aus dem bulgarischen Varna, aus dem sich der Vampir ausschifft, nach Wismar. Die Wirksamkeit dieser Symbole trug mit zur

Entwicklung von Vorstellungen über die Herkunft von Viren bei. Ein Virus aus der Dracula-Stadt Varna, wie MG, DIR oder Shake, wirkt gleich weitaus bedrohlicher als eines aus Kalifornien.

Auch außerhalb Bulgariens griff man bei der Produktion von Viren gerne auf dieses Symbolgut zurück: Das erste Virus für Windows 95, Boza, wurde 1996 von einem Mitglied der australischen Virenprogrammierergruppe VLAD (wie Vlad Dracul) entwickelt. Andere Viren tragen Namen wie WereWolf (in Frankreich entdeckt} oder Frankenstein (unbekannter Herkunft). Asien ist ebenfalls seit langem ein Symbol für Bedrohungsphantasmen, vom Mongolensturm bis zum Entstehungsherd neuer Krankheiten: Die Pest kam im Mittelalter aus Zentralasien nach Europa, [17] und für die Grippeschutzimpfungen wird jeweils das Serum der im letzten Jahr in Asien verbreiteten Grippe benutzt. Auch die Maul- und Klauenseuche soll durch die Verfütterung von Speiseresten aus chinesischen Restaurants wieder nach Europa gebracht worden sein. In den USA war die populäre Darstellung von Chinesen seit dem Chinese Exclusion Act 1882 über den Boxeraufstand bis hin zum Schlagwort von der »gelben Gefahr« überwiegend negativ, was sich unter anderem in Figuren der populären Kultur wie dem mit chinesischen Attributen ausgestatteten bösen Ming aus der Filmserie Flash Gordon oder in Dr. Fu Manchu niederschlug. Über diese eingeführten Bilder funktioniert die Unterstützung der Herkunftsvorstellungen von Viren ebenso gut: So ist zum Beispiel das Fu-Manchu-Virus nach dem amerikanischen Bild des schurkischen chinesischen Wissenschaftlers benannt.

Viren als Waffen der Cyberterroristen?

Allein das Fehlen verlässlicher statistischer Daten macht das Feld Computerviren zu einer Brutstätte für Gerüchte und Verschwörungstheorien. Berücksichtigt man zusätzlich noch die weltpolitische Entwicklung, vertieft sich der Spekulationssumpf weiter.

»Experten warnen vor Hacker-Gefahr«, war der Titel einer Meldung des San Francisco Examiner vom 7. Dezember 1999. Darin warnte Alan B. Carroll, ein Beamter der amerikanischen Bundespolizei FBI, vor Computerangriffen in der Größenordnung des Bombenanschlags auf das World Trade Center und orakelte, ob sich wohl Osama Bin Laden bald am »Cyberterror« beteiligen werde. [18]

Wie sieht nun solch »Cyberterror« genau aus? Im März 2001 tauchte ein pro-palästinensisches Virus namens VBS/Staple-A auf - ein einfacher Visual-Basic-Script-Wurm, der Microsoft Outlook zu seiner Fortpflanzung nutzte. Eine E-Mail mit dem Betreff »RE:Injustice« enthielt einen Anhang namens »injustice.txt.vbs«. Die angehängte Datei sendete den Wurm an 50 Empfänger aus dem Adressbuch weiter. Außerdem schickte es an eine Liste von 23 E-Mail-Adressen vorwiegend israelischer Regierungsstellen eine Antwortmail mit höflicher Anrede und dem Inhalt, dass man »das« nicht von ihnen erwartet hätte. Schließlich ruft der Wurm mit dem Internet Explorer eine Reihe von URLs auf, die auf palästinensische Anliegen hinweisen. Zu guter Letzt entschuldigt er sich für die Störung und schildert den Fall des von israelischen Soldaten erschossenen zwölfjährigen Mohammad Al-Durra. Bei genauerer Analyse des Wurms findet sich in etwas fehlerhaftem Englisch eine Meldung, dass dies ein harmloses Virus ohne Schaden für das Betriebssystem sei und man sich keine Sorgen machen solle. [19]

Was pompös »Cyberterrorismus« genannt wird, beschränkt sich im Allgemeinen auf das Versenden von E-Mails oder auf das Verändern fremder Webseiten. Alles eine Frage der Definition: Unter Info War fällt zum Beispiel für das taiwanesische

Verteidigungsministerium jede Handlung, »mit der entweder die eigenen Daten geschützt oder diejenigen des Feindes verändert werden«. Eine sehr weit reichende Definition, durch die sich schon bei der Installation eines Virenscanners von Krieg sprechen lässt. [20]

Dabei ist das dokumentierte amerikanische Interesse an der Kriegsführung mit Viren durchaus älter als das chinesische: General Carl Stiner, Kommandant der U.S. Special Forces, kündigte schon Anfang der 1990er Jahre an, mit Computerviren beim Feind Chaos im Kommunikationssystem und in der elektronischen Steuerung von Waffen schaffen zu wollen. Als er am 4. März 1992 von Senator William Cohen vom Senate Armed Services Committee gefragt wurde, ob er mit der Entwicklung von Programmen zu tun habe, die feindliche Computerspeicher löschen, antwortete Stiner: »Ohne mich in Gebiete zu begeben, die der Geheimhaltung unterliegen, würde ich sagen, dass dieser Bereich ein großes Potenzial aufweist [...].« [21] Ein gutes Jahr später nahm die amerikanisehe School of Information Warfare and Strategy ihre ersten 16 Studenten auf. [22]

Da nach dem Ende der Sowjetunion außer China kein ernsthafter militärischer Gegner für das Pentagon in Sicht war, mussten zusätzlich David-Theorien zur Erhaltung der Budgets herhalten. Für Computerangriffe ist keine besondere industrielle und militärische Infrastruktur vonnöten. Sie wirken auch bei Schwellenländern glaubhaft. Solch eine »Computerattacke« ist eine tolle Sache für Journalisten, weil sich darüber schreiben lässt, ohne dass erstens tatsächlich etwas passiert und man zweitens wirklich an Informationen kommt. Die »Auskünfte« für solche Meldungen kommen meist von namenlosen Informanten aus dem Pentagon, aus Regierungs- und Geheimdienstkreisen oder von nicht näher genannten Sicherheitsfirmen.

Jeder Migrant ein potenzieller Virenprogrammierer

Die Bedrohung wird im fremden, unerforschten virtuellen Raum erwartet, deshalb reichen zu ihrer Erzeugung Gerüchte aus, ganz so, wie sie vom 16. bis in das 20. Jahrhundert hinein die Entdeckung und Eroberung außereuropäischer Gebiete begleiteten. Reiseberichte zeichneten ein Bild von den fremden Kulturen, das den Europäern eine Vielzahl von Gründen bereitstellte, über diese zu herrschen - Menschenopfer, Anthropophagie, exzessive Sexualität und rassische Minderwertigkeit. Die eingeführten Vorwürfe wurden im Laufe der Zeit immer weiter ausgebaut. Man versuchte seine Vorgänger durch zahlreichere und drastischere Schilderung von Sensationen zu übertrumpfen. [23] Auf diese Weise erfolgte beispielsweise die ideelle Rechtfertigung der Conquista in den Briefen des Hernán Cortés. »Diese Leute waren insbesondere widerspenstig und von mir durch Kriegsgewalt gefangen worden. Überdies waren sie Menschenfleischfresser. Dieweil dies allbekannt ist, ist es nicht vonnöten, dass ich Eurer Kaiserlichen Majestät Beweise überschicke«, [24] schrieb der Eroberer Mexikos an Karl V. und legte damit das Schema fest, das auch für die Berichterstattung über den Cyber- und Computervirenkrieg gilt: Wenn genug Menschen daran glauben, sind keine Beweise nötig.

Die Folge solch einer Virenkriegs-Hysterie ist neben der Brandmarkung von Ländern und Erdteilen als Brutstätten von Viren auch ein wachsendes Misstrauen gegen Minderheiten. Programmierer, die ganz oder teilweise ausländischer Herkunft sind, werden als potenzielle Cybersaboteure diffamiert. [25] Im August 1999 veröffentlichte die Zeitschrift Signal ein Interview mit Richard Clarke, dem »Nationalen Koordinator für Sicherheit, Infrastruktur schütz und Gegenterrorismus«. Der Arbeitnehmer fremder Herkunft wird darin zum potenziellen Saboteur gestempelt: »Viele amerikanische Hard- und Softwarefirmen

hängen in zunehmendem Ausmaß von Experten aus anderen Ländern ab. Die meisten dieser Leute bleiben in den USA und erwerben sogar die Staatsbürgerschaft, aber einige davon könnten dem Feind als Saboteure dienen, sei es durch Überzeugung, durch Erpressung oder durch Bestechung.« [26] Am 24. Oktober 1999 brachte die Los Angeles Times einen Artikel, in dem gewarnt wurde, dass vor allem indische Computerexperten, die US-Computer Y2K-tauglich machen sollen, gleichzeitig bösartige und militärisch nutzbare Viren auf den Rechnern installieren könnten. In der Meldung wird zwar ein CIA-Mitarbeiter zitiert, der Indien und Israel als in der Cyber-Rüstung besonders aktive Länder bezeichnet, aber es wird kein einziger konkreter Anhaltspunkt für solche Vorfälle genannt. [27]

Warum bildete sich gerade für Asien die Vorstellung einer Brutstätte für Viren heraus, nicht aber für Afrika oder Südamerika - Gegenden, aus denen durchaus Viren, wie etwa Freddy, Z-90, Blood oder StinkFoot kamen? Diese Gegenden wiesen im Gegensatz zu Osteuropa und zu Asien weder ein militärisches noch ein ökonomisches Bedrohungspotenzial auf. Die Vorstellung des Kontinents als Virenbrutstätte ist jedoch im Falle Asiens ebenso ökonomisch wie militärisch geprägt. Zu den wachsenden Spannungen zwischen den USA und China kam das Wirtschaftswunder der Tigerstaaten in den 1980er und frühen 1990er Jahren hinzu. In den 1980er Jahren waren Länder wie Taiwan und Südkorea zu Kapitalexporteuren geworden, während die USA Kapital importierte. [28] Vor der Asienkrise wurde ganz Ostasien in den Medien der USA überwiegend als ökonomische Gefahr dargestellt. Diese Situation fand auch nach der wirtschaftlichen Erholung der USA in den 1990er Jahren kulturellen und sozialen Niederschlag: Amerikaner asiatischer Abstammung wurden im Rahmen eines Pacific Rim Viewpoint als Erweiterung von asiatischen Nationen bzw. von asiatischem Kapital und damit als potenzielle Bedrohung wahrgenommen. [29]

Das Austragen von Weltpolitik auf dem Rücken von Einwanderern hat in den USA eine gewisse Tradition: Obwohl in den 30er Jahren viele Amerikaner japanischer Abstammung den japanischen Imperialismus scharf angegriffen hatten, wurden nach Beginn des Krieges mit Japan fast 112.000 Amerikaner japanischer Abstammung deportiert und in bewachten Lagern im mittleren Westen interniert. [30]

Viren als Strafe für Urheberrechts-Vergehen

Neben der Bürokratie gibt es noch weitere potenzielle Gewinner einer Virenkriegs-Hysterie. Als Nutznießer der Angst vor Viren sehen sich beispielsweise diverse Hersteller proprietärer Software. In mancher Äußerung zeigte sich schon nach dem ersten Auftauchen von Viren offene Genugtuung über die erwartete Einschränkung des Teilens von Software durch das Übertragungsrisiko. So schrieb Reuven Ben-Zvi in der israelischen Tageszeitung Ma'ariv nach dem Auftauchen des Jerusalem-Virus: »Die Computergemeinschaft ist dankbar, dass der Prozess des unautorisierten Kopierens von Software, der in jüngster Zeit unglaubliche Ausmaße angenommen hatte, gestoppt wurde. Genau wie AIDS, das das Safer-Sex-Phänomen hervorbrachte, ist das Computervirus dabei, ein Phänomen des ausschließlich anständigen Gebrauchs von Software hervorzubringen.« [31]

Eher fragwürdig ist deshalb die oft vorgebrachte Vermutung, dass ein Mangel an urheberrechtlicher Ethik die Produktion von Viren begünstigt habe; Weder hat - wie beispielsweise von Veselin Boncév behauptet 132] - die Umgehung eines Kopierschutzes etwas mit der Entwicklung von Viren zu tun (eher trifft dies für die Herstellung eines

Kopierschutzes zu), noch lässt die Benutzung nichtlizenzierter Software die Hoffnung auf eigene wirtschaftliche Erfolge durch Programmieren zwangsläufig schwinden und lenkt das kreative Potenzial auf die Produktion von Viren um.

So gab etwa der Dark Avenger in einem frühen Interview eine bemerkenswerte Obsession mit dem Urheberrechtsschutz preis und legte gleichzeitig dar, wie die Produktion von Viren und von proprietärer Software sich gegenseitig nutzen. » [..]. Viren würden sich weitaus weniger gut verbreiten, wenn die ‚unschuldigen' Benutzer keine Software stehlen würden, und wenn sie ein bisschen mehr an ihren Arbeitsplätzen arbeiten würden, statt Computerspiele zu spielen. Man weiß zum Beispiel, dass das Dark-Avenger-Virus durch Spiele von Europa in die USA transportiert wurde.« [33]

Gefährlicher als Viren: Abhängigkeiten

Eine dauernde und ernsthafte Bedrohung erwächst derzeit weniger durch einen vorgestellten geplanten Virenkrieg aus Asien oder Osteuropa, sondern aus realen Geschäfts- und Politikpraktiken, wie sie unter anderem von den Herstellern von Antivirensoftware eingesetzt werden. Die bekämpfbare Bedrohung sind nicht Viren, sondern Abhängigkeiten. Abhängigkeiten, wie sie durch Patente entstehen, die Methoden des Schutzes vor Viren monopolisieren. Patente, wie sie in der Medizin die Entwicklung und Produktion von Generika und von Alternativlösungen gegen Aids in Ländern wie Südafrika oder Brasilien bedrohen und wie sie zunehmend auch im Softwarebereich auftauchen.

Finjan Software, Inc., ein kalifornischer Anbieter von Sicherheitssoftware, gab am 1. Februar 2001 die Vergabe von Patent 6.167.520 durch das U.S. Patent and Trademark Office für seine Virenschutzlösung SurfinShield Corporate bekannt. Das Patent erstreckt sich auf die Überwachung des Herunterladens von Programmen und Inhalten aus dem Internet in Echtzeit, auf die Anwendung von Sicherheitsbestimmungen auf das heruntergeladene Programm und auf das Blockieren des Programms, falls gegen eine Sicherheitsbestimmung verstoßen wird.

Aktive Web-Inhalte stellen aufgrund der Möglichkeit ungewollter Dateizugriffe ein potenzielles Infektionsrisiko und somit eine Gefahr dar. Eine weitaus größere Gefahr aber ist ein Trivialpatent, das die Entwicklung von Lösungen für den Umgang mit dieser Gefahr verhindert.

Literatur

[1] Vgl. Jürgen Kraus, »Selbstreproduzierende Programme«, Dortmund 1981 (Forschungsberichte der Universität Dortmund, Abteilung Informatik 110), und Frederick B. Cohen, »Computer Viruses«, Los Angeles, CA 1986

[2] In der gesellschaftlichen Rezeption wird wenig Unterschied zwischen eigentlichen Viren, Würmern und Trojanern gemacht. Deshalb muss auch diese Untersuchung die Phänomene unter dem Begriff »Viren« zusammenfassen.

[3] PM-Computer 10/87, Zit. nach Ralf Burger, »Das große Computerviren-Buch«, Düsseldorf 1989 [1987], S. 34-35

[4] Network Associates Inc., »Virus Information Library«, http://vil.nai.com/vil/default.asp, Abfragedatum: 26. März 2001

[5] »F-Secure Virus Descriptions«, http://www.europe.f-secure.com/v-descs/arusiek.shtml, Abfragedatum: 31. 03. 2001
[6] John Elsbury, »Country Statistics«, Online-Posting vom 14. März 2001, abgefragt am 14. März 2001, news:alt.comp.vims
[7] Yun-Sun Wee, »Re: Fwd: Re: Country Statistics?«, E-Mail an den Autor vom 19. März 2001
[8] Bulgarische Namen wurden nach dem ISO-Standard Tafel I für die Transliteration südslawischer Sprachen wiedergegeben. Hier danke ich Maren Roth für Rat und Hilfe.
[9] Veselin Boncév, »The Bulgarian and Soviet Virus Factories«, in: Proceedings of the First International Virus Bulletin Conference, Buckinghamshire 1991, S. 11 – 25, http://www.complex.is/~bontchev/papers/factory.html, Abfragedatum: 31. März 2001
[10] Winn Schwartau, »Influenza, Malicious Software, and OOPS!«, in: Winn Schwartau (Hrsg.), Information Warfare. Cyberterrorism: Protecting Your Personal Security In The Electronic Age, New York 1996 [1994], S. 148-166, hier S. 155
[11] Veselin Boncév, »The Bulgarian and Soviet Virus Factories«, a. a. O.
[12] Karlhorst Klotz, »Die Virenjäger«, in: Computerviren '95, Chip Spezial Anwenderpraxis, Würzburg 1995, 48-50, hier: S. 48
[13] Sarah Gordon. »Inside the Mind of Dark Avenger«, in: Virus News International 20 (01) 1993, http://vx.netlux.org/lib/asg02.html, Abfragedatum: 28. März 2001
[14] »Interview with Skism One - AKA Lord SSS (triple S)«, in: 40Hex 1 (2), http://www.ladysharrow.ndirect.co.uk/library/Magazines/40hex/40hex21.htm, und »The Dark Avenger«, in: 40Hex 1 (2), http://www.ladysharrow.ndirect.co.uk/library/Magazines/40hex/40hex21.htm, Abfragedatum: 20. März 2001
[15] Veselin Boncév, »The Bulgarian and Soviet Virus Factories«, a. a. O,
[16] Hans Schmid, Michael Farin und Arnold Loy, »Nosferatu. Eine Symphonie des Grauens«, München 1999, S. 20 ff.
[17] Jacques Ruffie und Jean-Charles Sourm'a, »Les epidemies dans l'histoire de l'homme: essai d'anthropologie medicale«, Paris .1984
[18] »Experts warn of hacker threat«, in: San Francisco Examiner, 7. Dezember 1999, http://www.businesstoday.com/techpages/hacker12071999.htrn, Abfragedatum: 27. März 2001
[19] »Sophos Virus info«, http://www.sophos.com/virusinfo/analyses/vbsstaplea.html, Abfragedatum: 27. März 2001
[20] Florian Rötzer, «Taiwan sieht sich im Info War«,in: Tetepolis. Magazin der Netzkultur, 11. August 1999, http://www.heise.de/tp/deutsch/special/info/6466/1.html, Abfragedatum 29, März 2001
[21] »U.S. General Wants Ray Guns tor Commandos«, Reuters Newswire, 5. Mai 1992
[22] Winn Schwartau, »Introduction to Information Warfare«, in: Winn Schwartau (Hrsg.), Information Warfare. Cyberterrorism: Protecting Your Personal Security In The Electronic Age, New York 1996 [1994], S. 8-14, hier S. 8
[23] Erwin Frank, »Sie fressen Menschen, wie ihr scheußliches Aussehen beweist«, in: Hans-Peter Duerr (Hrsg.), Authentizität und Betrug in der Ethnologie, Frankfurt/M. 1987, S. 199-224
[24] Die Eroberung von Mexico durch Ferdinand Cortes. Mit den eigenhändigen Berichten des Feldherrn an Kaiser Karl V. von 1520 und 1522, Leipzig 1918, S. 188 (Memoiren und Chroniken 3)

[25] George Smith, »Electronic Pearl Harbor: A slogan for U.S. Info-warriors«, http://www.soci.niu.edu/~crypt/other/harbor.htm, Abfragedatum: 31. März 2001
[26] Robert K. Ackerman, »Hidden Hazards Mcnace U.S. Information Infra-structure«, in: Signal, August 1999, http://www.us.net/signal/Archive/August99/hidden-aug.html, Abfragedatum: 27. März 2001
[27] Elizabeth Shogren und Bob Drogin, »Some Fear Sabotage by Y2K Consul-tants«, in: Los Angeles Times, 24. Oktober 1999, http://www.warroornresearch.com/MediaPresenSpeak/LATimes.htm, Abfragedatum: 27. März 2001 über Google-Archiv
[28] United Nations, World Investment Report 1992, Transnational Corpora-tions äs Engines of Growth, New York 1992, S. 14-24, und Steve Chan, Introduction, in: Steve Chan (Hrsg.), Foreign Direct Investment in a Changing World, Houndmills 1985, S. 1-2
[29] Glenn Omatsu, Sammelrezension von Mike Davis, City of Quartz, David Rieff, Los Angeles. Capitol of the Third World, und David Reid, Sex, Death and God in L.A., in: Amerasia Journal 18 (3} 1992, S. 73-77, hier S. 75-76
[30] Su-Cheng Chan, »Asian Americans. An Interpretive History«, Boston 1991, S. 117-118 und 125
[31] Reuven Ben-Zvi, »The Virus Reached Haifa«, in: Ma'ariv. Zit. nach Philip Fites, Peter Johnston und Martin Kratz, »The Computer Virus Crisis«, New York 1989, S. 124
[32] Z. B. von Vesetin Boncév, »The Bulgarian and Soviel Virus Factories«, a. a. O.
[33] Sarah Gordon, »Inside the Mind of Dark Avenger«, a. a. O.

Peter Mühlbauer lebt in München und promoviert in Nordamerikanischer Kulturgeschichte.

Von Virus- Warnungen, die selbst zu Viren werden,
Virus-Hype und -Hysterie, viralem Marketing, Hoax-Politik
und der Kunst des Internet-Hoax

Einen Hoax will er sich machen

Armin Medosch

Good Times, der klassische Virus-Hoax [1]

Anfang Dezember 1994 begann eine E-Mail im Internet zu kursieren, deren erster Satz lautete: »Hier ist eine wichtige Information. Nehmt euch in acht vor einer Datei namens Goodtimes.« Im Folgenden warnte die kurze E-Mail davor, dass ein Virus in America Online zirkulieren wurde, das sich via E-Mail verbreitete. Wer eine E-Mail mit dem Titel »Good Times« erhielte, solle sie weder lesen noch herunterladen. Es handle sich um ein Virus, das die Festplatte löschen würde, fuhr die Virenwarnung fort und schloss damit, dass man diese Warnung »an alle seine Freunde weiterleiten« solle, weil man ihnen damit sehr helfen würde.

Schon wenige Tage nach dem ersten verbürgten Auftreten der »Good-Times«-Virenwarnung gab das dem US-Energieministerium angehörende CIAC am 6. Dezember 1994 in einem offiziellen Bulletin bekannt, dass die Good-Times-E-Mail ein Scherz ist, dass kein derartiges Virus existiert und dass folglich keine Gefahr von ihm droht. Man muss kein Computerexperte sein, um zu verstehen, dass sich Computerviren nicht durch das bloße Öffnen einer E-Mail verbreiten können. Viren oder E-Mail-Würmer können in ausführbaren Programmen verborgen sein, die mit einer E-Mail als Anhang mitgeschickt werden. Der bloße Textteil einer E-Mail kann keine solchen Ereignisse auslösen, wie eine Festplatte zu löschen. Doch weder der relativ simple Charakter der Scherzwarnung noch aufklärende Stellungnahmen von AOL, Systemadministratoren, Mailinglisten-Moderatoren, Anti-Viren-Experten und Virenschutzfirmen verhinderten die Ausbreitung von »Good Times«. Der Virus-Fehlalarm breitete sich in Universitäts-, Regierungs- und Firmennetzen aus, infiltrierte Mailinglisten, Newsgroups, Bulletin-Boards, überquerte den Atlantik und wurde schon bald in verschiedene Sprachen übersetzt. Nach einem ersten Höhepunkt der Epidemie im Winter 1994/95 schien sie nachzulassen, doch es kam immer wieder zu neuen Ausbrüchen. Wie bei Gerüchten, Klatsch und ähnlichen Botschaften, die dadurch am Leben erhalten werden, dass sie im Stil einer »Flüsterpost« weitererzählt werden, wurde der Inhalt der »Warnung« mit der Zeit erweitert. In einer Variante heißt es, dass »Good Times« deshalb so gefährlich sei, weil es durch die Speicherung im ASCII-Buffer des Rechners aktiviert werde. Eine Variation über diese Variation endet in der Behauptung, dass »der Prozessor in den Zustand einer unendlichen binären Schleife von n-facher Komplexität versetzt« werde, was schließlich zur Zerstörung des Prozessors führen würde. Auch solcher offensichtlich pseudo-wissenschaftlicher Humbug konnte die Ausbreitung

von Good Times nicht stoppen. Good Times mutierte unterdessen weiter und trat unter neuen Namen wieder auf, z. B. als »Irina«, »Deeyeda«, später als »Penpal Greetings«, und ist unter diversen Identitäten auch heute noch im Netz aktiv, zuletzt als »It takes guts to say Jesus«. Trotz aller aufklärerischen Anstrengungen der Kräfte der Vernunft sind Good Times und seine Nachfolger resistent gegen ihre vollkommene Auslöschung. Die Virenwarnung ist selbst zu einem Virus geworden.

Die Experten streiten darüber, von wem dieser Hoax in die Welt gesetzt wurde. In manchen Berichten heißt es, Good Times sei zugleich von einem AOL-Kunden und einem Studenten verschickt worden. Doch eine nachweisbare, erste Quelle gibt es nicht, ebenso wenig wie ein Bekennerschreiben. Beinahe glaubwürdiger, im Sinne der Legendenbildung, erscheint die Theorie eines »spontanen Entstehens« aus dem Humus des Internets. Danach könnte es sich um einen stark verdrehten Bericht über eine wahre oder halbwahre Begebenheit handeln. Einer anderen Variante zufolge habe es einen Kettenbrief mit dem Namen Good Times gegeben. Um diesen Kettenbrief zu stoppen, habe jemand die Behauptung in die Welt gesetzt, dass Good Times ein Virus enthalte. Nachweisbar soll hingegen sein, dass es vor dem Good-Times-Scherz einen Kettenbrief namens »Good Luck« gegeben hat. Das Weiterleiten dieser Kettenbrief-E-Mail um die Welt würde allen Beteiligten Glück bringen, hieß es darin.

Angriff auf die Rationalität

Good Times und Konsorten enthalten keinen Code, der wie ein echtes Computervirus den Daten auf der befallenen Maschine oder der Hardware selbst Schaden zufügen könnte. Dennoch verursachen Virenwarnungen, die selbst zu Viren geworden sind, objektive Schäden. Gerade in großen Organisationen kann die Produktivität nachlassen, wenn die Hälfte der Beschäftigten auf der Suche nach einem Virus ist, das es nicht gibt. Systemadministratoren leiden unter einem Bombardement mit E-Mails von besorgten Usern, die Angst um ihre Rechner und die darauf gespeicherte Arbeit haben. Insbesondere auf Mailinglisten kann sich so ein Fehlalarm nach dem Schneeballprinzip aufschaukeln. Auch die Entwarnung seitens des Listen-Moderators, der darauf hinweist, dass es sich um einen Hoax handelt, kann die Lawine manchmal nicht mehr stoppen. Unter Umständen verschafft die Entwarnung dem Hoax nur noch mehr Aufmerksamkeit. E-Mail-Server sollen unter der Last von Diskussionsbeiträgen, die von einem Hoax ausgelöst wurden, schon in die Knie gegangen sein. Wie hoch die Schäden in Form von Produktivitätsverlusten durch Virus-Hoaxes sind, darüber lässt sich gewiss streiten. Sicher ist nur, dass sich immer wieder jemand findet, der auf den Scherz hereinfällt, den Faden wieder aufgreift, den Teufelskreis wieder in Gang bringt - es gibt scheinbar keine technische »Schutzimpfung« gegen diese Art von »Virus«, wie sie z.B. Virenschutzprogramme gegenüber echten Computerviren bieten.

Ein Computervirus ist ein Programm, das sich von einem anderen Programm einverleiben lässt, dessen Aktivitäten es dann so steuert, dass es die Weiterverbreitung des Virus bewirkt, aber u.U. auch Dateien schädigt oder andere zerstörerische Vorgänge ausführt. Die Viruswarnung, die zum Virus wird, infiziert hingegen keine Maschinen, sondern Menschen. Der User macht sich zum Wirt eines Programms, das die einfache Handlungsanweisung »verbreite mich« beinhaltet. Damit ist diese Art von »Viren« eigentlich kein Technikthema. Ihr Erfolg beruht auf geschicktem »social engineering«, d.h. dem Überlisten verstandesmäßiger Barrieren und dem Anspielen auf urmenschliche

Eigenschaften wie Angst, Gutgläubigkeit und Hilfsbereitschaft. Die Taktiken der Virus-Hoaxer haben mehr mit Werbung, Literatur, Psychologie und Gruppendynamik zu tun als mit Technik.

Virus-Hoaxes benötigen bestimmte Sets von Voraussetzungen, um geglaubt zu werden und sich weiterzuverbreiten. Am meisten gefährdet, sich von falschen Virenwarnungen anstecken zu lassen, sind relativ unerfahrene Computer- und Internetnutzer. In die Hände der Viren-Hoaxer spielt auch das Klima der Virenhysterie, das von den Medien frühzeitig geschaffen wurde. Computerviren eroberten bereits zu einem Zeitpunkt die Schlagzeilen, als es noch relativ wenige davon gab und als die meisten Menschen noch keinen Personal-Computer benutzten, zumindest nicht zu Hause. Ihre Attraktivität als Medienthema stammt möglicherweise daher, dass Viren tief verwurzelte, irrationale Ängste ansprechen - die Angst vor der Seuche, die sich nicht kontrollieren lässt und die plötzlich Fehlfunktionen im menschlichen Organismus oder im Computer auslöst, die man sich nicht erklären kann, weil man zu wenig über das entsprechende Betriebssystem weiß. Doch neben dem Schüren von Ängsten werfen Virus-Hoaxes auch einen Köder aus: Wer die Warnung rechtzeitig weitergibt, macht sich damit bei seinen Freunden beliebt, wird zum Retter der Gemeinschaft, Virenwarnungen beziehen sich auch gerne auf eine Autorität, d. h. sie geben als Ursprung das Forschungslabor einer führenden IT-Firma oder die Kundendienststelle eines führenden Internet-Providers an. Nicht zuletzt benutzen falsche Virenwarnungen einen bestimmten Tonfall, d. h. bestimmte Schreibweisen und typographische Methoden, um die Empfänger in den Zustand gesteigerter Erregung zu versetzen, in der sich der Verstand am ehesten überlisten lässt. Sie verwenden häufig Großbuchstaben und eine Menge Ausrufezeichen, was in der E-Mail-Etikette dem Brüllen in der realen Welt entspricht. Sie versetzen den Empfänger in das Gefühl, Teilhaber einer exklusiven, aber extrem wichtigen Information zu sein, indem sie darauf verweisen, dass »kaum jemand bisher davon weiß«, aber dennoch das Virus »in 24 Stunden bereits Millionen Computer infiziert« habe. Die (un)logische Folge ist, dass man JETZT handeln, die Nachricht SOFORT an ALLE FREUNDE weiterleiten muss.

Doch genau dieses schematische Vorgehen, das heute vor allem auch bei kommerziellem E-Mail-Spam in verschiedensten Variationen benutzt wird, macht Virus-Hoaxes eigentlich leicht erkennbar. Wer das Prinzip, den semantischen und typographischen Aufbau solcher Fehlalarme einmal durchschaut hat, fällt aller Wahrscheinlichkeit nie wieder darauf herein. Und wer ganz sicher gehen will, braucht nur eine der Anti-Viren-Sites von Herstellern oder Universitäten aufzusuchen und in den Listen mit den letzten echten Warnungen und den letzten Hoaxes nachzusehen. Doch ein solcher faktengestützter Zugang ist genau nicht der Punkt an der Sache. Wenn alles mit rationalen Dingen zugehen würde, wäre Good Times nach zwei Wochen ausgestorben.

Das Universum der Hoaxer

Viren-Hoaxes sind so »programmiert«, dass sie den Verstand, den ewigen Zweifler, überlisten und sich wie ein trojanisches Pferd in die Gefühlswelt einschleichen. Dort verstehen sie es, die richtigen Knöpfe zu drücken, um uns zu veranlassen, ihre Vervielfältigung zu gewährleisten. Insofern ist die Virenwarnung ein Sondertyp einer sehr verbreiteten Art von Botschaft, die sich viral im Internet verbreitet. Dazu zählen weitere auf Computerthemen bezogene Hoaxes, Aufrufe zu humanistischen Aktionen, Pyramidenspiel-Kettenbriefe und via E-Mail verbreitete Urban Legends (Großstadtmärchen). Sonderfälle,

auf die noch einzugehen sein wird, sind virales Marketing und künstlerische und literarische E-Mail-Hoaxes. Überschneidungs- und Kategorisierungsprobleme gibt es mit Spam (siehe Seite 105 »Werde reich, glücklich und satt!« von Florian Schneider) und dem Cyber- und Infowar (siehe Seite 155 »Krieger in den Datennetzen« von Ralf Bendrath).

Die Motive der Hoaxer scheinen relativ klar zu sein. Bei den verschiedenen Formen von Hoaxes geht es definitionsgemäß immer um ein Moment der Täuschung. Jemand nimmt sich die Freiheit, seinen Mitmenschen einen Streich zu spielen, indem ihnen etwas vorgemacht wird, das nicht stimmt oder das es so nicht gibt. Die Belohnung für diese Hoaxer mag die klammheimliche Freude sein, dabei zuzusehen, wie sich die Ente im Netz verbreitet. Viele Hoaxes haben aber auch zusätzliche Motive. Diese sind oft kommerzieller Natur wie zum Beispiel bei den Kettenbriefen, bei anderen mag es um eine eher persönliche Racheaktion gehen, andere wiederum richten sich in einem David-gegen-Goliath-Kampf gegen die Macht von Regierungen oder großer Konzerne. E-Mail-Hoaxes sind spätestens seit Good Times nicht mehr wegzudenkender Teil der Folklore des Internets geworden. Sie sind so unausrottbar wie Spam, extrem ärgerlich, wenn sie in großer Zahl auftreten, günstigstenfalls so erheiternd wie ein guter Witz und manchmal von geradezu literarischen Qualitäten.

Der erste Virus-Hoax wird auf 1988 datiert [2] und hört auf den Namen »2400 baud modem virus«. Ein sich als Experte ausgebender Warner beschreibt ausführlich in technischem Jargon, wie sich das Virus über einen so genannten »Subcarrier« - einen Kanal, der »normalerweise nur für Protokoll-Austausch zwischen Modems« gebraucht wird - verbreiten würde. Nach längeren Tests kommt der Autor zu dem Ergebnis, dass ältere 1200-baud-Modems davon nicht betroffen werden und rät daher, nur diesen langsameren Modem-Typ zu verwenden. Eine der schönsten Enten, was Computer und Internet betrifft, war der Internet-Cleaning-Day, der vor einigen Jahren im Monat Februar ausgerufen wurde. Die E-Mail beginnt mit der überraschenden Feststellung, »wie viele von Ihnen wissen, muss das Internet jedes Jahr einmal für 24 Stunden zur Säuberung geschlossen werden«. Es ginge darum, dass das Netz von »toten E-Mails und inaktiven FTP-, Gopher- und WWW-sites« gesäubert werden müsse (als ob sich wie bei Arterien Schadstoffe an den Innenwänden ablagern würden und damit den Blutkreislauf gefährden). Damit die Caches und Proxies an den wichtigsten Knoten gereinigt werden könnten, sollten Betreiber von ständig mit dem Internet verbundenen Rechnern diese für einen Tag vom Netz nehmen und jede physische Verbindung kappen, damit bei der Aufräumaktion nicht unabsichtlich Daten gelöscht würden. Es gibt leider keine Informationen darüber, wie viele Webmaster dem Aufruf gefolgt sind. Ein anderer Internet-Hoax, der scheinbar nie ausstirbt, ist der von der E-Mail-Steuer in den Vereinigten Staaten, welche die Federal Communications Commission {FCC) im Rahmen eines neuen Gesetzes demnächst zu erheben gedenke. Weit verbreitet sind auch die menschelnden Hoaxes, die dazu aufrufen, den Frauen unter dem Taliban-Regime zu helfen oder ein krankes Kind zu retten.

In einer privaten Klein-Umfrage habe ich mich an Leute gewandt, die mir diese oder ähnliche Botschaften in der Vergangenheit zugeschickt hatten. Eine der aus den Antworten gewonnenen Erkenntnisse ist, dass das Weiterleiten solcher E-Mails eine Art schüchterner Versuch der Kontaktaufnahme sein kann. Man versucht mit einer größeren Gruppe von Leuten zu kommunizieren, mit denen man sonst nicht permanent in Kontakt steht. Die weitergeleitete E-Mail dient dabei als eine Art Visitenkarte, man macht sich nützlich, man zeigt, welche Interessen man hat, man ist nicht nur »drin« im Netz, sondern auch »dabei«, Teil eines E-Mail-Kontaktnetzes Gleichgesinnter. Wie die Antworten auch zeigen, ist das überwiegend ein Anfängerverhalten, mit dem man spätestens dann aufhört,

wenn die E-Mails, die man einst selbst im Glauben, Gutes zu tun, weitergeleitet hat, nach sechs Monaten wieder in der eigenen Inbox landen.

Ein Mem ist ein Mem ist ein Mem

Ein wesentlicher Punkt am Hoax-Phänomen ist, dass mit dem Weiterleiten von Virenwarnungen oder Kampagnen auf rufen eine »community« imaginiert wird, der man sich zugehörig fühlen will. Das Internet vermittelt uns das Gefühl, »nicht allein da draußen« zu sein. Das Vorhandensein von Gemeinschaft ist Voraussetzung für die Annahme und Weitergabe dieser E-Mail-Viren. Auch die Urheber von Fehlwarnungen und Kettenbriefen interagieren auf verkappte Art und Weise mit Gemeinschaften. Das wesentliche Motiv ist das der Verbundenheit über das Netz.

In der Phase des schnellen Wachstums des Internets aus den geschützten Gemeinschaften von Forschung, Militär und einigen wenigen Wirtschaftsbetrieben heraus in eine breitere Öffentlichkeit kursierten parallel dazu verschiedene theoretische Ansätze - von der »kollektiven Intelligenz« über das »globale Gehirn« bis hin zur »Memetik«. Sie bezogen sich auf diejenigen Umstände, die auch Viren-Hoaxes ermöglichen und es mag kein Zufall sein, dass diese Theorien ihre publizistischen Höhepunkte genau in der klimaktischen Phase des Good-Times-Hoaxes feierten. Gemeinschaft ist nicht mehr auf die physische Welt beschränkt, Klatsch und Tratsch werden nicht mehr nur in Cafes, auf Parties und bei anderen sozialen Ereignissen verbreitet, sondern elektronisch verstärkt und beschleunigt durch die geographisch verstreuten Gemeinschaften des Internets rund um den gesamten Erdball verbreitet.

Es würde das Thema dieses Artikels sprengen, die philosophischen und wissenschaftlichen Ansätze hinter den Begriffen kollektive Intelligenz, globales Gehirn und Memetik erklären und evaluieren zu versuchen. Doch zumindest die Meme sind als Erklärungsansatz für die Verbreitung von E-Mail-Hoaxes einen Seitensprung wert. [3]

Geprägt wurde der Begriff der Meme vom britischen Evolutions forscher Richard Dawkins. Er setzte die biologischen Begriffe Gen und Genesis analog zu der Entwicklung von Ideen als Meme und Memesis. Nach Dawkins sind Meme Gedanken, die sich zu erinnerbaren Einheiten formen und einen physischen Ausdruck besitzen. Diese würden von Menschen ohne eigenes Zutun akzeptiert, so dass sie sich zu Wirten dieser Meme machen. Und genau das lässt sich auch von Viren-Hoaxes sagen. Man kann sie als Sets von Informationen betrachten, die nach der eigenen Fortpflanzung trachten und dazu Wirte - uns Menschen - benötigen. Sie existieren in einer Aufmerksamkeitsökonomie in Gestalt der E-Mail-Inbox jedes einzelnen Rezipienten. Dort konkurrieren sie mit einer Vielzahl anderer Botschaften: private und arbeitsbezogene E-Mails, abonnierte Newsletter und Mailinglisten, Spam etc. In dieser ausgesprochen wettbewerbsorientierten Umgebung entscheiden zunächst zwei Faktoren darüber, ob wir es überhaupt der Mühe wert finden, die Nachricht zu öffnen. Das ist die Absenderadresse einerseits und die Betreff-Zeile zum anderen. Da Hoaxes meist mit dem Trick arbeiten, dass man sie an Freunde weiterleiten soll, haben sie hier schon einmal einen Pluspunkt zu verzeichnen. Und die meisten erfolgreichen Hoaxes haben eine genial einfache Betreff-Zeile. Eine E-Mail mit dem Betreff »Gute Zeiten« (Good Times) oder »Grüße von einem Brieffreund« (Penpal Greetings) öffnet man gerne, vor allem wenn sie von einem Freund kommt. Derselbe Mechanismus greift übrigens auch bei echten Computerviren, die über E-Mail verbreitet werden, wie zum Beispiel »I LOVE YOU« und zuletzt »Homepage«. Auch bei kommerziellen Spam-E-Mails

werden die Betitelungen immer raffinierter. Betreff-Zeilen der letzten Zeit lauteten zum Beispiel »from John« (fast jeder kennt irgendwen, der John heißt), »Information that you requested« (habe ich in letzter Zeit um irgendwelche Informationen angefragt? Kann sein ...) oder »Re: Your Future« (ein Thema, das immer interessant ist).

Ist die Hürde der Schlagzeile erst einmal genommen, die E-Mail also geöffnet, dann geht es ans Eingemachte. E-Mail-Viren und -Würmer beruhen darauf, dass man dann auch noch das zugehörige Attachment Öffnet (und in einer E-Mail-Umgebung arbeitet, welche die Ausführung des Attachments erlaubt). E-Mail-Hoaxes beruhen darauf, dass man sie weiterleitet, weil man ihnen glaubt oder sie zumindest für interessant genug hält, sie anderen zuzumuten. Was danach folgt, ist, im Einklang mit Dawkins Meme-Theorie, darwinistische Auslese auf dem Gebiet der Ideen. E-Mail-Hoaxes versuchen möglichst starke Gefühle anzusprechen - Angst, Sex, Profit, Einsamkeit bzw. den Wunsch nach Zugehörigkeit, Geltungsdrang, Neugierde -, die in uns evolutionäre Trigger auslösen und uns veranlassen, den Panik-Button zu drücken: Forward ...

Kritiker der Memetik sind nicht einverstanden damit, dass, wie sie meinen, sozialdarwinistische Evolutionslehren auf das Feld der Kultur angewandt werden. Sie argumentieren damit, dass wir uns in einem bestimmten historischen Entwicklungsabschnitt der Zivilisation befinden, den man in der westlichen Welt mit den Begriffen Kapitalismus und Demokratie identifizieren kann, die jedoch nicht als gleichbedeutend mit einer »naturgesetzlichen« Evolution betrachtet werden könnten. Nicht zuletzt ist ihnen die angenommene Passivität ein Dorn im Auge, da der Memetik zufolge die parasitenhaften Meme uns nur als passive Träger benutzen. [4]

Hoax-Politik

Ein zentraler Internet-Mythos ist, dass die so genannte Many-to-many-Kommunikation, die Kommunikation vieler mit vielen, das traditionelle Sendermodell einer zentralen Nachrichtenquelle, die an viele Empfänger ausstrahlt, ablösen würde. Diese These ist zwar nicht bewiesen, denn selten gibt es eine klare lineare Abfolge von Entwicklungen, wobei ein System ein anderes ersetzen würde, doch manchmal erweist sich die Weitergabe von Nachrichten in Freundschafts- und Bekanntschaftsnetzen via Internet tatsächlich als mächtige Kommunikationsmaschine. Der signifikanteste Ausdruck dieser dezentralen Kommunikation sind heute technische Peer-to-peer-Netzwerke (P2P) im Stil von Napster oder Gnutella. Aber auch ohne technische Realisation zeigt Peer-to-peer immer wieder einmal seine Macht, so wie z. B. im Frühjahr 2001 im Falle einer die Firma Nike betreffenden E-Mail, die um die Welt ging.

Der Sportartikelhersteller bietet Käufern neuer Turnschuhe der oberen Preisklasse die Möglichkeit an, diese personalisieren zu lassen, indem man gegen einen kleinen Aufpreis über eine Website bestellen kann, dass ein Schriftzug eigener Wahl in die Schuhe gestickt wird. Wie es die Saga will, bestellte ein amerikanischer Student, dass der Begriff »Sweatshop« eingestickt wird. Dieser steht für ausbeuterische Arbeitspraktiken in Fabriken, die nicht den Standards des Arbeitnehmerschutzes der westlichen Welt entsprechen - und die Firma Nike hat seit Jahren unter Vorwürfen zu leiden, bei ihren von Subkontraktoren betriebenen Produktionsstätten in der Dritten Welt ebensolche Sweatshop-Zustände zumindest zu dulden. Als Nike es dem Kunden abschlug, diesen Schriftzug einzusticken, entwickelte sich ein ebenso interessanter wie amüsanter E-Mail-Dialog zwischen Kunde und Firma, bei dem der süffisante Fragesteller dem antwortenden

Firmenvertreter immer wieder neue verbale Windungen abnötigte. Dieser E-Mail-Dialog wurde in Umlauf gebracht und verbreitete sich mit viraler Ansteckungstendenz. Nachdem ich diese E-Mail zum ersten Mal auf einer Mailingliste gesehen hatte, erhielt ich sie innerhalb weniger Tage mindestens 20 Mal von verschiedensten Seiten zugeschickt. Wie groß der Imageschaden für Nike durch diese Selbstläuferkampagne tatsächlich ist, lässt sich schwer beurteilen, aber jedenfalls handelte es sich um. einen Fall der E-Mail-Ansteckung, der letztlich in den etablierten Medien landete und weltweit zum News-Item wurde.

Falsch wäre es aber, einen solchen Vorfall als Beweis für die dezentrale, demokratisierende Macht des Internets und damit als ein absolutes Gutes zu feiern. Solche »Erfolge« der P2P-Kommunikation beruhen auf bestimmten, schwer zu steuernden Voraussetzungen und lassen sich nicht generalisieren. Andere E-Mail-Hypes der jüngeren Vergangenheit lehren einen eher das Grauen, wie der Fall einer englischen Büroangestellten. Diese hatte sich von einem jüngst kennen gelernten Liebhaber in einen Austausch erotischer E-Mails verwickeln lassen. Dieser arbeitete in einer großen Firma und leitete die gesammelten Ergebnisse des Austauschs voller Stolz an seine fünf besten Freunde in der Firma weiter. Die fanden das so toll, dass sie die E-Mail ebenfalls an ihre jeweiligen Freunde weiterleiteten, und so weiter und so fort ... Innerhalb von 24 Stunden sollen angeblich Millionen Menschen in den Genuss ungeschminkter Diskussionen über oralen Sex gekommen sein. [5]

Die Bottom-up-Power aus dem Internet für einen groß angelegten Polit-Hoax zu nutzen, gelang der Kommunikationsagentur Ubermor-gen.com im Vorlauf zur amerikanischen Präsidentschaftswahl 2000. Ubermorgen.com, bestehend aus Luzius Bernhard - auch auftretend als Hans Bernhard, Hans Etxtrem und NET_Callboy - und Partnerin LIZVLX, zählt neben Hoaxes auch Schock-Marketing und Drama-Marketing zu ihren bevorzugten Taktiken. Ziel und Zentrum ihrer Täuschungs- und Konfrontationsmanöver ist aber, was sie den »Medien-Hack« nennen: so schnell wie möglich in CNN zu kommen.

Das gelang ihnen im Herbst 2000 mit Voteauction.com, einer Web-Plattform für die Versteigerung von Wählerstimmen zur US-Präsidentenwahl - und eine sehr freie Interpretation der freien Marktwirtschaft. Ein amerikanischer Student hatte Voteauction.com ursprünglich als Protest gegen die US-Praxis der Wahlkampffinanzierung programmiert, wo Firmen und Branchen-Lobbys über Spenden Einfluss auf die zukünftige Politik zu gewinnen versuchen. Nach einer gerichtlichen Verfügung im Staat New York übernahmen Bernhard und Partner die Site, setzten den Server außerhalb der USA auf und begannen mit einer E-Mail-Kampagne Aufmerksamkeit auf die Aktion zu lenken. Mit dem Argument, dass, wenn die Politik käuflich ist, auch einfache Wähler davon profitieren können sollten, entfachte Voteauction.com schnell einen Publicity-Wirbel. Erregt wurde allerdings auch die Aufmerksamkeit amerikanischer Gerichte, die durch Verfügungen und Domainsperrungen das offenbar illegale Treiben zu unterbinden versuchten. Doch das verschaffte Voteauction (später mutiert zu vote-auction.net, wo heute noch ein Erlebnisbericht zu lesen ist) nur noch mehr Publicity, und am Ende des Medien-Hacks gab es über 400 Zeitungsartikel und Fernsehberichte sowie fünf anhängige Gerichtsverfahren in verschiedenen US-Wahlbezirken. Tatsächlich versteigert wurde jedoch keine einzige Wählerstimme, da die ganze Aktion von vornherein als Fake - oder Web-Hoax - aufgebaut worden war.

Virales Marketing

Die Macht der Ansteckung von Virus-Hoaxes und E-Mail-Enten wurde nicht zuletzt auch von Wirtschaftstreibenden wahrgenommen. Seit einigen Jahren schon geht der Modebegriff vom »viralen Marketing« um. Ausgangspunkt dafür ist, dass sich bestimmte Konsumentengruppen, vor allem medien- und markenbewusste Jugendliche, immer resistenter gegen klassische Formen der Werbung zeigten. Deshalb begann man mit subtilem »Branding« von Veranstaltungen wie Clubbings und Raves, Snowboard- und Skateboard-Events. Die ultimative Idee dabei ist, dass die Sponsoren nicht einmal mehr ihr Logo in Zusammenhang mit einem Event bringen, sondern selbst zum Event werden. Die Konsumenten sollen aus eigenem Antrieb die Kampagne erzeugen, indem sie einen von der Firma ausgeworfenen Köder aufgreifen und untereinander weitergeben. Günstigstenfalls kann der Köder, wie im Fall von »Flat Eric«, selbst zu einem Popstar werden. Die Assoziation mit dem Auftraggeber erfolgt dann durch die Hintertür, da die Kampagne keineswegs aufgesetzt wirken darf: Es muss alles so aussehen, als wäre ein solches »Medien-Ereignis« tatsächlich nur von den Kunden selbst erzeugt worden.

Weniger metaphorisch als vielmehr praktisch wird das virale Marketing in der Szene der Virenschutz-Softwarefirmen verstanden. Dort gab es schon früh immer wieder Vorwürfe, dass manchen Firmen die Aufmerksamkeit, die Medien Viren entgegenbringen, und die daraus resultierende Viren-Hysterie gar nicht so unrecht sei. Das reicht bis hin zu der Anschuldigung, dass auch schon mal echte Viren ausgesetzt worden seien, nur um dann gleich den entsprechenden digitalen Impfstoff bereitzustellen (siehe dazu auch Seite 53 »Sie lieben uns.txt.vbs« von Janko Röttgers).

Selbst Branchengrößen sind schon ins Gerede gekommen, wenn es darum ging, im Sog von Viren-Hypes wie »Melissa« und »ILOVEYOU« die Nutzerbasis zu vergrößern. Meist scheinen es aber die kleineren Außenseiter zu sein, die durch negative Publicity ihren Marktanteil zu steigern versuchen. Berichte auf einschlägigen Websites wie vnunet.com zeugen von solchen Vorfällen, bei denen Firmen Warnungen über angebliche Virenepidemien verbreiten, die sich letztlich als drastisch übertrieben herausstellen. Die Spitze der Ironie ist, wenn, wie auch schon geschehen, die Virenschutzsoftware selbst falsche Viruswarnungen erzeugt. So soll der Virus-Scanner eines großen Herstellers die berechtigte Warnung eines kleineren Herstellers vor dem Homepage-Wurm fälschlicherweise als Virus identifiziert und daraufhin Viruswarnungen verschickt haben. Am Ende scheinen auch die Virenschutzprogramme selbst nicht mehr vor Virus-Hoaxes gefeit zu sein.

Den zweifelhaften Ruhm, den klassischen Virus-Hoax als verkaufsförderndes Mittel für ein computerfremdes Produkt eingesetzt zu haben, darf ein Buchverlag für sich beanspruchen. 1996 erschien eine Virus-Warnung mit der Betreff-Zeile »Irina« auf den Bildschirmen. [6] Ein Virenforscher erkannte die Ähnlichkeit zum Good-Times-Hoax und verbreitete seine Erkenntnis auf entsprechenden Bulletin-Boards. Laut einer englischen Tageszeitung handelte es sich um einen auf die schiefe Bahn geratenen PR-Gag. Der Verlag Penguin Books stand im Begriff, einen Roman namens »Irina« im Web zu publizieren. Der damalige Leiter für Electronic Publishing soll die falsche Viruswarnung »Irina« an ausgewählte Zeitungen geschickt haben, allerdings ohne Erwähnung von Penguin Books und dessen interaktivem Buchprojekt. Als Absender der Viruswarnung war ein Professor Edward Prideaux vom (nicht existierenden) »College of Slavonic Studies in London« angegeben.

Den Begriff »virales Marketing« etwas zu wörtlich aufgefasst haben drei holländische Jugendliche, die sich dazu bekannten, den Homepage-Wurm in die Welt gesetzt zu haben. [7] Sie nutzten das inzwischen hinlänglich bekannte Feature aus, dass Microsofts Outlook über eine API andere Programme zur Ausführung von Scripts bewegen kann. »Homepage« bewirkte, dass User, die das Attachment HOMEPAGE.HTML.VBS anklickten, damit unter anderem vier Fenster des Internet-Explorers öffneten, die zu Porno-Sites führten. Ob die Urheber tatsächlich Geschäftsinteressen mit diesen Pornosites verbanden, ist nicht bekannt. Laut eigenen Angaben hätten sie nur gehofft, dass sie mit ihrem Wurm eine Karriere in Sachen virales Marketing starten und den Menschen »die Freuden, im Netz bösartig zu sein«, zeigen könnten.

E-Mail-Hoaxes in der Netzkunstszene

Wie kaum anders zu erwarten, erfreuen sich E-Mail-Hoaxes in der Netzkunstszene besonders großer Beliebtheit. Vor allem in der Literatur haben Hoaxes eine große Tradition. In Briefwechseln ausgetragene Fehden zwischen rivalisierenden Fraktionen, mit falschen Namen gekennzeichnete Artikel und Pamphlete und in verleumderischer Absicht ausgestreute Gerüchte bestimmten die Infights von Künstlergenerationen und ließen in deren Zirkeln die Wellen hochschlagen - wobei dieselben Erregungen Außenstehende meist völlig kalt ließen. Und so ereignete es sich auch in der elektronisch beschleunigten Kommunikation der Netzkunstszene in der zweiten Hälfte der neunziger Jahre. Diese Phase sah eine Wiederbelebung eines netzgestützten Neokonzeptualismus, bei dem die Kommunikation oft wichtiger erschien als die Produktion von Werken. Das ist allerdings kein Vorwurf, sondern eine Feststellung. In einer Zeit stürmischer Entwicklung scheint die reine Fortbewegung entlang den Entwicklungslinien neuer Ideen und die Ausdifferenzierung und Abgrenzung zu rivalisierenden Ideen wichtiger als das Festhalten an einmal gefundenen Wahrheiten. Unter diesem Gesichtspunkt ist das rege Interesse an Hoax-Taktiken in der Netzkunstszene zu sehen, wobei die Annahme falscher Identitäten in E-Mails und die Verbreitung falscher Tatsachen unter solchen Deck-Identitäten eine der beliebtesten Vorgehensweisen ist.

Allzu plump packte es jener unbekannte Hoaxer an, der auf der Mailingliste Syndicate einen Streit zwischen dem Medientheoretiker Geert Lovink und dem Netzaktivisten und ICANN-Spezialisten Ted Byfield zu inszenieren versuchte. Allerdings glaubte wohl kaum jemand nur eine Sekunde daran. Es passte einfach nicht zum Persönlichkeitsprofil dieser gewieften Netz-Szene-Stars, sich öffentlich Kraftausdrücke wie »Arschloch« an den Kopf zu werfen. Auch war der Absender nicht wirklich kunstvoll versteckt, sondern leicht via Analyse des E-Mail-Headers als von einem schwedischen anonymen Remailer kommend zu identifizieren. Schon mehr Mühe gab sich ein Hoaxer, der die E-Mail-Identität des Kunstkritikers und Theoretikers Timothy Druckrey sowie des Schriftstellers und Künstlers Mark Amerika annahm und unter ihren Namen Beiträge auf Mailinglisten postete, die geeignet schienen, Unfrieden zu stiften und so Stimmung gegen Druckrey und Amerika zu machen. Gegen den oder die Hoaxer arbeitete, dass sowohl Druckrey als auch Amerika einen höchst individuellen Schreibstil pflegen, der trotz ersichtlieber Mühe nicht wirklich glaubhaft nachgeahmt wurde. Trotz dieses Mangels hatte dieser Sturm im Wasserglas zumindest ein gewisses literarisches Flair.

Dass sich kleine, eng verbundene Netz-Communities besonders gut als Ziele für Hoaxes eignen, zeigten jene Hoaxer, die 1999 die Preisentscheidung des Medienkunstfestivals Ars

Electronica diskreditierten. [8] Damals ging pünktlich zum Start des Festivals eine E-Mail in einschlägigen Mailinglisten um, die den Anschein erweckte, als Protestnote von vier der fünf Juroren des Prix Ars in der Kategorie .net verschickt worden zu sein. 1999 war der begehrte Preis an das Betriebssystem Linux vergeben worden. Die vier angeblichen Juroren beschwerten sich darüber, dass die Abstimmung vom fünften Juror im Interesse von Sponsoren des Festivals manipuliert worden sei. Das Festival sponsernde große IT-Unternehmen, so stand in der Aussendung zu lesen, würden planen, demnächst selbst Linux-Distributionen anzubieten und hatten deshalb ein Jury-Mitglied bestochen, um den Linux-Hype weiter hochzupushen. Obwohl völlig aus der Luft gegriffen, spielten die Vorwürfe geschickt auf Erwartungshaltungen in der Netz-Community an und fügten sich nahtlos in den Linux-Hype, der damals einen ersten Höhepunkt erreichte, mit dem Ergebnis, dass die Gerüchteküche in der Netzkunstszene brodelte. Auch die Aufdeckung des Hoaxes in Telepolis konnte den einmal geweckten Verdacht nicht mehr völlig aus der Welt schaffen.

Beinahe schon legendär ist der kombinierte E-Mail- und Web-Hoax, den die Künstler-Gruppe Etoy im Frühjahr 1996 mit dem »Digital Highjack« inszenierte. Zunächst analysierten Etoy mit Hilfe von Software-Robotern die fünf gängigsten Search-Engines, um herauszufinden, welche Suchbegriffe am häufigsten eingesetzt würden und wie diese Begriffe im Source-Code von Webseiten eingesetzt werden mussten, um im Ranking der Suchmaschinen möglichst hoch oben zu liegen. Das Ranking folgte damals noch recht einfachen Prinzipien. Der entsprechende Suchbegriff musste möglichst häufig vorkommen, allerdings im Fließtext und nicht einfach 50 Mal wiederholt in einem HTML-Tag am Anfang der Seitenbeschreibung. Entsprechend den gewonnenen Ergebnissen programmierten Etoy Websites, welche häufig abgefragte Begriffe wie »Sex« oder »Porsche« enthielten, mit dem Ziel, möglichst unter die ersten 30 Auflistungen einer Abfrage zu gelangen. Landeten Suchende dann auf einer Etoy-Site, wurden sie mit Hilfe des »Refresh«-Metatags, das in vorprogrammierten Intervallen ohne Zutun des Users neue Seiten aufruft, in deren Webseiten-Labyrinth »gefangen gehalten«. So gelang es Etoy, über den Zeitraum einiger Monate hinweg ca. eineinhalb Millionen User zu »entführen«. Mit begleitender E-Mail-Kampagne und entsprechend extremer Rhetorik von der »digitalen Entführung« gelangten Etoy in das damals sehr einflussreiche Wired-Magazine und gewannen den ersten Preis in der Kategorie Netzkunst des Prix Ars Electronica. [9]

In geistiger Nähe dazu stehen die Aktionen der Gruppe RTMark, die sich auf die Gestaltung gefälschter Politiker- und Firmen-Websites spezialisiert hat und mit zwischen Fakt und Fiktion balancierenden Pressestatements Besucherströme hin zu diesen Sites zu lenken versteht. Ebenfalls praktische Streiche zu lancieren pflegten Heath Bunting und Rachel Baker, die über ihren Server irational.org unter anderem gefälschte Studentenausweise aus Mexico City vertrieben, Surfer zum Bespitzeln ihrer Mitbürger via Polizei-Webcams aufforderten und zusammen mit dem russischen Künstler Alexeij Shulgin »Internet-Gold-Medaillen« an die geschmacklosesten User-Homepages verliehen. Das Künstlerpaar Jodi gestaltete Websites, die mit der Angst der User vor dem Browser-Crash, Viren und Systemabstürzen spielten. In einer frühen Arbeit bezogen sich Jodi auch explizit in einer Hommage auf den Good-Times-Hoax. [10] Zusammen mit dem in Slowenien lebenden Künstler Vuk Cosic können Bunting, Baker und Shulgin für sich beanspruchen, den Begriff net.art in ebendieser Schreibweise geprägt und die frühe Netzkunst entscheidend mit beeinflusst zu haben. Ihr gemeinsamer letzter Hoax scheint zu sein, dass sie sich - mit Ausnahme von Jodi - seit ca. 1999 als »retired net.artists« bezeichnen, als Netzkünstler in Frühpension sozusagen.

Was die genannten Künstler verbindet, kann als erfolgreiches virales Marketing im Netz bezeichnet werden. Ohne durch die herkömmlichen Instanzen des Betriebssystems Kunst gegangen zu sein, schufen sie sich rein durch Kommunikation im Netz ein Publikum und damit einen gewissen Grad an Berühmtheit. Das Ausstreuen medialer Viren, die sich wie trojanische Pferde in die Informationsverarbeitungssysteme der User einschlichen, steigerte ihren Netzwert - besser ist das Englische »net value« - als Künstler. Auf ähnliche Art wurde in den letzten beiden Jahren die später eingestiegene Netochka Nezvanova zu einer extrem bekannten Netzperson - im Guten wie im Schlechten.

Die unter dem Pseudonym Netochka Nezvanova, das einem Romanfragment von Dostojewski entlehnt ist, agierende Person hat einen ganz eigenen E-Mail-Stil entwickelt. Unter wechselnden Usernamen und Domains wie »god-emil«, »m9ndfukc« und zuletzt »relativ« konstant »integer«, formatiert sie ihre E-Mails so, als wären sie durch ein verrückt spielendes Buchstabenvermischungsprogramm gelaufen. Einer schwer zu durchschauenden Gesetzmäßigkeit folgend werden einzelne Buchstaben durch andere Zeichen des ASCII-Codes wie Ausrufezeichen, Kommas, Klammern und Zahlen ersetzt. Das Ergebnis erinnert manchmal an Programmcode, dann wieder mehr an natürliche Sprache, wobei auch letztere schwer entzifferbar ist. Nur wer sich auf diesen Code einlässt und viel Zeit auf dessen Entzifferung verwendet, kann aus Netochka-Nezvanova-Mails so etwas wie Bedeutung herausfiltern. Mit diesem E-Mail-Stil pflegte sie sich auf zahlreichen Mailinglisten herum- und deren Moderatoren in Tobsuchtsanfälle zu treiben. In ihren schlimmsten Tagen bombardierte sie Mailinglisten geradezu mit Dutzenden solcher Botschaften, was zu ihrem Ausschluss von einer Reihe von Foren führte. Bei den sich dabei entspinnenden Gefechten beschimpfte sie männliche Moderatoren gerne als »male korporate fascists«, was diese nur noch mehr auf die Palme brachte. Bei der teilweise großen Anzahl von Botschaften täglich ist der Ärger von Moderatoren und Listenteilnehmern verständlich. Was aber dennoch verwundert, ist, auf welche Feindseligkeit dieser Kommunikationsstil stieß. Obwohl ihre E-Mails keine Viren enthalten und keine Viruswarnungen aussprechen, scheint deren Ästhetik auf subtile Art die Virus-Paranoia anzusprechen. Sie erscheinen wie Verschmutzungen von eigentlich für rationale Diskussionen bestimmten Foren - chaotische Ansammlungen von ASCII-Zeichen signalisieren Unterwanderungsgefahr und Ansteckung mit der Angst vor dem Nicht-Identifizierbaren. Vor allem Männer eines bestimmten Charakterzuschnitts, und insofern schien ihr Pauschalvorwurf nicht ganz unbegründet zu sein, konnten über ihre Postings in herzgefäßverengende Wut ausbrechen. Dabei sind Nezvanova-E-Mails eigentlich sehr leicht zu identifizieren und insofern mühelos auszufiltern. Auch enthalten sie, bei näherem Hinsehen, recht subtile Botschaften, die sich häufig in dekonstruierender Weise auf vorhergegangene Postings beziehen und diese mit ASCII-Grafiken und indirekten Kommentaren umrahmen. Lesbare Zeilen dazwischen modulieren und variieren bestimmte Themen, wie etwa »maschinenkunst«, »memepool« und andere Reizworte der Netz-Insiderkultur. Durch die konsequente Verschleierung der eigenen Person schuf Netochka Nezvanova eine Kunstperson, in der sie zur ultimativen Hoax-Königin des Netzes wurde. Ihre E-Mails wecken Assoziationen, so als würde irgendwo im Netz eine künstliche Intelligenz sitzen, die permanent Botschaften recycelt, Bedeutungen vermischt, Konflikte aufrührt und mit orakelhafter Qualität demNetzgeschehen einen Zauber verleiht, der in der üblichen Fixierung auf Nutzen und Produktivität im Netz sonst nur selten so zu spüren ist. [11]

Resümee

Die Absicht ist sicherlich nicht, etwas schönzureden. Würde ich auf meinem eigenen System ein Virus vorfinden, würde ich es sofort rücksichtslos ausmerzen. Virusfehlwarnungen verursachen gerade in größeren Organisationen unnötige Kosten. Hoaxes können an die Grenze des Betrugs oder darüber hinausgehen. Andererseits aber haben gerade diese hier beschriebenen, mit unterschiedlichen Absichten hergestellten Fälschungen einen höheren Nutzen. Sie sind nicht so zerstörerisch, als dass sie unmittelbare fatale Folgen hätten wie etwa ein Virus, das wirklich die Festplatte formatiert. Parasitäre Botschaften, die das Immunsystem unserer Aufmerksamkeit besetzen, können wie Viren im richtigen Leben, wenn wir an ihnen nicht zu Grunde gehen, sondern sie überwinden, das Immunsystem sogar stärken. Sie bringen uns bei, wachen Geistes zu sein und die Tugend der gesunden Skepsis aufrechtzuerhalten. Sie tragen auch zur Artenvielfalt bei, bringen neue Nuancen ein, schaffen Erregungen. Der Abwehrkampf gegen solche Viren kann wie Doping wirken. Abwehrmechanismen, die wir dabei entwickeln, können uns auch in der Beurteilung anderer Situationen helfen, etwa, wenn die Medien bestimmte Hypes generieren oder die Politik in bauernfängerischer Weise zu polarisieren versucht. Kurz, so ärgerlich diese Art von Viren im Einzelfall sein kann, so ist ihr Vorhandensein im gesamten System vielleicht weniger ein Mangel als ein Zeichen für eine notwendige Diversifizierung. Mit Viren zu leben, kann uns eine Toleranz lehren, die sich dem Leben gegenüber großzügig erweist. Sie verschmutzen unsere Systeme, aber sie bereichern uns dadurch auch. Evolutionstheoretiker haben in den letzten Jahren festgestellt, dass es ohne parasitäre Lebensformen möglicherweise gar kein Leben gebe. [12] Insofern heißt, nach ihrer vollständigen Ausrottung zu trachten, auch dem Leben eine Absage zu erteilen. Völlige Effizienz mag ein Ideal sein, aber das zu erreichen verhindert auch jede Weiterentwicklung. Daher, ein Lob der Hoax-Kultur.

Literatur

[1] Ausführliche Informationen über Good Times finden sich in der deutschen Übersetzung des Good-Times-Scherz-Faq unter http://www.rafael-seifert.de/goodtime.htm
Informationen über Virus-Hoaxes allgemein bietet z. B. der Hoax-Info-Service der TU-Berlin unter http://www.tu-berlin.de/www/software/hoax.shtml

[2] Ferbrache, »A pathology of Computer Viruses«, Springer, London, 1992

[3] Interessanterweise greifen auch Sarah Gordon, Richard Ford und Joe Wells in einem ansonsten recht trockenen Text über Hoaxes und Hypes auf den Anti-Viren-Seiten von IBM die Theorie von den Memen auf. IBM Virus Research Papers, http://www.research.ibm.com/antivirus/SciPapers.htrn

[4] Mehr zum Thema Memetik im »Meme-Spedal« in: Telepolis, http://www.heise.de/tp/deutsch/special/mem/default.html

[5] Michaela Simon, »Fütter mein Email-Ego«, in: Telepolis, http://www.heise.de/tp/deutsch/inhalt/co/4494/1.html
Website mit dem gesammelten E-Mail-Dialog: http://bradley-chait.formosa.ch/

[6] Virus Myths Website: http://www.Vmyths.corn/

[7] Florian Rötzer, »Virales Marketing buchstäblich genommen?«, in: Telepolis, http://www.heise.de/tp/deutsch/special/auf/7596/1.html

[8] Armin Medosch, »Email-Fälscher spielt Ars Electronica bösen Streich«, in: Telepolis:

http://www.telepolis.de/deutsch/inhalt/sa/3424/1.html
[9] Etoy, http://www.etoy.com
[10] Jodi.org, Hommage an Good Times, http://404.jodi.org/
[11] Website Netochka Nezvanova, http://m9ndfukc.com/
[12] Florian Rötzer, »Ein Lob der Parasiten«, in: Telepolis,
http://www.heise.de/tp/deutsch/special/mem/2087/1.html

Armin Medosch ist Mitbegründer und Redakteur des Online-Magazins Telepolis.

Werde reich, glücklich und satt!!!

Florian Schneider

Es passierte am letzten Tag des Jahres 1936: Jay C. Hormel, ein Wurstfabrikant aus Austin, hatte Freunde, Mitarbeiter und Geschäftspartner zu einer großen Silvesterparty in sein Privathaus eingeladen. Eigentlich sollte bloß gefeiert werden, doch der ehrgeizige Jung-Unternehmer Hormel konnte es wieder einmal nicht lassen: Weil er für den Siegeszug einer revolutionären Produktinnovation noch dringend den passenden, unverwechselbaren Namen suchte, rief er die versammelten Partygäste zu einem Wettbewerb auf. Er versprach 100 Dollar demjenigen, der noch in der Neujahrsnacht die zündende Idee haben sollte, wie in kleine Blechdosen gepacktes Würzfleisch künftig bezeichnet werden solle. Mit steigendem Alkoholpegel dürften die Vorschläge besser und besser geworden sein, bis schließlich zu vorgerückter Stunde der Schauspieler Kenneth Daigneau, Bruder des Vizepräsidenten der »Hormel Foods Corporation«, das Preisgeld einsackte. Er kam darauf, die jeweils ersten und letzten beiden Buchstaben von »Spiced Ham« zu dem Kunstwort »Spam« zusammenzuziehen.

»SPAM Luncheon meat«, wie es von nun an heißen sollte, besteht aus Schinken, Schweineschulter und einer streng geheim gehaltenen Gewürzmischung. Umso wilder wuchern die Gerüchte rund um das Frühstücksfleisch: Liebhaber fechten Glaubenskriege aus über die Frage, ob die rosafarbene Masse besser in Scheiben oder in Streifen geschnitten werden solle. Die Briten behaupten, deswegen den Zweiten Weltkrieg nicht nur überstanden, sondern auch gewonnen zu haben. Amerikanische Veteranen reklamieren ebenfalls kriegsentscheidende Bedeutung für SPAM: Sie hätten umso härter gekämpft, um so schnell wie möglich wieder Hamburger und Schweinesteaks zu sich nehmen zu dürfen und nie mehr wieder SPAM. Und die sagenhafte Beliebtheit von SPAM unter den Bewohnern der pazifischen Inselwelt soll auf den früher praktizierten Kannibalismus zurückzuführen sein.

Kaum glaubliche Zeugnisse virtueller Großzügigkeit

SPAM [1] ist von der »Hormel Foods Corporation« in 101 Ländern dieser Welt markenrechtlich geschützt. Völlig vergeblich, denn was mittlerweile meist unter Spam verstanden wird, hat mit der ersten Mahlzeit des Tages so wenig zu tun wie eine Schweinshaxe mit Hawaii. In der Umgangssprache des Internets steht Spam für elektronische Postwurfsendungen, unverlangt eingehende Werbung, Junk-E-Maii oder wie es offiziell heißt: »Unsolicited Commercial Email« (UCE) oder »Unsolicited Broadcast Email« (UBE).

Weit mehr noch als Kinderpornografie und Nazi-Seiten verkörpert Spam für die puritanische Netzgemeinde das Böse schlechthin. Also Nachrichten, die meist mit Sätzen beginnen wie: »Vielen Dank für Ihr Interesse ...«, »Lesen Sie diese Nachricht bitte zweimal!« oder »Beinahe hätte ich mir diese Gelegenheit durch die Lappen gehen lassen ,..« und dann Angebote beinhalten, die beim Wort genommen eigentlich gar nicht ausgeschlagen werden können: »Finanzielle Unabhängigkeit auf immer und ewig«, »50.000 Dollar in den nächsten 90 Tagen«, »Sofortige Entschuldung« bis hin zur »Umkehrung des Alterungsprozess«. Oft handelt Spam auch von zwielichtigen Offerten wie pornografischen Angeboten oder dem Zugang zu bislang geheim gehaltener Software, die Ausstellung von Reisepässen oder Decoder, die angeblich Pay-TV-Programme entschlüsseln. Ganz zu schweigen von kaum glaublichen Zeugnissen virtueller Großzügigkeit: hochwertige Handtelefone kostenlos, Gratis-Pornos, Firmenanteile umsonst, Bargeld auf die Hand ...

Dass nun ausgerechnet Frühstücksfleisch als Metapher für ebenso überflüssige wie störende Kommunikation herhalten muss, geht der Legende nach auf einen Klassiker der englischen Komikertruppe Monty Python [2] zurück. Der Sketch [3] aus dem Jahr 1970 spielt in einem Restaurant, das ausschließlich Speisen mit Frühstücksfleisch anbietet. Mrs. Bun, die mit ihrem Mann zu Gast ist, bittet flehentlich um eine Mahlzeit ohne Spam, doch ihr akuter Widerwille wird von einem Wikinger-Chor erstickt, der immer lauter den Gesang von »Spam, lovely spam, wonderful spam« anstimmt.

Greencard-Werbung und politische Propaganda

So oder ähnlich müssen sich die Nutzer des Usenet Anfang der 90-er Jahre gefühlt haben, als sie Opfer der ersten Spam-Attacken wurden. Der ominöse Serdar Argic, auch bekannt als »Zumabot«, »Ahmed Cosar« oder »Hasan B-) Mutlu«, ist wahrscheinlich der erste Serienspammer der Internetgeschichte, Urahn aller unerwünschten Nachrichten. [4] In nur zwei Wochen konnte Serdar Argic mehr als sieben Megabyte Datenmüll versenden: 935 Nachrichten, im Durchschnitt 66 Stück pro Tag oder ein halbes Prozent der gesamten Datenmenge des Usenet. So nicht-kommerziell wie die Frühgeschichte des Internets waren auch Argics Absichten. Ihm ging es darum, mithilfe von unzähligen Postings den Völkermord an den Armeniern während des Ersten Weltkriegs weißzuwaschen. Ende April 1994 stellte Argic von einem Tag auf den anderen seine Aktivitäten ein, doch »Usenetters« spekulieren bis heute, wer wirklich hinter der Fassade des fanatischen Armenier-Hassers steckt.

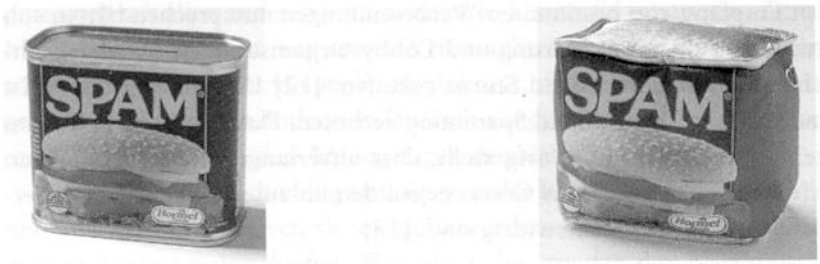
Im April 2001 erst tauchte eine mysteriöse Nachricht bei Slashdot auf, die einige Andeutungen über die Identität des ersten Spammers machte. Argic beziehungsweise Cosar habe sich eines kleinen Skripts bedient, das automatisch den ersten Absatz eines gewöhnlichen Usenet-Postings zitierte, eine zufällig ausgewählte Beschimpfung erzeugte und dann mit pro-türkischer Propaganda fortfuhr. [5] Warum er so plötzlich aufsteckte, soll daran gelegen haben, dass er sein US-Visum verlor und dann über keinen Internetzugang mehr verfügte. Andere Quellen vermuten hinter Argic den US- oder den türkischen Geheimdienst, doch eines steht fest; In die Geschichtsbücher des Internets ist Argic als erster Spammer eingegangen und selbst seine Opfer huldigten ihm posthum auf T-Shirts. [6]

Als legitime Erben von Argic gelten Ganter & Siegel, eine Rechtsanwaltskanzlei aus Phoenix, die in Hunderten von Diskussionsforen ihre Dienste als Einwanderungsberater dermaßen dumm-dreist anboten, dass daraufhin Tausende von Nutzern des Usenet zur

Gegenwehr schritten und Ganter & Siegel mit Protestmails überschütteten. [7] Seinerzeit war dies noch ein probates Mittel: Zweimal wurde die dubiose Kanzlei von ihren Internet-Providern wegen unlauteren Gebarens der Netzzugang gekappt. Er möge nicht einmal im Traum daran denken, auf diese Art und Weise in die Geschichte einzugehen, warnte der Moderator einer Newsgroup den Anwalt Laurence Canter. Doch der sah sich zusammen mit seiner Partnerin Martha Siegel an der Spitze einer historischen Mission, der Erschließung des Netzes für kommerzielle Zwecke. Entsprechend selbstbewusst kanzelten die beiden alle Proteste ab: »If you cut through all this what you will find is a group of old timers who don't want their private domain invaded.«

Möglichkeiten virtueller Mülltrennung

Die vermeintlichen Ewiggestrigen gründeten bald eine eigene Newsgroup »alt.current-events.net-abuse«, wo dann erstmals und eingehend diskutiert wurde, wie dem Missbrauch des Usenet Einhalt geboten werden könne. Noch lange bevor von E-Business, E-Commerce und New Economy überhaupt die Rede war, wurde hier diskutiert, wie ungezügelter Geschäftemacherei, Betrug und grenzenlosem Nepp Einhalt geboten werden könnte. Im Gegensatz zu Telefonmarketing oder Werbefaxen zahlt beim Usenet- oder E-Mail-Spamming schließlich der Empfänger die Rechnung für die unverlangt eingegangene Nachricht. Den Spammer kostet der Massenversand nur ein paar Mark Traffic plus einmalig rund zweihundert Mark für Zigmillionen E-Mail-Adressen. Diese werden mit besonderen Programmen von Webseiten, aus Mailinglisten-Archiven und Newsgroups abgefischt, um dann von windigen Adressenhändlern in eigenen Spam-Angriffen (»68 Millionen E-Mail-Adressen für nur 149 Dollar«) verscherbelt zu werden.



Hunderte von Seiten, allen voran »Spam.abuse.net«, haben sich inzwischen ganz und gar dem erbitterten Kampf gegen Spam verschrieben. [8] Virtuelle Mülltrennung sollte sich aber auch automatisieren lassen: Die allererste Anti-Spam-Software hieß Cancelmoose und war in der Tat so etwas wie ein Elchtest für E-Mail. [9] Als Spam identifizierte Newsgroup-Nachrichten werden von dem Skript als bereits gelesen markiert und deswegen beim Lesen der Newsgroup nicht heruntergeladen. Nach ähnlichen Prinzipien funktionieren Filter, die Spam entweder schon Server- oder Client-seitig aussortieren und erst gar nicht in die heimische Inbox vordringen lassen. Gesperrt wird beispielsweise der Weitertransport von E-Mails, welche von Mailservern stammen, die in entsprechenden schwarzen Listen geführt werden. Diese Methode trifft aber auch genügend unbescholtene E-Mails, die überhaupt nichts mit Spam zu tun haben, aber eben zufällig denselben SMTP-Server benutzen wie irgendwann einmal ein Spammer. Diese verschaffen sich schließlich

meist ohne das Wissen der Systemadministratoren Zugang, um ihre Massensendungen fremden Netzen wie Kuckuckseier ins Nest zu legen.

Die andere Möglichkeit, Spammern Einhalt zu gebieten, besteht deswegen darin, das Übel an der Wurzel zu packen und die Benutzung von Mailservern grundsätzlich so restriktiv wie möglich zu handhaben. Der Kampf gegen »unsichere« Server, die »Open Relaying« erlauben, also auch von außen für das Versenden von E-Mail benutzt werden können, ähnelt bislang zumindest noch einem Kampf gegen Windmühlen und wird zudem durch kostenlose Webmail-Dienste, wo sich Spammer kurzfristig mit Accounts eindecken können, zusätzlich erschwert.

»Ein Gespenst geht um in Europa«, dermaßen pathetisch beginnt das »Opt-In-Manifesto«: »Das Gespenst grenzenlos verbreiteter, unerwünschter E-Mail«. CAUCE ist ein Zusammenschluss von Internetnutzern, Netzwerkprofis und Systemadministratoren, die dem Spamming den Kampf angesagt haben. [10] Deren europäische Dependance Euro-CAUCE hat Anfang 1999 zusammen mit der Computerzeitschrift c't und dem Online-Magazin »Politik-Digital« eine Petition gestartet, die dafür sorgen sollte, dass Spamming per EU-Gesetz verboten wird. [11] »Stimm gegen Spam!« heißt eine Aktion, die die meisten User allmorgendlich für gewöhnlich mit dem Delete-Button durchführen und die nun im Stile einer Online-Abstimmung organisiert wird. Knapp vierzig-tausend Teilnehmer wollen nun in zwei Jahren mit einem Mausklick für ein europaweites Verbot von Spam plädiert haben.

Im Mai 2000 verabschiedete das EU-Parlament dann in dritter Lesung ein Gesetz, das vorschreibt, unverlangt versandte Werbe-E-Mails als solche klar erkennbar zu machen. Die Versender dürfen keine Werbung an Adressaten schicken, die sich in ein entsprechendes Opt-Out-Register eingetragen haben. Gegen ein generelles Verbot von Spam beziehungsweise ein Opt-In-Register, wo die Nutzer sich eindeutig für den Empfang von bestimmten Werbesendungen aussprechen hätten sollen, waren die US-Regierung und Lobby-Organisationen wie der Deutsche Multimedia-Verband Sturm gelaufen. [12] Unabhängig davon ist und bleibt in Deutschland Spamming verboten. Das Landgericht Traunstein hatte 1997 schon festgestellt, dass unverlangte Werbe-E-Mails an Privatpersonen gegen das Gesetz gegen den unlauteren Wettbewerb verstoßen und damit rechtswidrig sind. [13]

Die Versprechen des Internets ins Absurde verkehrt

Wie machtlos Gesetze gegenüber den ohnehin meist anonym und aus dem digitalen Niemandsland operierenden Spammern sind, beweist die »Opt-Out«-Option, die heutzutage die Fußzeile vieler Spams schmückt. Wer auf das gnädige Angebot, an eine so genannte »Remove«-Adresse zu antworten, um angeblich ein für allemal aus dem Verteiler gestrichen zu werden, eingeht, kommt in der Regel vom Regen in die Traufe. Die Spammer erhalten die wertvolle Bestätigung, dass sich hinter der E-Mail-Adresse eine real existierende Person verbirgt und vervielfachen sogar die Frequenz der Attacken. Vollkommen hilflos sind alle Filter und Gesetze gegenüber einer besonders perfiden Abart des Spammings. Wie eine elektronische Plage breiten sich Kettenbriefe im Netz aus, bei denen die Empfänger aus ebenso durchsichtigen wie undurchsichtigen Gründen angehalten werden, die E-Mail an möglichst viele Adressaten weiterzuleiten. Appelliert wird dabei nicht nur an die Habgier, sondern immer Öfter auch an die Gutmütigkeit: Krebskranken Kindern einen letzten Wunsch zu erfüllen, afghanische Frauen vom

Schleierzwang zu erlösen, Nazis aus Newsgroups zu verbannen sind die Vorwände für fadenscheinige und völlig überflüssige Rundsendungen, die jahrelang kursieren und letztlich auch seriöse, weil ordentlich datierte und mit gültigen Absender- und Webadressen versehene Kampagnen in Misskredit bringen. [14]

Spam wird es wahrscheinlich so lange geben, solange es Menschen gibt, die darauf hereinfallen. Spam verkörpert so etwas wie den Anti-Christ des E-Commerce und geht untrennbar mit der Kommerzialisierung des Internets einher, so sehr sich Asketen - allen voran Usability-Guru Jakob Nielsen - dagegen auch sträuben mögen. Nielsen wird seit Jahren nicht müde, die generelle Untauglichkeit des Internets für Werbezwecke zu predigen. [15] Doch die groß angelegte Bandbreitenverschmutzung durch Massenrundsendungen ist schließlich nichts anderes als das in den Schwachsinn verkehrte Versprechen, dass jeder Mensch von nun an potenziell mit allen anderen kommunizieren könne. So genanntes »Direct Marketing«, wie Spam von seinen Verursachern euphemistisch genannt wird, ist insofern nicht viel mehr als Unkraut, das nach wie vor prächtig gedeiht auf dem fetten Boden von Überschwänglichkeit und viel beschworener Libertinage aus den Anfangstagen des Netzes.

Und weil es letztlich völlig egal ist, was der Inhalt von Spam-Mails ist und aus welchen Motiven sie versandt werden, kann dagegen auch nur eine radikale Lösung helfen. Wie etwa die, zu der der Netzkünstler Heath Bunting schon 1997 griff: Aus Notwehr gegen überhand nehmende unpersönliche Anschreiben per E-Mail legte er sich eine Netz-Identität zu, die sich nach einem bestimmten Schema monatlich verändert. [16] Indem er auf die menschliche Intelligenz setzte, konnte er eine Zeit lang zumindest die recht einfach gestrickten Robots überlisten, mit denen die Adressenhändler das Netz nach E-Mail-Adressen scannen.

Vom Neurotiker bis zum Spam-Liebhaber

Wer Opfer von Spamming wird, kann im Prinzip zwischen drei verschiedenen Reaktionen wählen: Die vernünftigste dürfte wohl darin bestehen, die unerwünschte E-Mail ebenso zu ignorieren wie die Prospekte von großen Einkaufshäusern, die spätnachmittags den Briefkasten vollstopfen, oder wild plakatierte Konzertankündigungen. Die neurotische Variante ist ebenfalls aus der Offline-Welt bekannt: Woche für Woche versuchen gereizte Nachbarn aufs Neue, Halbwüchsige, die sich mit dem Austragen von Gratis-Drucksachen ihre erste Mark selbst verdienen, auf die Einhaltung von kleinen »Werbung verboten! «-Plaketten zu verpflichten. Solche Charaktere scheinen mittlerweile den Sprung in die Online-Welt geschafft zu haben und antworten auf jede Veranstaltungsankündigung mit einer automatisch generierten Mitteilung an die »abuse.net«-Clearingstelle.

Die dritte und vielleicht raffinierteste Antwort aber lautet: Spam zu goutieren oder gar zu verklären. Schließlich können die ungeschlachten Botschaften durchaus als das Hereinbrechen des Realen in die heimische Mailbox verstanden werden. Die symbolische Ordnung des elektronischen Postfachs gerät in Gefahr; denn Spam ist ein Gift, das die Atmosphäre kleinkarierter Kommunikation zersetzt, die vorgibt, nichts als zielgerichtet und nützlich zu sein. Und das Allerschlimmste: Man kann vermeintlich nichts dagegen tun und ist den Werbesendungen, Kettenbriefen und Pyramidenspielen als unbedarfter Endnutzer wehrlos ausgeliefert. Diese Hilflosigkeit führt zu aufschlussreichen Formen von Eskapismus. So scheint für manche Menschen von Spam eine eigenartige Faszination auszugehen. Wenn sie auch dem Inhalt keinen Glauben schenken, und wenn es für sie

auch keinen Sinn macht, dagegen anzukämpfen, dann lässt diese Faszination sie solche Nachrichten doch zumindest akribisch registrieren, archivieren und aufbereiten.

Passionierte Spam-Sammler protzen gerne mit persönlichen Statistiken (»38 Megabyte in mehr als 5200 einzelnen Nachrichten. Das ist eine Menge Spam für etwas mehr als drei Jahre«) oder bieten gleich die komplette Privat-Kollektion zum Herunterladen an - kostenlos versteht sich. »CSpam.com« hat eine große Auswahl ständig wechselnden Spams animiert und lässt die aufregenden Nachrichten durch das Browserfenster scrollen, wahlweise sogar mit passender Musikbegleitung von Bach bis Verdi. [17] Auch echtes Spammen ist im Online-Shop von CSpam möglich: Auf Wunsch wird eine Dose »Original Hormel Luncheon Meat« an die gewünschten Empfänger versandt. Eine Kollektion ausgesuchten Spams ist in gebundener Vorzugsausgabe erhältlich. Nur die personalisierte Ausgabe »myCSpam«, der individuelle Zugang zu Tausenden von unterhaltsamen und informativen Internetangeboten, lässt noch auf sich warten.

Seine Aktivitäten mittlerweile eingestellt hat das »Historical Spam Museum and Archive«, das in den Jahren 1996 bis 1999 immerhin 5,6 Megabyte Spam sammelte, um das Material künftigen Generationen von Netzarchäologen zu Forschungszwecken zur Verfügung zu stellen. [18] Gedacht war das Museum aber auch als eine Hommage an das immense Ausmaß an Bedeutungslosem und Trivialem, das sich im Internet aufhält. Am bekanntesten ist jedoch die »Make Money Fast (MMF) – Hall of Humiliation«, die schon 1997 auf der Ars Electronica mit einer Goldenen Nika in der Kategorie ».net« ausgezeichnet wurde. Es handelt sich um eine öffentlich zugängliche Plattform, die Spam nicht nur in einer Datenbank ablegt, sondern vor allem eines ermöglicht: lästige Werbung bis zum Ursprungsort zurückzuverfolgen.

Gegen Echelon und den kleinen Hunger

Wie jede Form von Müll kann aber auch der Datenschrott, der beim Spamming anfällt und im virtuellen Papierkorb landet, wiederverwertet und für ziemlich praktische Zwecke eingesetzt werden. Dies versuchen zumindest die Betreiber von »Spammimic.com« unter Beweis zu stellen. [20] In einer Dialogbox auf deren Homepage können kürzere Nachrichten so ver- und wieder entschlüsselt werden, dass sie als einschlägiger Spam kodiert völlig belanglos wirken und wohl kaum die Aufmerksamkeit von Geheimdiensten und anderen elektronischen Lauschern erregen. Die Idee ist geradezu ideal für Menschen, denen die ständige Benutzung von herkömmlichen Kryptografieprogrammen zu aufwendig ist oder die nicht durch plötzlich kodierte Nachrichten kundtun wollen, dass nun auf einmal Geheimnisse ausgetauscht werden. Die sicherlich kurioseste Methode, das Briefgeheimnis zu wahren, dürfte insofern selbst High-Tech-Abhörsystemen wie Echelon oder Carnivore überlegen sein. Echter Spam, schreiben die Gründer von »Spammimic«, sei so erschreckend dumm, dass es kaum möglich ist, den von der Maschine künstlich erzeugten Unsinn von authentischem Spam zu unterscheiden.

Ein Problem, mit dem sich schließlich auch die »Hormels Food Corporation« herumschlagen muss. Doch die Hersteller des Ur-Spam verzichten auf zivilrechtliche Schritte gegen die geschäftsschädigende Gleichsetzung ihres Markennamens mit Belästigungen wie Junk-E-Mail und machen einen Vorschlag zur Güte: Wer echtes Frühstücksfleisch meint, solle SPAM einfach in Großbuchstaben schreiben.

Literatur

[1] Spam Homepage, http://www.spam.com
[2] Monty Python Online, http://www.pythonline.com
[3] Wikinger Sketch, http://www.btinternet.com/~basedata/sinkordie/spam.htm
[4] Serdar Argic, HOWLING IN THE WIRES. A net.poltergeist Horror story, http://www.kkc.net/eyenet/1994/net0728.htm
[5] http://slashdot.org/comments.pl?sid=01/03/25/1617212&cid=141
[6] http://geekt.org/geekt/cornment.cgi?newsid=1113
[7] http://www.coin.org.uk/roadshow/presentation/canter.html
[8] http://spam.abuse.net
[9] http://www.cm.org
[10] http://www.cauce.org
[11] http://www.politik-digital.de/spam
[12] http://europa.eu.int/ISP0/ecommerce/legal/documents/2000_31ec/2000_31ec_de.pdf
[13] Landgericht Traunstein, AZ: 2 HKO 3755/97
[14] http://www.tu-berlin.de/www/software/hoax.shtml
[15] http://www.useit.com/alertbox/9709a.html
[16] http://www.irational.org/heath
[17] http://www.cspam.com
[18] http://www.visi.com/~drow/spam
[19] http://ga.to/mmf
[20] http://www.spammimic.com

Florian Schneider ist Künstler und Journalist und lebt in München. Aktiv involviert in der Bürgerrechtsbewegung »kein mensch ist illegal«, gestaltete er einen Arte-Themenarbeit zu Immigration und Bürgerrechten und schreibt regelmäßig Beiträge im Feuilleton der Süddeutschen Zeitung.

3. Skripte kennen keine Ethik

»Script Kiddies« sind die Sündenböcke der Strafverfolger und Computerindustrie, aber sind sie wirklich so, wie sie dargestellt werden?

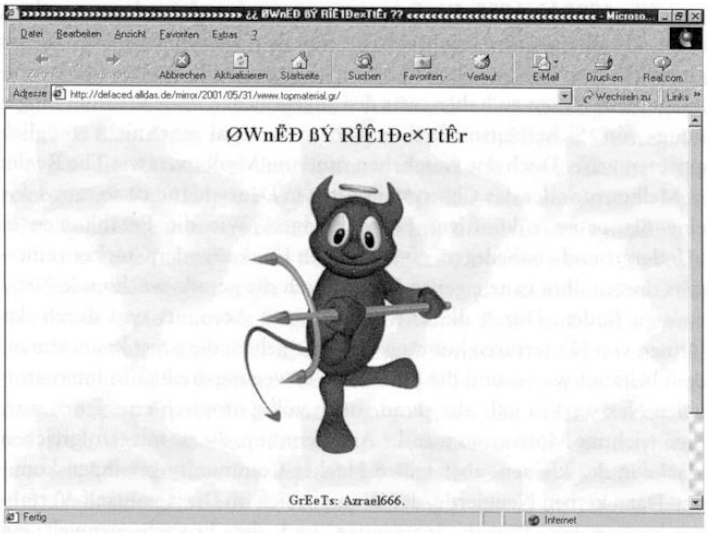
The Kids are out to play

Armin Medosch

Wenn es eine Gruppe von Personen gibt, auf deren Wahrnehmung als die »bösen Buben des Internets« man sich scheinbar universal geeinigt hat, so sind es die so genannten »Script Kiddies«. Bezeichnet werden damit meist männliche Jugendliche, die sich als »Cracker« Zugang zu fremden Rechnern verschaffen, Web-Sites verunstalten und Server durch Denial-of-Service-Attacks in die Knie zwingen. Da sie dabei (angeblich) keine originären, also selbst geschriebenen Programme benutzen, sondern auf Programme zurückgreifen, die über spezialisierte IRC-Channels, Web- und FTP-Server Verbreitung finden, wurde ihnen das Attribut »script« vorangestellt, während sich »kiddies« auf ihr jugendliches Alter bezieht. Spätestens nach den DDoS-Attacken auf CNN.com, Yahoo!, eBay und andere führende E-Commerce-Server im Februar 2000 [1] waren Script Kiddies in aller Munde. Bis heute ist nicht mit Sicherheit geklärt, wer einige der weltweit sicherlich am besten geschützten und mit den dicksten Leitungen verbundenen Server für mehrere Stunden massiv beeinträchtigen konnte. Schätzungen der Schadenshöhe Hegen zwischen 1,5 und 3 Milliarden US-Dollar. Als vermutlicher Täter wurde später ein zum Zeitpunkt der Tat 15-jähriger Kanadier angeklagt und vor Gericht gebracht, doch die Experten sind sich einig, dass er nicht der einzige Urheber der Attacken gewesen sein kann. [2] Sein wirklicher Name wurde wegen seines jugendlichen Alters nie publiziert, doch als »Mafiaboy«, so sein Internet-Pseudonym, ging er in die Netzgeschichte ein. Die Bedrohung durch Script Kiddies wie »Mafiaboy« oder »Coolio« wurde zur Schlagzeile auf Seite eins der Zeitungen und in den Nachrichtensendungen der elektronischen Medien und diente Strafverfolgungsbehörden als ein Grund mehr für die Verschärfung von Gesetzen gegen Cyberkriminalität. Der britische Ex-Außenminister Robin Cook ging sogar so weit zu behaupten, »Hacker« seien »schlimmer als Terroristen«. Hochrangige Staatsbeamte skizzierten eine Situation, wonach Teenager aus ihren Kinderzimmern in der elterlichen Wohnung heraus mittels Computer, Modem und kopierter Software kritische nationale Infrastrukturen zusammenbrechen lassen könnten: vom Stromnetz gekappte Großstädte, Krankenhäuser, Finanzzentren, Militärbasen in heillosem Aufruhr oder doch zumindest aus dem Geschäft geworfene E-Business-Server und Staatsgeheimnisse in den Händen verantwortungsloser Jugendlicher. Doch auch die, die es besser wissen sollten, da sie unter denselben oder ähnlichen Dämonisierungen gelitten haben und immer noch leiden, erfahrene, echte »Hacker«, brachten wenig Sympathie für die Kids auf. Sie benutzten den Begriff »Script Kiddies«, um sich als Hacker einer anderen, älteren Ethik von ihnen abzugrenzen. Sie verachten sie wegen des unterstellten Mangels wirklich tiefer Computerkenntnisse und weil sie durch ihre unbedachten Handlungen den Regierungen

die Legitimation lieferten, ein weites Spektrum von sicherheitsrelevanten Computeraktivitäten - im Volksmund »Hacking« - zu kriminalisieren. Wobei sie mit letzterem durchaus recht haben könnten. Doch es muss im selben Moment hinzugefügt werden, dass die Scharfmacher in Polizei- und Politikkreisen immer Gründe zur Verschärfung von Gesetzen und Strafverfolgungspraktiken finden werden.

Aber möglicherweise sind die so genannten Script Kiddies eine weit weniger homogene und stereotype Gruppe, als Polizei, Medien und Alt-Hacker uns glauben machen wollen. Mit allergrößter Wahrscheinlichkeit ist das durch sie repräsentierte Schadenspotenzial weit geringer als unterstellt. Mit dieser Aussage soll nicht in Zweifel gezogen werden, dass jugendliche Cracker Gesetzesverstöße begehen, dass sie Betroffenen persönlichen und wirtschaftlichen Schaden verursachen und dass gegen diese zahlenmäßig wachsende Bedrohung etwas unternommen werden soll. Doch sind »Script Kiddies« wirklich eine derartige »Menace to Society«, eine Herausforderung an die Werte der Gesellschaft? Oder sind sie nicht vielmehr ein Produkt ebendieser Gesellschaft, die sie so verdammt? Vielleicht ist ihr Verhalten Symptom wesentlich tiefer liegender und weit verstreuter, sozusagen systembedingter Fehler, die ihren (Un-)Taten Vorschub leisten? Ähnlich wie die Frage, ob ein Verbrecher rein individuell für seine Taten »schuldig« zu sprechen ist oder ob ihn die Umstände erst zu dem gemacht haben, was er ist, sind solche Fragen nicht auf einer allgemeinen moralischen Ebene lösbar. Script Kiddies sollen hier weder pauschal in Schutz genommen oder entschuldigt werden noch soll das negative Bild von ihnen repliziert werden, das ohnehin bereits vorherrscht. Wenn man sich mit dem Phänomen genauer befasst, kommt man relativ bald zu der Auffassung, dass es diese stereotypen Script Kiddies eigentlich gar nicht gibt, sondern vor allem Kids, mit einer Reihe verschiedener Auffassungen und Motivationen, die nur eines wirklich verbindet, nämlich dass sie einen großen Teil ihrer Freizeit mit der Beschäftigung mit Computern und Netzwerken verbringen. Spätestens an dieser Stelle ist der Begriff Script Kiddies als von außen auferlegte Negativbeschreibung ad acta zu legen. Man sollte sie zunächst, ohne vorher festgesetzte moralische Wertungen, als das sehen, was sie repräsentieren: eine relativ neue, technologische, unangepasste, bisweilen störrische, störende und zerstörerische Jugendkultur, wobei die Betonung jedoch auf Kultur liegt.



Wurzeln jugendlicher Hackerkultur aus der Perspektive der beteiligten Jugendlichen, ihren persönlichen Beweggründen nachforschend, beschreibt das Buch Underground (1997). [3] Dieses handelt von jugendlichen Hackern in Australien, USA und England im Zeitraum von ungefähr 1988 bis 1992. Die Parameter waren damals noch ganz andere, denn »Hacking«, der Einbruch in fremde Computer Systeme, diente einem Hauptzweck, nämlich überhaupt Zugang zu weltweiten elektronischen Netzwerken zu haben, was den Jugendlichen ohne kreative Umgehung von Sicherheitsmaßnahmen damals legal gar nicht möglich gewesen wäre. Doch das Geschehen rund um Mailboxen wie The Realm in Melbourne oder das Chatsystem Altos in Deutschland ist so etwas wie eine Blaupause zukünftiger Entwicklungen. Wie die Erzählungen in »Underground« nahe legen, ging es diesen Hackern oder Crackern einerseits darum, ihre ganz eigenen Wege durch die gerade wachsende Netzwelt zu finden. Durch die Entwendung von Accounts und durch das Öffnen von Hintertüren konnten sie Wege gehen, die sonst kaum jemandem bekannt waren und die ihnen eine Bewegungsfreiheit in internationalen Netzwerken gab, die gerade noch völlig utopisch erschienen war. Eine wichtige Motivation war die Anerkennung, die sie mit erfolgreichen Hacks in der kleinen, aber feinen Hacker-Community gewinnen konnten. Dazu kamen Neugierde, der Wunsch, sich im Do-it-yourself-Verfahren technisches Wissen anzueignen und der Erwachsenenwelt ein Schnippchen zu schlagen. Die minimale Ethik bestand darin, in fremden Systemen keinen Schaden anzurichten, keine Rechner zum Absturz zu bringen, keine Dateien zu löschen und sich keine finanziellen Vorteile zu verschaffen. Wichtig war auch das Fair Play, innerhalb der Community Informationen - z. B. Wissen über Hintertüren und Passwort-Crackmethoden - auszutauschen. Moralische Grenzen waren zwar durchaus porös, so gab es auch Fälle von »carding« (Kreditkartenbetrug) und »phreaking« (Missbrauch von Telefonschaltanlagen), doch die eigentliche Herausforderung bestand darin, Meisterschaft über Unix-Systeme zu erlangen.

»Underground« zeichnet das Bild eigentlich nicht kriminell gesinnter Jugendlicher verschiedener Herkunft, die allerdings bereit sind, bestimmte Grenzen der Legalität zu überschreiten. Hervorgehoben werden auch die starken Bindungen an andere Jugendkulturen, vor allem Musik (Indie-Rock wie z.B. Midnight Oil), und die Gegensätze zur Erwachsenenwelt. Der Konflikt der Kulturen und Generationen einschließlich gegenseitigen Unverständnisses könnte größer nicht sein - auch ein Element, das bis heute so geblieben ist. Da ist einerseits die Welt von Sicherheitsbeauftragten mit Visitenkarten, verbrieften elektronischen wie realweltlichen Identitäten in fest gefügten Hierarchien und Karrieren. Ihnen gegenüber stehen nur unter kryptischen Internet-Pseudonymen (Nicknames, auch genannt »handles«) agierende jugendliche Slackertypen aus den Vorortbezirken von Melbourne oder Manchester. Die verschiedenen Geschichten, die sich zehn Jahre später fast identisch wiederholen, führen zum langsamen Aufbau des Gegenschlags der Realweit und damit zum negativen Höhepunkt. FBI und Secret Service werden auf die Aktivitäten der Hacker aufmerksam. Spektakuläre Fälle gelangen in die Schlagzeilen, Neue Anti-Hacker-Gesetze werden eingeführt, Schuldige müssen gefunden und exemplarisch bestraft werden.

Für heutige Jugendliche ist der Zugang zum Internet selbst kein Problem mehr, sie werden sogar von allen Seiten dazu ermutigt. Doch der Anreiz oder Spielraum für illegale Aktivitäten ist damit nicht verschwunden. Wie es ein Sicherheitsexperte kürzlich formulierte, gibt es eine Art neuer Währung im Internet: Hintertüren. [4] Im Kern geht es dabei um dasselbe Spiel wie vor 10 Jahren: Wege zu gehen, die anderen verschlossen sind, die beamteten Profis der Erwachsenenwelt zu überlisten, »root« (Administrator-Privilegien) auf fremden Servern zu bekommen und der Insidergemeinde zu zeigen, dass

man, wie es im Jargon heißt, »elite« geworden ist, also zur Elite wahrer, amtlicher Hacker gehört. Wer sich Zugang zu möglichst vielen Systemen verschafft (und, indem dies nicht an die große Glocke gehängt wird, sich dieses Privileg über längere Zeit bewahrt), erhöht seinen Status in der Gruppe. Die Etablierung des angenommenen nom de guerre, des eigenen Internet-Nickname, als anerkanntes Markenzeichen in der Hacker-Community ist der höchste Preis. Allerdings kann dieses Ziel nicht nur allein dadurch erreicht werden, klammheimlich und still und leise Hintertüren und Zugangsrechte zu horten. Deshalb gilt es, gelegentlich öffentlich ein Zeichen zu setzen. Die jugendlichen Internet-Missetätern am häufigsten zugeschriebenen und wahrscheinlich auch wirklich von ihnen verursachten Vandalenakte sind Website-Defacement, auch genannt Web-Graffiti, und DoS-Angriffe bzw. Distributed-DoS-Attacks.

Bei »Distributed Denial of Service «-Attacken (DDoS) geht es im Grundprinzip darum, einen Server mit möglichst so vielen Datenpaketen zu bombardieren, dass die ihm zur Verfügung stehende Bandbreite an Internetanbindung durch diesen unerwünschten Traffic verstopft wird, so dass »normale« Datenpakete, also z.B. Webserver-Abfragen von an dessen Angebot interessierten Usern, nicht mehr durchkommen. Die Methoden für diese Art von Angriffen haben sich mit der Entwicklung verschiedener Formen von DDoS-Attacken verfeinert. Über einschlägige Kanäle erhältliche Programme wie »Stacheldraht« oder »Tribal Flood Net« geben relativ unerfahrenen Usern mächtige Angriffswaffen in die Hände, was den Medien-Hype über Script Kiddies nur weiter beflügelte.

Doch jugendliche Hacker wollen sich eigentlich gar nicht mit diesem Begriff bezeichnet sehen und können sehr unwirsch reagieren, wenn sie sich zu Unrecht in diese Kategorie gesteckt fühlen. Diese Erfahrung machte der Computerfachmann Steve Gibson, dessen Firmenserver Opfer eines fortgesetzten DDoS-Angriffs wurde. [5] In dem Fall, den er selbst im Netz ausführlich dokumentiert hat, fand eine DDoS-Attacke von über 400 weltweit verstreuten Windows-PCs aus statt, in die der Angreifer kleine Scripte (»Zombie« oder »Bot« genannt) eingeschleust hatte und die über spezielle IRC-Kanäle von ihrem »Herrn« gesteuert wurden. Die Anbindung von Gibsons Firma GRC ans Internet wurde mit riesigen Datenpaketen völlig überflutet. Da die Angriffe nicht aufhörten, machte sich der Betroffene auf zu Ermittlungen im Netz-Underground. Dank seiner Fähigkeiten als Althacker gelang es ihm, einen 13-Jährigen, der unter dem Nickname »Wicked« auftrat, als Urheber zu identifizieren und über eine Forumsseite mit ihm in Dialog zu treten. Wicked gab zu, Urheber der Angriffe zu sein, weil er aus zweiter Hand gehört habe, dass Gibson ihn als Script Kiddie bezeichnet hätte. Seine Netzanbindung habe er überflutet, um ihm seine Macht zu demonstrieren. Gibson, der durch eine kathartische Erfahrung gegangen war, schlussfolgerte,

- dass er trotz aller Kenntnisse diesen Angriffen gegenüber wehrlos ist, folglich bekannte er, »ich gebe auf, du hast gewonnen«,
- dass die Verletzlichkeit von Microsoft-Betriebssystemen, als »Zombies« für DDoS-Angriffe übernommen zu werden, einen Kern des Übelsausmacht und sich mit neuen Generationen, Windows 2000 und Windows XP noch verschlimmern werde,
- dass ihm die Provider der User-Rechner, die als »Zombies« befallen wurden, nicht helfen konnten oder wollten bzw. einfach die Augen schlössen und
- dass ihm auch das FBI nicht helfen konnte oder wollte.

Erst nachdem er seine Niederlage eingestanden hatte und seinem Gegenüber vermitteln konnte, dass er besagte Äußerung bezüglich »Script Kiddie« nie gemacht hatte, hörten

»Wickeds« Attacken freiwillig auf. Gibson macht sich in der Folge daran, ein Tool gegen DDoS-Attacken zu entwickeln.

Bei der Verunstaltung von Websites, passender auch »Web-Graffiti« genannt, geht es darum, sich temporär Zugang zu einem Webserver zu verschaffen und dessen Homepage durch Inhalte eigener Wahl zu ersetzen. Diese Praxis hat fast schon epidemische Ausmaße angenommen. 60 bis 80 Websites werden angeblich täglich übernommen und mit Graffitis versehen. Diese haben die verschiedensten Inhalte, weisen aber einige gemeinsame Charakteristika auf: Die digitalen Spraykünstler hinterlassen ihre Namenssignatur, einen typischen im Hackerjargon geschriebenen Namen, bestehend aus Buchstaben, Zahlen und Zeichen (z.B. »Z3BR4 X«, »DigiAlmighty«, »f0rpaxe«), Jargon wie »XY rulez« oder »ownz«, d.h. »Soundso« hat die Kontrolle über den Server erlangt. Viele arbeiten auch in Gruppen, die unter Namen wie »PoizonB0x« oder »World of Hell« auftreten. Nicht zwingend aber häufig sind »shouts«, d.h. Grüße an die eigene Community, andere Gruppen, manchmal auch Botschaften an Mädchen und Hackergrößen wie Kevin Mitnick und 2600-Magazine. Kundgebungen allgemeiner Befindlichkeit (Bier, Joints) und gelegentlich politische Botschaften, Grafiken und sogar Midi- und MPEG-Daten sind ebenfalls Bestandteil spezifischer Handschriften. In den vergangenen Jahren blieb kaum ein populärer Webserver von solchen temporären Übernahmen verschont, seien es die Server der New York Times, der NASA oder auch des Weißen Hauses. Je zentraler ein Server in der öffentlichen Gewichtung der Bedeutung ist, um so größer der Sieg für die »Cracker«. Cracks von Servern wie dem der New York Times haben in der Vergangenheit noch Schlagzeilen verursacht. Heute sind sie so zahlreich, dass es sich schon um eine konzertierte Übernahme zahlreicher Server gleichzeitig handeln muss, um noch einen Journalisten hinter dem Ofen hervorzulocken. Interessanter als der jeweils einzelne Fall sind Serien oder bestimmte Konflikte. So gibt es Cracker-Truppen, die sich auf die Übernahme von Servern aus dem militärisch-industriellen Komplex spezialisiert haben. Andere wieder bevorzugen Ziele unter ausgewählten, weltgrößten Konzernen. Im Kontext politischer Konflikte zerschießen gegnerische Cracker die jeweils anderen Web-Sites - wie kürzlich US-Amerikaner gegen Chinesen, Palästinenser gegen Israelis, Serben gegen Kroaten und Kosovo-Albaner.

Die Medien spielen solche Vorfälle gerne als Aufflammen des lange prophezeiten Info- oder Cyberwars hoch. Doch eines sollte dabei keineswegs übersehen werden. Es handelt sich »nur« um die temporäre Zerstörung von Information auf einem öffentlich zugänglichen Webserver, die verändert oder unzugänglich gemacht wird. Kritische Applikationen sollten davon nicht betroffen sein, da sie, eine der Grundregeln jedes Sicherheitshandbuchs, auf anderen Rechnern laufen sollten, die nicht direkt mit einem Webserver verbunden und zusätzlich geschützt sein sollten. Das Cracken des Webservers einer Stromgesellschaft bedeutet nicht, Zugriff auf den Rechner zu erhalten, mit dem sich das entsprechende Stromnetz herunterfahren ließe. Doch in der medialen Wahrnehmung solcher Vorfälle wird diese Differenzierung oft (bewusst?) unterlassen. Wenn Cracker, die eigentlich nur ihr Web-Graffiti veröffentlichen wollen, über Datenbanken mit Kundeninformationen, Kreditkarteninformationen oder andere sensible Informationen stolpern, handelt es sich um einen gravierenden Mangel der Sicherheitspolitik des entsprechenden Unternehmens. Es ist ausgesprochen unwahrscheinlich, dass jemand, auf den die Bezeichnung Script Kiddie zutrifft, also ein Anfänger, der nur mit vorgefertigten Programmen operiert, ein gut gewartetes System penetrieren kann, in dem alle bekannten Sicherheitslücken geschlossen sind. Doch es scheint leichter, über die Medien Sündenböcke zu schaffen, als Sicherheit ernst zu nehmen. Darüber hinaus stellt die Monokultur Microsofts scheinbar ein

ideales Umfeld für die Aktivitäten von Script Kiddies dar - z. B. die Verwundbarkeit von MS Outlook Express durch Viren und Würmer, die mit Standard-Viren-Tool-Kits erstellt wurden.

Die Website Alldas.de [6] ist inzwischen die einzige Website, die noch ein Archiv von gecrackten Websites veröffentlicht. Dort veröffentlichte Interviews mit Web-Graffiti-Attentätern legen die Vermutung nahe, dass das »Script-Kiddie-Stadium« so etwas wie die erste Stufe auf einer Leiter des Lernens in der Beschäftigung mit Computer- und Sicherheitsthemen ist. Ganz anders als die Medienberichte nahe legen, sind jugendliche Cracker nicht unbedingt auf eine Karriere als hartgesottene Cyber-Kriminelle oder -Terroristen fixiert. Viel eher schielen sie auf einen Job in der Computerindustrie als - Überraschung - Sicherheitsexperte, auch White Hat Hacker oder Ethical Hackers genannt. Aktivitäten in der Computer-Unterwelt, und das wird auch von ihnen selbst oft so verstanden, dienen der Gewinnung einer Reputation unter Freunden, einem erweiterten Expertenkreis und damit quasi der Vorbereitung auf ein Ticket in die spätere Berufslaufbahn. Sie zu kriminalisieren oder gar als Terroristen hinzustellen lässt sich nur mit dem berühmten Sprichwort »mit Kanonen auf Spatzen schießen« vergleichen.

Jugendliche Computerfreunde, fälschlich Script Kiddies genannt, sind oft eher idealistische junge Menschen, die sich mit übermächtigen Institutionen des Staates und der Wirtschaft konfrontiert sehen. Misstrauisch gegen die Ausübung von Autorität, sehen sie es als legitim an, in ihren Augen kleinere Gesetzesverstöße zu begehen. Was früher als der militärisch-industrielle Komplex bezeichnet wurde, ist im Internet immer nur eine Ecke entfernt. Ohne sich ganz im Klaren zu sein, mit wem sie sich anlegen, testen sie die Grenzen des zivilen und militärischen Internets aus und fordern die Staatsmacht heraus. Diese ist in ihrer Gegenreaktion nicht zimperlich. Razzien gegen 15-Jährige mit nicht uniformierten, schwer bewaffneten Agenten sind vor allem in Nordamerika keine Seltenheit. Öffentliche Brandmarkung als Kriminelle und Terroristen und das Austeilen von Gefängnisstrafen senden das Signal, die Reihen im Untergrund zu schließen. Die Tendenz ist ähnlich wie die im »Krieg gegen Drogen«. Wer wegen Besitzes einiger Gramm Marihuana für ein Jahr oder länger ins Gefängnis geht, kommt höchstwahrscheinlich als verhärteter Krimineller in die Welt zurück. Kurz nach den DDoS-Angriffen auf Yahoo! usw. schrieb der amerikanische Cyberkritiker Douglas Rushkoff, dass ihn diese erfolgreichen Angriffe nicht nur mit geheimer Schadenfreude erfüllen, sondern dass er auch eine Vermutung über die Beweggründe für diese Angriffe hat. Es sei die zunehmende Kommerzialisierung des Netzes, die es nötig mache, dieses zu einem immer sichereren, besser überwachten Raum zu machen. Möglicherweise seien diese Angriffe also als Befreiungsschlag gegen die Konsequenzen der Kommerzialisierung des Netzes zu sehen, schrieb Rushkoff. [7] Jugendliche heute sehen sich mit einer vielfach reglementierten, von Konsum, Markennamen und Behörden regierten Welt konfrontiert. Rebellion gehört zur Jugend, ebenso wie ein erwachendes Interesse an Sex und ein gesteigertes Gerechtigkeitsgefühl. Ein häufig verwendetes Vorurteil gegen jugendliche Computerfreaks lautet, sie seien vereinsamte Typen, ohne soziales Leben in der »normalen« Welt. Interviews auf Alldas.de ebenso wie das Buch »Underground« widersprechen diesem Klischee. Jugendliche Computerfreaks sind ganz normale Jugendliche, mit Interesse an Anerkennung in einer Gruppe, Selbstbestätigung und Kontakt mit dem anderen Geschlecht. Sie zu dämonisieren und zu kriminalisieren kann bedeuten, einige der begabtesten und wissbegierigsten Leute in dieser Gesellschaft, die einen wertvollen Beitrag zu liefern hätten, zu stigmatisierten Außenseitern zu machen, denen der Einstieg in ein normales Leben unnötig schwer gemacht wird.

Merkwürdigerweise haben über ein Jahr nach den DDoS-Attacken auf CNN, Yahoo! usw. die Medienberichte über Script Kiddies in ihrer Frequenz deutlich nachgelassen. Auf einschlägigen Computer-Newssites finden sich noch Berichte zu den Verfahren gegen Aushängeschilder wie Mafiaboy oder Coolio, doch über die Gefängnisstrafen, zu denen sie letztlich verurteilt wurden oder nicht, findet sich trotz ausgiebiger Recherche rein gar nichts. Ein Grund kann sein, dass dem Dot-Com-Boom die Luft ausgegangen ist und daher der Schlagzeilenwert solcher Meldungen gesunken ist. Ein anderer Grund klingt schon etwas konspirativer. Praktisch alle hoch industrialisierten Länder haben inzwischen drakonische Gesetze gegen Cyberkriminalität, die kaum einen Unterschied machen zwischen kriminellen Aktivitäten {Identitätsdiebstahl, Kreditkartenbetrug) und typischen Script-Kiddie-Aktivitäten. Auf internationaler Ebene, Europarat, EU, G8-Staaten, werden derzeit weitere internationale Abkommen geschnürt, die jegliches Schlupfloch gegen Cyberkriminalität stopfen, ganz im Sinne einer Null-Toleranz-Politik. Öffentlicher Widerstand in der liberalen Presse gegen diese Gesetzgebungen, die viele Bürgerrechte im Cyberspace zu beseitigen drohen, ist minimal bis gar nicht vorhanden. Wie kausal man diesen Zusammenhang - zwischen Gesetzgebung und Boom und Ende der Berichterstattung über Script Kiddies - auch sehen mag, es scheint, die »Script Kiddies« haben ihre Schuldigkeit als Sündenböcke für die Bedrohung aus dem Internet vorerst getan.

Literatur

[1] Florian Rötzer, ECommerce-Websites lahmgelegt, Telepolis 09.02.2000, http://www.heise.de/tp/deutsch/inhalt/te/5766/1.html

[2] Stefan Krempl, Rätselraten um die Hintermänner der Cyberattacken auf US-Sites, Telepolis 10.02.2000, http://www.telepolis.de/deutsch/special/info/6616/1.html

[3] »Underground«, Suelette Dreyfus with research by Julian Assange, Random House, Australia, 1997, http://www.underground-book.corn/

[4] »Hackers are also exchanging vulnerability information with one another«, said Tom Noonan, president and CEO of Internet Security Systems Inc. In Atlanta. »There is a whole new currency on the Internet that's called the back door«, he said, adding that attackers are trading information about back doors that provide access to different systems.
http://www.computerworld.com/cwi/Printer_Friendly_Version/0,1212,.NAV47_ST059280-,00.html

[5] Anatomie einer DDoS-Attacke, Heise Online, http://www.heise.de/newsticker/result.xhtml?url=/newsticker/data/ps-04.06.01-000/default.shtml&words=Kiddies,
Dokumentation des Falles: http://grc.com/dos/grcdos.htrn

[6] Archiv von Web-Graffitti auf Alldas.de, http://defaced.alldas.de

[7] Douglas Rushkoff, Yahoos letztes Gefecht, Telepolis 11.02.2000, http://www.telepolis.de/deutsch/kolumnen/rus/5776/1.html

Die neuen Cracker

Janko Röttgers

Das Brechen von Verschlüsselung, Kopierschutzmechanismen und Zugangsbeschränkungen ist ein altes Spiel. Vom polnischen Crypto-Spezialisten Marian Rejewski, der 1933 den Code der deutschen Enigma-Chiffriermaschine knackte, [1] über die Unix-Hacker der siebziger Jahre bis zu den Codebrechern der heutigen Warez-Szene haben sich immer wieder Programmierer daran versucht, den Geheimnissen anderer Programmierer und ihrer geschützten Geschöpfe auf die Schliche zu kommen.

Die Motive dafür waren und sind höchst unterschiedlich: Einige Cracker-Angriffe sind politisch oder gar militärisch motiviert, anderen geht es nur um den Spaß an der Sache. Doch von der Öffentlichkeit wird der Cracker häufig als Egoist wahrgenommen, als jemand, dem es allein um Urheberrechtsverstöße und kostenlose Software geht. Ein Bild, an dem auch die sich von den Crackern abgrenzenden »ethischen« Hacker nicht unschuldig sind.

Schon bald könnte sich dieses Bild allerdings wieder wandeln. Mit dem Prozess um das DVD-Entschlüsselungstool DeCSS und den Auseinandersetzungen um Kopierschutzmechanismen der Secure Digital Music Initiative (SDMI) tritt eine neue Riege von Crackern ins öffentliche Rampenlicht. Nicht mehr pickelige Jugendliche auf der Suche nach dem neuesten Quake-Patch, sondern Code-brechende Universitätsprofessoren und Aktivisten der Electronic Frontier Foundation dominieren plötzlich die Debatte.

Der DeCSS-Fall

CSS ist ein im Auftrag der DVD-Copy Control Association (DVD-CCA) entwickeltes Verschlüsselungsverfahren, mit dem der direkte Zugriff auf die Videodaten einer DVD verhindert werden soll. Damit soll das Konvertieren von Videodaten in andere Formate sowie anderer unlizenzierter Zugriff auf diese Daten unterbunden werden. Das System benutzt zu diesem Zweck eine 40-Bit-Ver-schlüsselung. Einer der beiden Schlüssel befindet sich auf der DVD, ein anderer im DVD-Hardware-Player beziehungsweise der entsprechenden Software - sofern diese von der DVD-CCA dafür lizenziert wurde.

Für das Open-Source-Betriebssystem Linux gibt es jedoch bis heute keine Software mit einer derartigen Lizenz. De facto konnten DVDs damit bis vor kurzem nur auf Windows- und MAC-Rechnern abgespielt werden. Dies nahmen einige Cracker im Sommer 1999 zum Anlass, sich genauer mit dem CSS-System zu beschäftigen. Ein deutscher Cracker entdeckte, dass der Hersteller eines Windows-DVD-Players den CSS-Schlüssel nur unzureichend vor Zugriffen geschützt hatte. Mittels dieses Schlüssels

rekonstruierte er den CSS-Quellcode. Ende September/ Anfang Oktober 1999 tauchte dann das Programm DeCSS im Netz auf, das den Inhalt einer DVD unverschlüsselt auf der Festplatte speichern kann. DeCSS und der CSS-Quellcode verbreiteten sich im Netz in Windeseile und lieferten die Grundlage für zahlreiche Player und Kopierprogramme (Ripper).

Im November 1999 wurde der erste ISP dazu bewegt, eine Website mit DeCSS vom Netz zu nehmen. Ende Dezember verklagte die DVD-CSS zahlreiche Einzelpersonen wegen der Verletzung von Firmen- und Handelsgeheimnissen. Mitte Januar folgte eine zweite Klage der in der Motion Picture Alliance of America organisierten Filmstudios gegen die Betreiber von vier Websites, darunter auch die des US-Hacker-Magazins 2600, wegen eines angeblichen Verstoßes gegen den Digital Millennium Copyright Act, der das Umgehen von Kopierschutzmaßnahmen verbietet. 2600.com-Betreiber Eric Corley gewann die Unterstützung der Electronic Frontier Foundation und führte den Prozess durch bisher zwei Instanzen.

Das SDMI-Debakel

Auch im Falle von SDMI ist es mittlerweile zu einer Klage gekommen, jedoch unter umgekehrten Vorzeichen. Kurz vor Redaktionsschluss dieses Buches klagte der Princeton-Professor Edward Felten mit Unterstützung der Electronic Frontier Foundation gegen die Secure Digital Music Initiative (SDMI), die Recording Industry Association of America (RIAA), den Wasserzeichenhersteller Verance und das US-Justizdepartment, da er die Freiheit seiner Forschungsarbeit durch offene Drohungen der Industrie-Lobbyverbände bedroht sah. Die Vorgeschichte: Vor dem Hintergrund immer weiter verbreiteter CD-Brenner und des Booms des MP3-For-mats entwickelte die Musikindustrie seit Mitte der neunziger Jahre Sicherheitskonzepte für den digitalen Musikvertrieb. Nach einigen erfolglosen Alleingängen gründete sich Ende 1998 die Secure Digital Music Initiative als Zusammenschluss von rund 180 Plattenfirmen und Technologie-Unternehmen.

Die Strategie dieser Initiative sieht ungefähr so aus: durch ein Zusammenspiel von Hard- und Software eine sichere Umgebung zu schaffen, in der bestimmte Medientypen auch nur auf den für sie vorgesehenen Playern wiedergegeben werden können. Wie bei CSS geht es zunächst einmal nicht so sehr darum, die 1:1-Kopie einer CD unmöglich zu machen, sondern ihre Konvertierung in andere Medienformen, speziell MP3-Dateien. Am Ziel der Bemühungen steht dann irgendwann eine rein digitale Distribution mit einem strikten Digital-Rights-Management - so jedenfalls die Theorie. [2]

In der Praxis beschäftigte sich die Gruppe jahrelang mit internen Auseinandersetzungen, bis dann im September 2000 ein ungewöhnlicher Praxistest folgte. Der »Hack SDMI!« genannte Wettbewerb sollte eigentlich bei der Evaluierung möglicher SDMI-Techniken helfen. Doch die Hacker um Felten knackten gleich alle vorgeschlagenen Mechanismen und stürzten damit die Gruppe in eine tiefe Krise.

Fortsetzung folgt

DeCSS und der SDMI-Hack haben Crackern wieder eine neue Legitimation gegeben. Das Knacken der Kopierbeschränkungen wird von weiten Teilen der Öffentlichkeit als legitimer Versuch angesehen, die Fair-Use-Rechte der Konsumenten zu verteidigen. Das

öffentliche Dokumentieren der Cracks gilt nicht nur der Netzgemeinde als berechtigte Wahrnehmung des Rechts auf freie Meinungsäußerung. Die nachfolgenden Artikel beschreiben also nicht nur zwei wichtige Auseinandersetzungen um die Zukunft digitaler Mediendistribution, sondern auch einen Paradigmenwechsel in Bezug auf die Cracker-Szene und ihre Motive.

Natürlich können diese Artikel nur eine Momentaufnahme bieten. Die Auseinandersetzungen gehen weiter: Zum Redaktionsschluss dieses Buchs (Juni 2001) befindet sich Eric Corley in einer Revisionsverhandlung. Das SDMI-Konsortium ist seinem Ziel immer noch nicht näher und hat sich bei einem Treffen im Mai ergebnislos auf September 2001 vertagt. Gleichzeitig schaut sich die DVD-CCA nach Technologien um, die mehr Sicherheit versprechen als CSS - ironischerweise interessiert sie sich besonders für Wasserzeichen. Den neuen Crackern wird also auch in Zukunft nicht langweilig werden.

Literatur

[1] Siehe http://home.us.net/~encore/Enlgma/enigma.html

[2] Eine genauere Beschreibung dieser Strategie findet sich unter http://www.julienstern.org/sdmi/system.php3

Das Pferd, das auch ein Richter nicht mehr einfangen kann

DVD-Prozess: Showdown im Gerichtssaal

Armin Medosch

Die Hauptverhandlung im Prozess von acht Hollywood-Studios gegen Emmanuel Goldstern, bürgerlich Eric Corley, Herausgeber des Magazins 2600 Hacker Quarterly und der zugehörigen Website [http://www.2600.com/], führte am vierten Verhandlungstag neben den obligatorischen harten Bandagen auch zu einigen blumigen Vergleichen. Richter Lewis A. Kaplan verglich an einer Stelle die Verbreitung der Windows-Utility DeCSS damit, dass »die Stalltür aufgeschlossen wurde und das Pferd nun draußen ist«. Man verlange von ihm nun »eine gerichtliche Verfügung dagegen, dass die Stalltür noch einmal aufgeschlossen wird, obwohl das Pferd schon draußen ist«.

Die von der Electronic Frontier Foundation gesponserten Verteidiger machen sich darauf gefasst, den Fall möglicherweise bis zum Obersten Gerichtshof der USA weiterzutreiben. Nicht minder entschlossen sind die klagenden Studios Columbia, Disney, Fox, MGM, Paramount, Time Warner, Tristar und Universal sowie ihre Interessenvertretung, die Motion Picture Alliance of America (MPAA). Sie sehen die Zukunft der Filmindustrie auf dem Spiel, falls Tools wie DeCSS ungestraft in Umlauf gebracht werden dürfen.

In ihrem Eröffnungsstatement nahm die Verteidigung den Standpunkt ein, der Vertrieb und die Anwendung von DeCSS falle unter das garantierte Recht des Käufers auf Kopien zum privaten Gebrauch (»fair use«). Die Einschränkungen im DMCA gegen Reverse Engineering würden zudem das Recht auf Kopien 2um privaten Gebrauch aushöhlen, Außerdem werde mit der Klage gegen Linksaufexterne Sites auch gegen das Recht auf freie Meinungsäußerung verstoßen.

Die Filmstudios brachten als ersten Zeugen der Anklage einen Computerwissenschaftler der Carnegie Melon University, Michael Shamos, der zeigen sollte, wie einfach es sei, mittels DeCSS eine DVD zu entschlüsseln und eine DivX DVD herzustellen. Im Kreuzverhör musste Shamos zugeben, dass es insgesamt 20 Stunden verteilt über vier nächtliche Arbeitssitzungen gedauert hatte, das Experiment durchzuführen. Mehr noch, er gestand auch ein, die »Raubkopie« eines Hollywood-Films im Auftrag der Anwaltsfirma der Anklage, Proskaur & Rose, nach deren Vorgaben hergestellt und dafür 30.000 US-Dollar erhalten zu haben.

Am zweiten Verhandlungstag brachte die EFF den Computerexperten Frank Andrew Stevenson in den Zeugenstand, der in der Forschungsabteilung einer führenden norwegischen Computerspielefirma arbeitet und als erster den CSS-Algorithmus analysiert und die Ergebnisse publiziert hatte. Eine von ihm schon zuvor abgegebene schriftliche Erklärung lässt keinen Zweifel daran, dass

DeCSS nicht, wie die Studios behaupten, das Tool ist, das der Piraterie mit DVDs Tür und Tor öffnet. Aktive Piraten würden sich die Mühe mit DeCSS sparen und alle auf einer DVD befindlichen Daten einfach Bit für Bit kopieren, wogegen CSS keinen Schutz bietet. Eine mit Hilfe von DeCSS entschlüsselte DVD würde hingegen soviel Speicherplatz belegen, nämlich 6 GB, die gar nicht auf handelsübliche Consumer-DVDs geschrieben werden könnten, die nur 4,7 GB Speicherplatz haben. Zudem sei der Preis für Consumer-DVD-Rohlinge höher als der Preis für kommerziell erhältliche Filme.

Ein weiterer Zeuge der Verteidigung, Computerwissenschaftler Edward Felten von der Princeton University, legte mit wissenschaftlicher Klarheit den Sinn und Zweck von CSS dar. Es wurde zu dem Zweck entwickelt zu verhindern, dass mit CSS enkodierte DVDs von Playern abgespielt werden, die CSS nicht enthalten. Zweitens hat das die Auswirkung, jede andere Nutzung zu verhindern, als die DVDs abzuspielen. Die Zielsetzung der Verteidigung hinter solchen Feststellungen ist klar: Es soll gezeigt werden, wie die Lizenzpolitik der DVD CCA »fair use« unterbindet und das Reverse Engineering von CSS legitimieren, da es der Interoperabilität von Systemen dient und ohne das kein Linux-Player für handelsübliche DVDs zur Verfügung stehen würde. Die DVD CCA hatte angeblich der Linux-Video-Entwicklergruppe keine CSS-Lizenz erteilen wollen.

Ohne in technische Details zu gehen, führte er aus, welche Fehler bei der Entwicklung von CSS gemacht wurden. Anstatt ein etabliertes und als sicher bekanntes Chiffriersystem zu verwenden, habe man ein eigenes entwickelt und sich obendrein für die Verwendung eines 40-Bit-Keys entschieden. Dieser kann mit einem sogenannten »Brute force«-Angriff geknackt werden. Weitere Designfehler würden sogar noch schnelleres Brechen der Verschlüsselung ermöglichen.

Als zweite Zeugin der Anklage trat Mikhail Reider gestern in den Zeugenstand. Sie ist Hauptverantwortliche der MPAA für Internet-Piraterie. Sie sagte aus, dass der Verband der Filmindustrie regelmäßig Websites, FTP-Sites, File Sharing Utilities (FSUs), IRC und Newsgroups nach Piratenaktivitäten überwacht und durchsucht. An die 40 Sites habe ihre Abteilung entdeckt, die raubkopierte DVDs zum Tausch oder Kauf anbieten. Doch konnte sie nicht sagen, ob es nachweisbar ist, dass irgendeiner dieser Anbieter DeCSS benutzt. Der Frage, was die MPAA gegen diese Sites unternehme, wich sie aus, indem sie auf laufende Untersuchungen verwies. Dazu arbeite die MPAA mit dem »US-Zoll, dem Geheimdienst und dem FBI« zusammen.

Den vorläufigen Höhepunkt bildete der Auftritt des norwegischen Teenagers und DeCSS-Programmierers Jon Johansen im Zeugenstand. Er hielt sich mit seinem Vater in New York auf, um an der dritten Hackerkonferenz von 2600, »HOPE 2000«, teilzunehmen. Johansen beschrieb die Entstehungsgeschichte von DeCSS und bezeugte sein Desinteresse an Piraterie. Für die Entwicklung von DeCSS hatte er einen norwegischen Computerpreiserhalten. Gefragt, was er mit dem Geld gemacht habe, antwortete er, er habe sich einen High-End-DVD-Player von Sony für 1200 Dollar gekauft.

Redaktionell gekürzte Fassung Erstmals in Telepolis veröffentlicht am 21.07.2000

Das T-Shirt, das seinen Träger zum Hackerwerkzeug werden lässt

Geek Chic

Peter Mühlbauer

Die T-Shirt-Herstellerfirma Copyleft [http://www.copyleft.net/], deren mit dem DeCSS-Quellcode versehenes T-Shirt dem Informatikprofessor David Touretzky bei seiner Aussage im DeCSS-Prozess zur Illustration dazu diente, dass Code sehr wohl eine Meinungsäußerung sein kann, wurde jetzt ebenfalls wegen »Verbreitung« des DeCSS gerichtlich vorgeladen.

»Wenn man etwas auf ein T-Shirt drucken kann, dann ist es eine Äußerung«, so hatte Touretzky, der als Experte im Prozess der Motion Picture Association of America gegen den Webseitenbetreiber Eric Corley geladen war, seine technische Sicht der zu klärenden Frage begründet. Corley war verklagt worden, weil er auf seiner Webseite erst den DeCSS-Code, mit dem DVDs auf Linux benutzt, aber theoretisch auch raubkopiert werden können, später dann Links auf Webseiten, die diesen Code enthielten, zur Verfügung gestellt hatte. Die Firma Copyleft (Werbeslogan: »Geek Chic«) bietet ein »OpenDVD«-T-Shirt an, das auf der Vorderseite ein wie ein Parkverbotsschild gestaltetes Zeichen mit einem durchgestrichenen »DVD CCA«-Schriftzug, auf der Rückseite den DeCSS-Quellcode enthält.

Das T-Shirt wird explizit als Meinungsäußerung gegen die DVD Copy Control Association (DVD CCA) und ihr Vorgehen beworben. Von den fünfzehn Dollar, die ein T-Shirt kostet, leitet Copyleft vier Dollar an die EFF weiter, die den Prozess finanziell unterstützt. Mit der Klage nahm die DVD CCA Touretzkys Argument wörtlich, dass, wenn der DeCSS-Code aus Webseiten verbannt werde, konsequenterweise auch ein Verbot der Beschreibungen in englischer Sprache und der Darstellung auf Bildern oder eben T-Shirts erfolgen müsse.

Erstmals in telepolis veröffentlicht am 02.08.2000

Die Filmindustrie hat einen ersten Sieg erzielt

Florian Rötzer

In einem grundlegenden Urteil wurde es 2600.com verboten, den Code von DeCSS, denn Umgehungsprogramm für die DVD-Verschlüsselung, zu veröffentlichen oder einen Link auf Websites mit dem Programm zu legen. Der New Yorker Richter Lewis Kaplan begründete sein über 90 Seiten umfassendes Urteil wesentlich damit, dass Computercode nicht prinzipiell, wie die Angeklagtenseite ins Feld führte, von der amerikanischen Verfassung als Meinungsfreiheit geschützt sei. Code könne für politische oder künstlerische Aussagen benutzt werden, aber ihn zur Verletzung des Urheberrechts zu benutzen, sei schlichtweg illegal.

Der Prozess der Motion Picture Association of America gegen Emmanuel Goldstein bzw. Eric Corley, den Herausgeber des Magazins 2600 Hacker Quarterly und den Betreiber der entsprechenden Website www.2600.com, gilt als entscheidender Schritt für die Auslegung der Urheberrechte im digitalen Zeitalter. Goldstein wurde wegen der Verbreitung von DeCSS verklagt. Wichtigster Punkt der Anklage und wichtigster Gegenstand des Prozesses ist dabei der Paragraph des Digital Millennium Copyright Acts, der jede »Umgehung von Kopierschutzmaßnahmen« verbietet. Schon im Januar hatten die Kläger von Richter Kaplan eine einstweilige Verfügung gegen die Verbreitung von DeCSS erwirkt, die jetzt von ihm in seinem Urteil noch einmal bekräftigt wurde. Goldstein und seine Verteidiger hatten vor allem darauf abgezielt, dass Computercode von der Verfassung als »speech« geschützt sei und daher nicht in seiner Verbreitung eingeschränkt werden dürfe. Die dafür von der Verteidigung angeführten Argumente bezeichnete der Richter in seinem Urteil allerdings als »grundlos«. So schrieb er beispielsweise: »In einem Zeitalter, in dem die Verbreitung von Computerviren ... Systeme stören kann, von denen die Nation abhängig ist, und in dem andere Computerprogramme auch Schaden verursachen können, muss es der Gesellschaft möglich sein, die Verwendung und Verbreitung von Code in angemessenen Umständen zu regulieren.« Kaplan verglich die Verbreitung von Computercode über das Netz überdies mit einer Epidemie: »Die Verbreitung von Mitteln zur Umgehung der Sicherungen von urheberrechtlich geschützten Werken in digitaler Form ist analog zum Ausbruch einer Epidemie. Wenn man die erste Infektionsquelle herausfindet (d. h. den Autor von DeCSS oder die erste Person, die es benutzt), nutzt das gar nichts, da die Krankheit (die durch DeCSS ermöglichte Copyrightverletzung und die daraus resultierende Verfügbarkeit von entschlüsselten DVDs) sich weiter von einer Person, die Zugang zum Entschlüsselungsprogramm oder zu einem entschlüsselten DVD hat, auf eine andere

überträgt. Alles ist >infiziert<, d.h. ermöglicht perfekte Kopien der digitalen Daten.«

Normalerweise werden die von einer Krankheit befallenen Opfer eine medizinische Behandlung suchen, was aber im Falle von DeCSS nicht der Fall sei. Man könne nicht davon ausgehen, dass sie sich von dieser Krankheit heilen lassen wollen. Deswegen sei in diesem Fall die »kausale Verbindung zwischen der Verbreitung von Computerprogrammen als solchen und ihrer illegalen Verwendung« auch anders als sonst gelagert. Die Verbreitung selbst kann bereits Schaden zufügen und eröffnet die Möglichkeit einer »praktisch unbeendbaren Urheberrechtsverletzung«, die immer weiter geht. Kaplan scheute auch vor einem anderen drastischen Vergleich nicht zurück und sagte: »Computercode ist ebenso wenig rein expressiv, wie die Ermordung eines Politikers eine reine politische Äußerung ist.«

Redaktionell gekürzte Fassung
Erstmals in telepolis veröffentlicht am 18.08.2000

SDMI kopfloser denn je

Janko Röttgers

Richard Chiariglione, geschäftsführender Direktor der Secure Digital Music Initiative (SDMI), hat seinen Rücktritt bekannt gegeben. Kurz zuvor hatten zwei französische Hacker damit begonnen, ihre erfolgreichen Angriffe auf die SDMI-Technologien im Web zu dokumentieren. Der Zeitpunkt des Abgangs ist für das SDMI-Projekt denkbar schlecht gewählt: Es befindet sich in seiner schwersten Krise seit seiner Gründung im Dezember 1998. Damals schlössen sich auf Initiative der Musikindustrie rund 180 Platten- und Technologiefirmen zusammen, um einen Standard für sichere Musikdistribution zu schaffen. Als ehrgeiziges Ziel wurde verkündet, noch vor Weihnachten 1999 mit SDMI-Endgeräten auf den Markt zu kommen. Doch die Größe der Gruppe und die Schwierigkeit des Unterfangens führten zu Verzögerungen, so dass man statt dessen Weihnachten 2000 anpeilte.

Auch daraus wurde nichts. Bisher hat die Initiative erst einen einzigen, bescheidenen Erfolg zu verzeichnen. Im Juni 1999 veröffentlichte sie Spezifikationen für so genannte »Phase eins kompatible portable Audio-Player«. Da die eigentliche Sicherheitstechnologie zu diesem Zeitpunkt aber noch gar nicht entwickelt war, beinhaltet die Phaseeins-Spezifikation nicht viel mehr als die Möglichkeit, die Geräte später einmal zu Phase-zwei-Playern updaten zu können.

Dann wurde es Herbst, und schon wieder stand ein Weihnachten ohne SDMI-Geräte vor der Tür. Unter den Mitgliedern der Initiative machte sich Unruhe breit, es wurden Ergebnisse angemahnt. In dieser Situation kam das SDMI-Konsortium auf eine folgenschwere Idee: Man wollte die bisher entwickelten Technologien einer öffentlichkeitswirksamen Prüfung unterziehen und rief die Hacker dieser Welt auf, sich an ihnen zu versuchen. Wer eine der vorgestellten Technologien knacken könne, sollte 10.000 Dollar bekommen.

Bereits kurz nach Ende des Wettbewerbs machte das Gerücht die Runde, alle Techniken seien den Hackern zum Opfer gefallen. Was dann folgte, glich einer zweitklassigen Seifenoper: Das SDMI-Konsortium dementierte auf der Stelle. Einige SDMI-Mitglieder erklärten jedoch gegenüber dem Onlinemagazin Salon.com, das Dementi sei nur ein Ablenkungsmanöver, die Hacker hätten tatsächlich auf ganzer Front gesiegt. Das SDMI-Konsortium dementierte weiter. Dann erklärten einige Crypto-Experten der Princeton-Universität, sie seien bei allen Wasserzeichen erfolgreich gewesen. Eine genaue Dokumentation der Angriffe folge bald auf ihrer Website.

Im Januar musste Princeton-Professor Edward Felten in diesem Punkt einen Rückzieher machen; Die Watermarking-Firma Verance hatte sich gegen die Veröffentlichungen gewehrt und diese mit Hinweis auf den Digital Millennium Copyright Act unterbunden. Ohne

Dokumentation wurde der Hack allerdings vom SDMI-Konsortium nicht anerkannt, weshalb dieses erleichtert erklären konnte, nur zwei Technologien seien Hackern zum Opfer gefallen. Die beiden Glückspilze bekamen je 5000 Dollar. Alle anderen 445 Versuche waren demnach erfolglos - oder eben einfach nur schlecht dokumentiert.

Ganz ausgezeichnet dokumentiert haben zwei französische Hacker ihren SDMI-Angriff. Julien Stern und Julien Beuf veröffentlichen auf ihrer Anfang der Woche gelaunch-ten Website [http://www.julienstern.org/sdmi/] genaue Details zu einer der vorgestellten Technologien: Mögliche Angriffsmethoden werden hier ebenso erörtert wie die angenommene Funktionsweise des betreffenden Wasserzeichens.

Ob die Veröffentlichungen zu Chiargliones Rücktritt beigetragen haben, ist ungewiss. Kurz zuvor hatte das Konsortium zwei weitere herbe Schlappen hinnehmen müssen: Der Freiburger Chiphersteller Micronas hatte erklärt, aus der Initiative aussteigen zu wollen. Außerdem stellte Sony auf der Computer Entertainment Show in Las Vegas erstmals CD-Player vor, die neben normalen Audio-CDs auch selbst gebrannte CD-ROMs mit MP3s abspielen können. Bis dahin galt Sony dank hauseigenem Plattenlabel als ausgemachter MP3-Feind. Nicht nur Kritiker sahen deshalb in Sonys Kehrtwende ein deutliches Zeichen in Richtung SDMI-Konsortium. Offenbar hat Richard Chiarglione dieses Zeichen verstanden.

Redaktionell gekürzte Fassung
Erstmals in telepolis veröffentlicht am 25.01.2001

Wenn Professoren zu viel hacken

Janko Röttgers

Princeton-Professor Edward W. Felten sieht so aus, wie man sich seinen Schwiegersohn wünscht. Jedenfalls, wenn man Amerikaner und um die 50 ist. Nett, adrett, nur ein ganz klein bisschen nerdig. Einer, der dir garantiert nie den Sonntagnachmittagskaffee ruinieren würde. Einer, dem man keinen Wunsch ausschlagen, dem man nichts verbieten kann.

Kann man doch, wie jetzt die Recording Industry Association of America (RIAA) bewiesen hat. Der Vereinigung der großen amerikanischen Plattenfirmen sind Schwiegersöhne offenbar ziemlich egal, und Felten mag sie schon mal gar nicht. Die Vorgeschichte: Im September letzten Jahres rief die Secure Digital Music Initiative (SDMI) die Hacker der Welt dazu auf, sich an verschiedenen Kopierschutzmechanismen zu versuchen. »Hack SDMI« hieß dieser Wettbewerb. Felten und seine Studenten von der Princeton University [http://www.cs.princeton.edu/sip/sdmi/] nahmen das wörtlich und knackten alle sechs vorgestellten Verfahren.

Dumm gelaufen. Nur wollte die SDMI-Gruppe sich und uns diese Schlappe partout nicht eingestehen, weshalb Felten einen Maulkorb verpasst bekam. Sollte er seine Ergebnisse publizieren, drohe ihm eine Anklage wegen Verstoßes gegen den Digital Millennium Copyright Act, hieß es damals. Felten fügte sich.

Jedenfalls bis Ende April, Da stand der »Fourth International Information Hiding Workshop« an, und Felten wollte der Forschergemeinde partout nicht mehr länger vorenthalten, wie man SDMI geknackt hatte. Seine Gruppe schrieb ein Paper unter dem Titel »Reading Between the Lines - Lessons from the SDMI Challenge« und reichte es bei den Kongressveranstaltern, einer illustren Gruppe vom GERT über Intel bis zum IBM Research Lab, ein. Die waren davon begeistert und fieberten Feltens Auftritt entgegen.

Weniger begeistert war die RIAA, als sie von Feltens Plänen erfuhr. Sie schickte ihm einen bösen Brief, sprach von Rechtsmitteln und erklärte, dass mit dem geplanten Auftritt Rechte des Wasserzeichenherstellers Verance verletzt würden. Wohl oder übel musste Felten abermals einen Rückzieher machen. Damit wollte sich aber offenbar jemand aus dem Kreis der Kongressveranstalter nicht zufrieden geben, weshalb er das Paper an den Antizensur-Server Cryptome.org [http://cryptome.org/sdmi-attack.htm] weiterleitete.

Durch diese Indiskretion kann sich jetzt jeder ein Bild davon machen, wie das Princeton-Team die Kopierschutzmechanismen geknackt hat. Zwei Techniken werden eingehender analysiert und zeigen, mit welchem detektivischen Spürsinn sich die Forscher an ihre Aufgabe gemacht haben. Im Falle

des ersten Wasserzeichens entdeckten sie eine Reihe von unhörbaren, sehr kurzzeitigen Echos in einem bestimmten Teil des Frequenzbandes. Sobald sie genug über dieses Phänomen erfahren hatten, stöberten sie ein bisschen im Archiv des US-Patentamts, und siehe da: unter der Nummer 5940135 wurden sie fündig.

Ein Patent zum »Ver- und Entschlüsseln von Informationen in analogen Signalen«, angemeldet von der Firma Aris, die heute zum Wasserzeichenhersteller Verance gehört. Mit der typisch schwammigen Patentanwalts-Sprache brachte das Papier den Forschern zwar nicht viele neue Informationen. Aber sie wussten, das sie auf dem richtigen Wegwaren. Mit einigen weiteren Tests und Analysen konnten sie ein recht genaues Bild von der Funktionsweise des Kopierschutzverfahrens zeichnen.

Allerdings wäre so viel Mühe gar nicht notwendig gewesen. Alle vorgestellten Wasserzeichen ließen sich auch relativ einfach mit so genannte Brute-Force-Angriffen, also sozusagen mit der Holzhammermethode, knacken. Mal fügten die Forscher dazu kleine, unhörbare Delays in die Test-Tracks ein, mal änderten sie minimal die Tonhöhe, mal filterten sie einfach ein paar Events in einem bestimmten Frequenzbereich heraus. Und jedes Mal meldete das SDMI-Orakel, das während des Wettbewerbs automatisch alle Einsendungen analysierte: Test bestanden, Verfahren geknackt.

Feltens Gruppe resümiert deshalb, dass kein Wasserzeichen gegen Reverse Engineering Bestand haben kann. Und weiter: Wenn es für den Konsumenten möglich ist, sich geschützte Inhalte anzuhören oder anzusehen, dann wird es für ihn technisch möglich sein, diese Inhalte zu kopieren.« Das ist natürlich Wasser auf die Mühlen der Kopierschutzgegner.

Diese hatten bisher immer mit dem Problem zu kämpfen, dass es in Auseinandersetzungen wie um DeCSS immer um seltsam zwielichtige Hacker ging, die von der Öffentlichkeit eh für grundböse gehalten werden. Dan Burke von der University of Minnesota erklärte dazu gegenüber ZDNET: »Sobald ein Richter >Hacker< sagt, weißt du, dass du verloren hast.«

Einem netten Kerl wie Felten würden die meisten dagegen nur hehre Ziele unterstellen. Deshalb denken Initiativen wie die Electronic Frontier Foundation bereits darüber nach, ihn zur Gallionsfigur im Kampf gegen den Kopierschutz-Wahn zu machen. Denn wenn Organisationen wie die RIAA einem Professor wie Felten das Recht auf freie Rede verweigern, dann finden das die Schwiegermütter und -väter Amerikas gar nicht lustig.

Der Text erschien erstmals in der Ausgabe 47 (Mai 2000) der De:Bug- Zeitschrift für elektronische Lebensaspekte

The Script Kiddies Are Not Alright

Boris Gröndahl

In der Berichterstattung ist die Sache klar: Es vergeht kaum ein Monat, in dem nicht irgendeine Zeitung, ein Nachrichtenmagazin oder einer der Infotainmentclips, die auf den kommerziellen TV-Kanälen die Zeit zwischen den Werbeblöcken überbrücken, eine Schauergeschichte über Hacker zu berichten hat. Hier legen sie eine Website lahm, da stehlen sie Kreditkartennummern und dort verbreiten sie Viren und Würmer, die E-Mail-Systeme auf der ganzen Welt mit »Liebesbriefen« oder Ähnlichem verstopfen. Im öffentlichen Sprachgebrauch ist längst entschieden: Hacker sind bestenfalls jugendliche Delinquenten, schlimmstenfalls destruktive Terroristen. Sie lauern im Cyberspace und haben es dank schwarzer Computermagie in der Hand, den Stecker aus der Informationsgesellschaft zu ziehen.

Im kanonischen Schrifttum der Hacker, jedenfalls der US-amerikanischen, ist die Sache freilich ebenso klar: Was in den Medien unter »Hacker« läuft, hat mit den »wahren« Hackern nichts zu tun. Das Jargon File - eine Art Enzyklopädie des Hackertums, die seit 1975 von freiwilligen Autoren kontinuierlich aktualisiert und erweitert wird - erklärt gebetsmühlenhaft immer wieder, dass böse Hacker gar keine seien, sondern richtig »Cracker« genannt werden müssen. Sie fordert die Leser auf, Journalisten, die diese begriffliche Verwechslung begehen, denselben Leserbrief zu senden, den einst Richard Stallman, der Gründer der Free Software Foundation und sprichwörtliche »letzte wahre Hacker« [1], ans »Wall Street Journal« richtete. Darin heißt es:

> »Ich bin ein Hacker. Mit anderen Worten, ich habe Spaß daran, mit Computern herumzuspielen - daran, mit cleveren Computerprogrammen zu arbeiten, daran, sie zu begreifen, und daran, sie zu schreiben. Ich bin kein Cracker; ich beschäftige mich nicht damit, Computer-Sicherheitssysteme zu knacken. Das Hacken, wie ich es betreibe, ist nichts, wofür ich mich schämen müsste. Aber wenn ich Menschen erzähle, dass ich ein Hacker bin, dann denken sie, ich würde etwas Anrüchiges zugeben -weil Zeitungen wie die Ihre das Wort >Hacker< missbrauchen, indem sie den Eindruck vermitteln, es bedeute >Sicherheitsknacker< und sonst nichts. Sie bringen Hacker in Verruf. [...] Sie schulden Hackern eine Entschuldigung; mehr noch, Sie schulden uns schlicht Respekt.« [2]

Dass die Medien seit Mitte der 1980er Jahre ein Bild von Hackern zeichnen, das zu großen Teilen denunziatorisch und sensationalistisch ist, und dass sie sich oft nicht um authentische Berichterstattung scheren, ist offenkundig. Doch darum soll es in diesem Beitrag nicht gehen. Denn interessant und keineswegs unschuldig ist auch die andere Seite der Auseinandersetzung. Die Empfindlichkeit der Wahren« Hacker gegenüber der falschen Verwendung des Begriffs ist nicht nur ein nerdiger sprachlicher Sauberkeitsfimmel und auch nicht bloß das defensive Bestehen auf »ordinary respect«. In

dem Begriffskampf um das Recht auf die Bezeichnung »Hacker« manifestiert sich auch der Versuch, andere Hacker auszugrenzen. Ein Versuch, der viel damit zu tun hat, wie sich in den vergangenen vierzig Jahren Computer, Netzwerke und mit ihnen die Hackerszene verändert haben.

Steven Levys »Hackerethik«

Schon am Beginn des Problems mit dem Begriff »Hacker« steht ein Journalist. Die wichtigste Grundsatzerklärung des Hackertums stammt nicht von einem Hacker, sondern von Steven Levy, Autor unter anderen der Musikzeitschrift Rolling Stone. Levy brachte 1984 mit seinem Buch »Hacker« das erste Mal einer breiten Öffentlichkeit diese seltsamen Computerfreaks nahe. Die Hackerszene, die er beschrieb, hatte zu diesem Zeitpunkt schon bis zu 30 Jahre auf dem Buckel.

Ein Kapitel aus Levys Buch entwickelte aber vor allem innerhalb der Hackerszene großen Einfluss: Darin schildert er, wie sich um die ersten Computer der 50er Jahre »etwas Neues verdichtete ...: eine neue Lebensweise mit einer Philosophie, einer Ethik und einem Traum.« Aus den vielen Gesprächen, die Levy mit Hackern der ersten und zweiten Stunde geführt hatte, destillierte er Grundwerte der Hackerszene, die er als »Hackerethik« bezeichnete:

> »1. Zugang zu Computern - und allem, was Dich etwas über die Funktionsweise der Welt lehrt - sollte unbegrenzt und umfassend sein. Mitmachen heißt die Devise!
> 2. Alle Informationen sollten frei sein.
> 3. Misstraue Autorität - fördere Dezentralisierung.
> 4. Hacker sollten anhand ihres Hackens beurteilt werden / nicht nach unsinnigen Kriterien wie akademischen Rängen, Alter, Rasse oder Stellung.
> 5. Du kannst mit einem Computer Kunst und Schönheit erzeugen.
> 6. Computer können Dein Leben verbessern.« [3]

Levys Hackerethik wird häufig verwendet als Definition des Begriffs Hacker oder als universelles Selbstverständnis der Szene. Das ist sie jedoch nicht. Es handelt sich hierbei nicht um Beschlüsse oder Diskussionsergebnisse irgendeiner Gruppe, nicht um Eintrittsbedingungen, nicht um Selbstverpflichtungen. Levys Hackerethik ist nichts anderes als seine nachträgliche (und wohlwollende) Interpretation einer bestimmten historischen Konstellation.

Sie ist gekennzeichnet durch eine soziologische Situation: Levy beschreibt weiße angelsächsische Jungs an US-Eliteuniversitäten der 50er bis 70er Jahre. Diese Akteure hatten sich zudem mit technischen Gegebenheiten auseinander zu setzen: Computer und Rechenzeit waren knappe, teilweise - wenigstens nach Auffassung der Hacker - auch künstlich knapp gehaltene Güter, die von einer bürokratischen Elite, den »Hohen Priestern« der Großrechner, eifersüchtig gehütet wurden. Computer waren tendenziell eine Angelegenheit des Militärs, keinesfalls eine Technik für jedermann.

Ob Levys Interpretation zutrifft, soweit es um die Gruppe geht, aus der sich in den 50er Jahren etwa am legendären Massachusetts Institute of Technology (MIT) die Hacker rekrutierten, kann hier gar nicht entschieden werden. Wichtig ist nur festzuhalten, dass seine Hackerethik nicht die Eintrittskarte zum Hacker-Sein ist oder war und auch nicht die typische oder gar einzige Motivation, die jemanden zum Hacker werden lasst.

In einer Diskussion der legendären Mailbox The Well, die 1989 aus Anlass eines Hacker-Kongresses geführt wurde, wurde Levy bereits für seine selektive Wahrnehmung kritisiert. In den Worten von Jef Poskanzer, einem der Teilnehmer der Online-Diskussion: »Mir ist inzwischen klar geworden, dass die > Hackerethik< nie wirklich existiert hat. Letzten Endes hat sich Steven Levy von Richard Stallman einreden lassen, eine sehr eingeschränkte Sichtweise einiger Hacker darzustellen und so zu tun, als sei das die ganze Geschichte. Aber das war sie niemals. Selbst damals war mehr dran am Hacken als Stallmans Philosophie glauben macht ... Beim Hacken geht es ums Erkunden und ums Erschaffen. Hacken liegt quer zu ethischen Prinzipien.«

Praktisch zeitgleich mit Levys Buch kam der Film »War Games« in die Kinos, in dem ein amerikanischer Vorstadt-Teenager mit seinem PC vom Kinderzimmer aus in die Rechner des Pentagon eindringt und so beinahe den Dritten Weltkrieg auslöst. Damit war die Verunreinigung von Levys emphatischem Verständnis von Hackern durch die Medien geschehen, über die sich Levy im Nachwort zu einer späteren Auflage bitter beklagt.

Gute Hacker, böse Cracker

Seitdem wird die Auseinandersetzung um die Definitionshoheit über den Begriff »Hacker« geführt. Das Jargon Eile gibt die folgenden Umschreibungen:

> »:Hacker: n. [ursprünglich jemand, der Möbel mit einer Axt herstellt]
> 1. Jemand, der Spaß daran hat, die Einzelheiten programmierbarer Systeme zu erforschen und bis an die Grenzen ihrer Fähigkeiten zu gehen, im Gegensatz zu normalen Usern, die lieber nur das notwendige Minimum lernen.
> 2. Jemand, der begeistert (sogar obsessiv) programmiert oder dem das Programmieren mehr Spaß macht als das Theoretisieren darüber.
> 3. Jemand, der in der Lage ist, einen guten Hack zu erkennen.
> 4. Jemand, der besonders schnell programmieren kann.
> 5. Ein Experte für ein bestimmtes Programm oder jemand, der häufig damit arbeitet; man sagt etwa >Unix Hacker«. (Definitionen 1 bis 5 hängen miteinander zusammen, und die Menschen, die ihnen entsprechen, sind häufig die selben.)
> 6. Ein Experte oder Enthusiast jeder Art. Zum Beispiel ein. Astronomie-Hacker.
> 7. Jemand, der die intellektuelle Herausforderung liebt, auf kreative Weise Hindernisse zu überwinden oder zu umgehen.
> 8. [abwertend] Böswilliger Fummler, der versucht, geheime Informationen zu entdecken, indem er herumstochert. In diesem Sinne: >Passwort-Hacker<, >Netzwerk-Hacker<. Die korrekte Bezeichnung für diese Bedeutung ist >Cracker<.«

Über diese »Cracker« haben die Autoren des Jargon Files (der prominenteste ist derzeit Eric Raymond, der Vertreter des rechten neoliberalen Flügels der Bewegung für freie/quelloffene Software) dagegen nur Mokantes zu bemerken:

> »:Cracker: n. Jemand, der die Sicherheit eines Systems durchbricht. Geprägt um 1985 von Hackern, die sich gegen den journalistischen Missbrauch des Begriffs >Hacker< zur Wehr setzten. [...] Man wird bei jedem echten Hacker davon ausgehen können, dass er Erfahrung mit spielerischem Cracken gesammelt hat und die grundlegenden Techniken beherrscht. Doch von jedem, der aus dem Larvenstadium herausgewachsen ist, wird erwartet, dass er diesem Bedürfnis widersteht, es sei denn, er muss in einer bestimmten Situation aus gutwilligen, praktischen Gründen cracken (zum Beispiel wenn es notwendig ist, irgendwelche Sicherheitsmaßnahmen zu umgehen, um arbeiten zu können).«

Obwohl man sich erkennbar Mühe gibt, die Denunziation der Medien gegenüber »Crackern« nach besten Kräften mitzumachen, verraten beide Definitionen bereits das grundlegende Dilemma. Die Grenze zwischen der in Punkt sieben als zulässig definierten »intellektuellen Herausforderung, auf kreative Weise Hindernisse zu überwinden oder zu umgehen« und dem in Punkt acht abgelehnten »Fummeln« und »Schnüffeln« ist natürlich historisch völlig variabel und letztlich bloß künstlich und willkürlich. Auch die für die Autoren offenbar vollkommen unproblematischen Grenzen des Kavaliersdelikts »spielerisches Cracken« und des Crackens als typisches Entwicklungsstadium, aus dem man herauswächst, sind selbstverständlich fließend und verwaschen.

Diskussionen innerhalb der Hackerszene

Ignorante Journalisten waren denn auch nicht die einzigen, die Levys Hackerethik in den 17 Jahren seit ihrem Erscheinen anders interpretiert haben, als ihr Autor es gerne hätte. Die Geister schieden sich in den 80er Jahren vornehmlich an der Frage, ob bereits das Eindringen in fremde Computersysteme gegen die Hackerethik verstoße oder ob erst das bösartige Manipulieren unzulässig sei. Das Jargon File ist wiederum restriktiv; es zitiert zwar mit spitzen Fingern und zugehaltener Nase als eine mögliche Definition von »Hackerethik«: »Die Überzeugung, dass das Knacken von Systemen aus Spaß und Neugier ethisch OK ist, solange der Cracker nicht Diebstahl, Vandalismus oder Vertraulichkeitsbruch begeht«, beeilt sich aber hinzuzufügen, dass nicht alle Hacker dieses Verständnis teilen.

Wie man mit dem Thema auch anders umgehen kann, lässt sich beispielhaft nachvollziehen an der Geschichte des deutschen Hackervereins Chaos Computer Club (CCC). Gegründet Anfang der 80er Jahre standen seine Mitglieder der ersten Generation wegen der lächerlich restriktiven Fernmeldegesetze der Bundesrepublik ungewollt stets mit einem Bein im Gefängnis. Eine der ersten Aktionen des Clubs war das Verbreiten eines Bausatzes für ein Modem. Wer das zusammengesetzte Gerät ans Telefonnetz anschloss, wurde nicht etwa als Pionier der Informationsgesellschaft geehrt, sondern machte sich strafbar.

Die frühen Ausgaben der CCC-Zeitschrift »Datenschleuder« strotzen auf jeder Seite von nonchalanten, aber gerissenen Anspielungen auf die empfohlene Missachtung dieser Gesetze. Gleichwohl bemerkte der CCC im Laufe der Jahre, dass er den Geist nun nicht so einfach wieder in die Flasche bekam: Die Computerfans, die nun das illegale Modem besaßen, wollten auch etwas damit anfangen, und in Ermangelung interessanter öffentlicher Angebote stromerten sie eben in nichtöffentlichen herum.

Das warf neue Probleme auf. Es war einfach gewesen, die autoritären Fernmelderegeln der Bundespost schlicht abzulehnen. Doch bei ihren Datenreisen stießen Leute aus dem CCC-Umfeld auf Material, das Begehrlichkeiten bei konkurrierenden Firmen, Geheimdiensten und Medien weckte. Und die der Informationsfreiheit verpflichteten Hacker, die stets für die Herstellung von Öffentlichkeit plädiert hatten, fanden sich plötzlich auch inmitten privater Daten wieder, die sie eigentlich eher gerne geschützt gesehen hätten.

Das führte zu moralischen Konflikten, die den CCC schließlich zu einer Anpassung der Levyschen Regeln brachten. Er übernahm Levys Prinzipien als seine eigenen; betonte, dass neben Hautfarbe und gesellschaftlicher Stellung auch das Geschlecht kein zulässiger

Maßstab für die Beurteilung von Hackern sei; und fügte den Regeln noch zwei hinzu, die sich aus den Erfahrungen in den Datennetzen ableiteten:

> »Mülle nicht in den Daten anderer Leute.
> Öffentliche Daten nützen, private Daten schützen.« [4]

Mit dem Verständnis des Jargon Files ist diese Position des CCC offensichtlich vollkommen unvereinbar. Tatsächlich wird in ihr der Club als Bande von »alienated, drug-addled crackers« beschimpft, ein Image des CCC, das in den USA dank der denunziatorischen Werke von Clifford Stoll [5] und (etwas abgemildert) Katie Hafner/John Markoff [6] gang und gäbe ist. Derselbe Verein ist in Deutschland synonym mit den geradezu amtlichen Hackern und wird bekanntlich von Regierung, Parteien, Banken, Industrie, Datenschützern und Medien gleichermaßen als Experten-NGO konsultiert. Um die Verwirrung komplett zu machen, schimpfen die In den USA als Outcasts geltenden CCC-Mitglieder in Diskussionen über jugendliche Daten-Bad-Boys ihrerseits fast mit denselben Worten, mit denen sie in der US-Debatte belegt werden.

Externe und interne Grenzziehungen

Es ist klar, dass sich die Binnenwahrnehmung und Selbstdefinition von Gruppen wie Hackern nicht nach wissenschaftlichen Kriterien richtet, sondern auch der Abgrenzung untereinander und nach außen dient. Soweit es um Hacker geht, können vier wichtige Selbstverständnis-Komplexe unterschieden werden:

Die »wahren« Hacker

Die »wahren« Hacker sind das normative Ideal des Jargon Files. Ihrem Selbstverständnis nach unorthodoxe, genialische Programmierer, die dem Ideal der Informationsfreiheit verpflichtet sind, staatliche Autoritäten, gewisse Großunternehmen (IBM, Microsoft) und einige kulturelle Konventionen ablehnen. Zur Zeit dürfte diese Variante hauptsächlich in den Linux-/Open-Source-/Free-Software-Communities anzutreffen sein. Obwohl sie tendenziell Regeln missachten, die sie nicht selbst aufgestellt haben oder die sie für unsinnige und überflüssige Beschränkungen halten, propagieren sie keine illegalen Aktionen. Auch innerhalb dieser Definition gibt es eine große Bandbreite an Differenzierungen, die man personell an den Antipoden Eric Raymond (einem Vertreter eines typisch amerikanischen ultraliberalen Markt- und Waffenfetischismus) und Richard Stallman (einem ebenso typisch amerikanischen Linksliberalen) festmachen kann.

Die »aufklärerischen« Hacker

Das charakteristische Selbstverständnis des CCC ist es dagegen, die Informationsgesellschaft über sich selbst und die Geister, die sie ruft, aufzuklären. Eine ähnliche Haltung findet sich bei den niederländischen Hackern und in den USA rund um die Zeitschrift 2600. Seit 1983 pflegt er die Strategie, Sicherheitslücken etwa bei Banken und Telefongesellschaften zu ermitteln und sie dann öffentlichkeitswirksam zu

präsentieren. Das hat ihm in den USA das oben geschilderte Cracker-Image, in Deutschland allerdings eher das eines Daten-Robin-Hood eingebracht, dessen Informationen erstens seriös sind und zweitens nicht zum eigenen Vorteil verwendet, sondern an die Öffentlichkeit gegeben werden. Die stärkere politische Erdung dieser Gruppe zeigt sich auch in der Verwendung sozialer Hack-Techniken wie Adbusting oder Medien-Hacking. Viele Vertreter dieser Version würden allerdings die Ausgrenzung des Jargon Files nicht auf sich beziehen, sondern auch für sich in Anspruch nehmen, wahre«Hacker zu sein.

Die Bösen Buben: Script Kiddies, warez d00dz und Freunde

Auch die Hacker der zweiten Generation distanzieren sich heute von den so genannten »Script Kiddies«. Die abschätzige Bemerkung über jene Bad Boys, von denen dieser Band hauptsächlich handelt, spricht das schlimmste Verdikt aus, das einem Hacker widerfahren kann: dass er in Wirklichkeit nicht programmieren kann, sondern nur mit vorgefertigten Werkzeugen unkundig herumhantiert. Der Teil der Hackerszene, gegen den sich solche Beleidigungen richten, fühlt sich mit seinem Bad-Boy-Image indes gar nicht so unwohl und integriert es in die eigene Selbstdarstellung. Zu den popkulturellen Vorbildern, die sich in den Pseudonymen und Gruppennamen widerspiegeln, gehören Punk, Heavy Metal, Grunge und Hip Hop. Die Demo/Warez/Viren-Szene ist tendenziell jung und wesentlich stärker von Immigranten geprägt als die traditionelle Hackerszene - weiblicher ist auch sie allerdings nicht.

Polithacker: Von den Yippies nach Seattle

Eine besondere Untergruppe stellen schließlich jene Hacker dar, die ihr verbotenes technisches Wissen in den Dienst politischer Aktionen stellen. Diese Gruppe hat eine lange Tradition. Ihre bekannteste Vertreterin war in den 60er Jahren in den USA die »Youth International Party«, die so genannten Yippies. Die Yippies waren eine recht Aufsehen erregende Spaßguerilla mit Wurzeln in der Beat Generation, berühmt für an den Situationismus erinnernde Aktionen wie die, ein Schwein in der US-Präsidentschaftswahl gegen Richard Nixon kandidieren zu lassen. In ihrem Newsletter »Youth International Party Line« gaben sie praktische Tipps zum kostenlosen Telefonieren mit Hilfe der so genannten Blueboxen, was sie als Protest gegen den Vietnamkrieg propagierten. In den letzten Jahren wurden technische Sabotage-Aktionen wie Denial-of-Service-Attacken oder das Manipulieren von Websites (»Defacing«) vor allem zunehmend in politische Kampagnen integriert. Beispiele sind Internetangriffe gegen die mexikanische Regierung aus Anlass der Chiapas-Aufstände oder Aktionen von Globalisierungsgegnern im Umfeld von Treffen der WTO oder des World Economic Forum in Davos. Ein Sonderfall sind diese Polithacker insofern, als sie häufig den Begriff »Hacker« gar nicht für sich in Anspruch nehmen, auch wenn sie klarerweise Hackertechniken anwenden.

Wozu all diese Abgrenzungswut?

Der Versuch der »wahren« Hacker, sich gegenüber ihren schlechter beleumundeten Verwandten abzugrenzen, muss notwendig auf künstliche und willkürlich bestimmte Kriterien zurückgreifen. Es gibt keine positive Definition des Begriffs »Hacker«, die illegale, verbotene, sogar illegitime Tätigkeiten nicht wenigstens implizit auch mit einschließen würde. Denn keine wie auch immer geartete Definition des Begriffs, die überhaupt zur Unterscheidung taugt, kommt aus, ohne dass auf das Brechen von Regeln rekurriert wird, auf Wissen, das entweder nicht dem Mainstream gehört oder ihm entwendet wurde, auf den Umgang mit Technik in einer Weise, die nicht beabsichtigt war. Lässt man den expliziten Anti-Cracker-Paragraphen aus der Definition des Jargon Files weg, so findet sich nichts in ihr, was verbieten würde, »Cracker« als Hacker zu bezeichnen. Im Gegenteil, Paragraph sieben (»Umgehen von Hindernissen«) lädt geradezu dazu ein, sie als Teil der Gemeinde zu verstehen.

Klar ist auch, dass des einen Kavaliersdelikt des anderen Straftat ist. Levys »Hacker« und auch das Jargon File kennt zahllose Beispiele von Regelübertretungen, die in den Augen der »wahren« Hacker harmlose Jungsstreiche, befreiende Heldentaten oder berechtigten Ungehorsam darstellen. Aber diejenigen, gegen die sie sich richteten, haben zu ihrer Zeit natürlich ebenso über »delinquente Jugendliche« geschimpft wie die Wahren« Hacker es heute tun.

Warum dann diese Abgrenzungswut? Veränderte individuelle Lebensumstände können sicher teilweise zur Erklärung dieser zweierlei Maßstäbe dienen. Wer sich mühsam vom Außenseiter in die Mitte der Gesellschaft vorgearbeitet hat, mag nicht von späteren Generationen daran erinnert werden, dass er nun seine Rebellenposition aufgegeben hat. Auch dass ihm die heutigen Codes der Jugendkultur - ihre Musik, ihre Mode, ihre Sprache - nichts mehr sagen, mag schwer zuzugeben zu sein. Auch der gesellschaftliche Kontext hat sich während 40 Jahren Hackergeschichte gewandelt. Computer sind heute - nicht zuletzt dank der Hacker - keine Veranstaltung in der abgeschirmten heilen Welt weißer Eliteuniversitäten mehr. Damit haben sich auch die Zwecke, zu denen sie eingesetzt werden können, vervielfältigt. Und nicht zuletzt hat die massive Kriminalisierung der Hackerszene, die insbesondere in den USA seit Anfang der 90er Jahre stattgefunden hat (von Bruce Sterling in »The Hacker Crackdown« [7] und von Josh Quittner / Michelle Slatalla in »Masters of Deception« [8] eindrucksvoll beschrieben), einen Distanzierungsdruck erzeugt, dem sich viele nicht entziehen konnten.

Literatur

[1] Steven Levy, Hackers. Heroes of the Computer Revolution, New York 1984

[2] The on-line Hacker Jargon File, Version 4.3.0
http://www.tuxedo.org/~esr/jargon/, abgerufen am 7. Mai 2001

[3] Steven Levy, a. a. O.

[4] Chaos Computer Club, Die Hacker-Ethik,
http://www.ccc.de/Hackerethik.html, abgerufen am 7. Mai 2001

[5] Clifford Stoll, The Cuckoo's Egg. Tracking a Spy through the Maze of Computer Espionage, New York 1989

[6] Katie Hafner und John Markoff, Cyberpunk. Outlaws and Hackers on the Computer Frontier, New York 1991

[7] Josh Quittner und Michelle Slatalla, Masters of Deception. The Gang that Ruled Cyberspace, New York 1995
[8] Bruce Sterling, The Hacker Crackdown. Law and Disorder on the Electronic Frontier, New York 1992

Boris Gröndahl, geboren 1967 in Marburg, ist Berlin-Korrespondent des Nachrichtenmagazins »The Industry Standard«. Nach dem Studium der Mathematik und Physik war er Redakteur der Zeitschrift konkret, Verlagsleiter der Tageszeitung Junge Welt, freier Journalist und Redakteur der Financial Times Deutschland. 1996 kuratierte er die Ausstellung »Hacker« im Heinz Nixdorf Museumsforum, Paderborn. 2000 erschien das Buch »Hacker« in der Reihe Rotbuch 3000.

4. Info-Krieger und Freiheitskämpfer

Krieger in den Datennetzen

Ralf Bendrath

Die Gefahr eines groß angelegten Angriffs aus dem Cyberspace gehört heute zum Standardrepertoire der Reden, Strategieentwicklungen und Studien amerikanischer Sicherheitspolitik. Bereits seit zehn Jahren wird vor dem »elektronischen Pearl Harbor« gewarnt, das durch eine »Softwarebombe auf dem Aktienmarkt«, einen durch Hacker verursachten Ausfall von Flugsicherungssystemen oder massive Denial-of-Service-Attacken auf die amerikanische Internetwirtschaft ausgelöst werden soll. Die chinesische Volksbefreiungsarmee, die islamischen Terroristen von Osama Bin Laden oder sogar das abgewirtschaftete Militär Kubas gehören laut Angaben der US-Geheimdienste zu den möglichen Gegnern, die sich auf die virtuelle Kriegführung in den Datennetzen vorbereiten.

Was in den strategischen Analysen wie in den jede Horrormeldung aufgreifenden Medien allerdings nie genannt wird, ist der Ursprung dieses neuen Wettrüstens. Begonnen hat die militärische Eroberung des Cyberspace nämlich nicht in den Bergen Afghanistans oder den Militärakademien Chinas, sondern in den USA selber. Seit Anfang der 1990er Jahre haben die US-Streitkräfte in ihren Forschungslabors elektronische Waffen für den Hacker-Krieg entwickelt, in den Denkfabriken theoretische Grundsatzanalysen erstellt und in den Planungsstäben neue Einsatzdoktrinen geschrieben. Bereits mehrfach wurden von US-Spezialtruppen Cybereinsätze durchgeführt, so zuletzt im Kosovokrieg 1999. Vieles davon findet bis heute unter strikter Geheimhaltung statt. Was an öffentlich zugänglichen Quellen verfügbar ist, lässt sich allerdings zu einem recht umfassenden Bild der amerikanischen Cyberkrieger, ihrer Waffen und Organisationen zusammensetzen. Dabei zeigen sich auch die inneren Widersprüche und Schwierigkeiten, die mit einem solchen Kriegsbild verbunden sind, und es zeigt sich die Notwendigkeit, in diesem Bereich über neue Formen der Rüstungskontrolle nachzudenken.

Zwei Entwicklungslinien - eine technische und eine strategische - haben vor allem zu den aktuellen Bemühungen der USA für einen Krieg in den Datennetzen geführt.

Zum einen hat die militärische Verwendung von Elektronik und Computertechnologie eine lange Geschichte - immerhin wurden die ersten Computer von britischen und amerikanischen Abhörspezialisten zur Entschlüsselung der deutschen Militärkommunikation im Zweiten Weltkrieg entwickelt. Nach der Einführung von Radar, drahtloser Kommunikation und elektronisch gelenkten Bomben entwickelte sich ein eigener Teilbereich der so genannten »elektronischen Kriegführung«. Mit Signal-Störern (»Jammern«), elektronischen Täuschkörpern und Waffen, die Signale suchen und ihre Sendeanlagen zerstören, entwickelte sich in den 1980er Jahren sogar ein eigener Rüstungswettlauf zwischen »electronic Countermeasures« und »electronic Counter-Countermeasures«, dessen Ziel es war, das elektromagnetische Spektrum vollständig zu nutzen und dem Gegner genau dies unmöglich zu machen. Die Mittel dazu waren

Waffensysteme wie die Anti-Radar-Rakete »HARM«, spezielle elektronische »Kampfflugzeuge« wie die EC-130H »Compass Call« oder der EA-6B »Prawler« und eine hoch entwickelte Elektronik zur stör- und abhörsicheren Kommunikation. Diese Entwicklung war allerdings in der Situation der nuklearen Abschreckung politisch nicht besonders interessant und wurde daher vor allem technologisch betrieben. Darüber hinaus fielen solche Maßnahmen in den Bereich der »Operations Security« und waren bei den Militärgeheimdiensten und Aufklärungseinheiten angesiedelt. Deren institutionelle Sonderrolle - nicht den Kommandeuren der kämpfenden Truppen unterstellt zu sein - verhinderte ein Nachdenken darüber, ob und wie man die Kriegführung mit Hilfe moderner Elektronik grundlegender verändern kann.

Hierzu brauchte es andere Einflüsse auf anderen, nichttechnischen Wegen. Diese kamen von den historisch geschulten Denkern des Pentagon, die wie John Arquilla an der Naval Postgraduate School in Monterey, David Ronfeldt und Martin Libicki in der Pentagon-nahen Denkfabrik RAND Corporation in Santa Monica oder Dan Kuehl an der National Defense University in Washington lehrten und forschten. Sie und andere begannen Anfang der 1990er Jahre, über gesellschaftliche - und damit auch militärische - Veränderungen durch neue Informationstechnologien nachzudenken. Entsprechend dem neoliberalen Zeitgeist basierten die ersten Studien auf neuen Managementkonzepten mit flexiblen Organisationsformen und flachen Hierarchien. Mit der Ausbreitung des Internets und der entstehenden Diskussion um die »Informationsgesellschaft« geriet dann das Konzept von Information als Ressource ins Zentrum der Aufmerksamkeit. Wenn postindustrielle Gesellschaften und ihre Streitkräfte nicht mehr vor allem auf Menschen und Maschinen als Mittel von Produktion oder Destruktion angewiesen sind, so die Überlegungen, dann sind die Angriffsziele militärischer Operationen nicht mehr die Kräfte des Gegners, sondern seine Informationsverarbeitungssysteme. [1]

Institutionalisierung und Operationalisierung

Damit erreichte der »Informationskrieg« das militärstrategische Denken. Erste Überlegungen dafür waren zwar bereits in den 1970ern angestellt worden, aber erst in den 1990er Jahren mündeten sie in eine breitere Diskussion über neue Ziele, Strukturprinzipien und Möglichkeiten der Kriegführung. Bereits 1992 wurde die erste streng geheime Direktive TS-3600.1 des Pentagon zu »Information Warfare« geschrieben, mit der ein bis heute andauernder organisatorischer und strategischer Reformprozess begann.

Die Debatte um Informationskriegführung verankerte sich schnell auch organisatorisch im militärischen Apparat. Die Folge war die Gründung der School for Information Warfare and Strategy an der National Defense University in Washington im Jahr 1994 sowie die Einrichtung und Umwidmung verschiedener Einheiten für den »Informationskrieg«. Bereits ein Jahr später war »Information Warfare« das Leitbild für alle Forschungs- und Entwicklungspläne des US-Militärs, und Air Force und Army legten als erste Teilstreitkräfte eigene Strategieentwürfe vor. Die Navy erstellte 1995 ihre Instruktion OPNAVINST 3430.26 zur Umsetzung des Informationskriegs, und auch das Marine Corps verfügt mittlerweile über die Order 3430.1, »Policy for Information Operations«. Im Jahr 1996 wurden weitere Schlüsseldokumente erstellt. Zwei Tage nach dem Jahreswechsel legte der Vorsitzende der Vereinigten Stabschefs im Pentagon die Anweisung CJCSI 3210.01, »Joint Information Operations Policy«, vor. Im August veröffentlichte die Army ihr neues Field

Manual 100-6, »Information Operations«, und im Dezember verfasste der Generalstab die ebenfalls geheime Ergänzung S-3600.1, »Information Operations«, zu seiner Direktive von 1992.

Der »Informationskrieg« ist nach den seitdem geltenden Vorstellungen der US-Streitkräfte ein übergreifendes Konzept, das weit mehr umfasst als reine Computerattacken. Im Kern besteht es aus der Idee, nicht mehr die Kräfte oder den Raum des Gegners zu erobern, sondern seine Informationsflüsse zu kontrollieren. Das Ziel ist die vollständige »Informationsüberlegenheit«. Die Mittel dazu können Elemente der psychologischen Kriegführung wie Flugblätter oder Radiosender, Täuschungsmanöver, »normale« Bomben auf Kommunikationszentralen oder -leitungen und eben auch elektronische Angriffe sein.

Dieser umfassende Anspruch konnte aber nur teilweise eingelöst werden - zu schwierig ist es, ein fremdes soziales System, dessen technische Infrastruktur eben nur einen Teil des Ganzen darstellt, genau zu kennen und die Wirkungen von einzelnen Eingriffen in allen Verkettungen abzuschätzen. Dies gilt bis heute, wie in der aktuellen Praxis deutlich zu sehen sein wird. Die militärische Umsetzung in Form des »Command and Control Warfare«, dessen Militärdoktrin ebenfalls 1996 vorgelegt wurde, [2] zielt daher nach alter Art vor allem auf die Zerstörung der Kommunikationsinfrastrukturen des Gegners, um seine Kampftruppen von ihrem »Kopf« in den Kommandozentralen abzuschneiden. Dies wurde bereits im Golfkrieg 1991 betrieben: Die ersten irakischen Ziele, die von den USA angegriffen wurden, waren Sendemasten, Telefonzentralen und Brücken, in denen Kommunikationskabel verliefen. Viele irakische Einheiten waren so von der Verbindung zu ihren Führungsebenen abgeschnitten und wurden handlungsunfähig. Darüber hinaus wurden gezielt irakische Kommandobunker angegriffen.

Die konkreten Anstrengungen der US-Streitkräfte in diesem Bereich richteten sich aber bis Mitte der 1990er Jahre vor allem darauf, die eigenen Datennetze, Sensoren und Kommandosysteme gegen Hackerangriffe und gegnerisches Eindringen abzuwehren. Man konzentrierte sich zunächst auf die Wiederherstellung der Systeme im Fall eines Angriffs und richtete auch die militärische Softwareentwicklung an diesem Ziel aus. Dies macht einerseits Sinn, denn bevor man in die Computer anderer eindringt, um sie zu verfälschen oder zu zerstören, sollte man sich gründlich vor einem Gegenschlag schützen. Andererseits spiegelt diese Schwerpunktsetzung die generelle Politik der Clinton-Regierung wider, die sich seit 1996 systematisch mit dem Schutz der US-Infrastrukturen vor Hacker-Angriffen befasste. [3] Im Hintergrund und unter strengster Geheimhaltung begann man aber in den Streitkräften, nun systematischer auch offensive Konzepte des Cyberkriegs zu entwickeln. Erstmals wurde 1996 in der Direktive S-3600.1 auch der neue Begriff der »Computernetzwerkattacken« (»Computer Network Attack«, CNA) verwendet. Diese umfassen »Operationen zur Unterbrechung, Verweigerung, Verschlechterung oder Zerstörung der Informationen, die in Computern oder Netzwerken gehalten werden, oder der Computer und Netzwerke selber«. Bis Ende der neunziger Jahre liefen diese Entwicklungen in der Abgeschiedenheit der militärischen Geheimdienste und Forschungslabors, und Angehörigen der Streitkräfte war es noch 1998 verboten, den Begriff »offensive Computer-Operationen« in der Öffentlichkeit zu verwenden. Auch im Kongress wurden die Programme nicht offen diskutiert. Bei einer Anhörung des Senats zur defensiven Seite der Informationskriegführung im Juni 1998 antwortete CIA-Direktor George Tenent auf die Frage, ob offensive Fähigkeiten entwickelt würden, nur mit einem Satz: We're not asleep at the switch in this regard.« Gleichzeitig war allerdings die Debatte in der Öffentlichkeit durch Winn Schwartaus Webseite www.infowar.com, eine Reihe populärer Veröffentlichungen, diverse konzeptionelle Artikel in den militärischen

Fachblättern und einige Presseberichte so weit gediehen, dass man mit der Geheimhaltungspolitik im Pentagon nicht mehr weiterkam. Diese hatte nämlich auch verhindert, dass die Kommandeure der kämpfenden Truppen sich ein genaues Bild davon machen konnten, was für Instrumente ihnen überhaupt in diesem neuen Bereich zur Verfügung stehen und wie sie bei der Einsatzplanung damit verfahren sollen. Die vereinigten Stabschefs hatten bereits 1997 für die Truppe eine Broschüre erstellen lassen, in der es u.a. hieß: »Der Informationskrieg wird in allen Phasen und im gesamten Bereich militärischer Operationen und auf jedem Level der Kriegführung angewandt.« Diese recht allgemeine Anweisung erforderte allerdings für die Kommandeure, die klare Operationsprozeduren gewohnt sind, eine genauere Erläuterung. Sie wurde vom Generalstabsvorsitzenden Henry Shelton am 9. Oktober 1998 in Form der Militärdoktrin JP 3-13, »Information Operations«, vorgelegt. Diese beschreibt neben der Verteidigung der eigenen Informationssysteme, wie »offensive Informationsoperationen« durchgeführt und welehe Ziele auf strategischer oder taktischer Ebene wie ausgewählt werden, wie die Organisationsstruktur und die Kommandokette aussehen und die Erfolge der Maßnahmen ermittelt werden sollen.

Trotz der allgemeinen Offenheit, mit der das Thema »Informationsoperationen« seitdem in den US-Streitkräften behandelt wird, herrscht zum heiklen Bereich der Computerattacken noch immer überwiegend Stillschweigen. Welche Techniken den US-Cyberkriegern zur Verfügung stehen, ist unter strengster Geheimhaltung. In der »Joint Doctrine for Information Operations« wird etwa im Kapitel II, »offensive Informationsoperationen«, ausführlich auf die anderen Methoden wie psychologische Kriegführung, Täuschung, elektronische Kriegführung oder Medienaktivitäten eingegangen, nur für den Bereich »Computer Network Attacks« findet sich lediglich ein Verweis auf den geheimen Anhang A, »Supplemental Information Operations Guidance«. Es lassen sich jedoch aus offenen Quellen einige Rückschlüsse ziehen, mit welchen Methoden die Informationskrieger arbeiten.

Zielsuche: Wie erfasst man alle Datennetze der Erde?

Die größte Herausforderung beim Krieg in den Computern besteht zunächst darin, möglichst viele Daten über die Informationssysteme des Gegners zu sammeln. Dies geschieht mit herkömmlichen Mitteln der Spionage, mittels elektronischer Überwachung des Funkverkehrs anderer Staaten (Signals Intelligence} und durch die Auswertung offener Quellen. Eine enge Verbindung findet sich zu Techniken der elektronischen Kriegführung. Auch hier werden elektromagnetische Signale in die Systeme möglicher Gegner eingespeist (»electronic probing«), um Informationen über ihre Funktionsweise zu bekommen. [5] Das Air Force Information Warfare Center (AFIWC) führt solche Auswertungen im Rahmen des Projekts »Sensor Harvest« durch. Darüber hinaus wird hier der Bereich »funktionale Netzwerke« der integrierten Pentagon-Datenbank gepflegt, der unter dem Namen »Constant Web« die kämpfenden Truppen mit Informationen über die Kommandosysteme und -netzwerke der Gegner versorgen soll. Für ausgewählte Staaten werden hier die kritischen Knoten in ihren Netzwerken und Infrastrukturen identifiziert. Das National Air Intelligence Center unterhält ebenfalls Datenbanken über die Telekommunikationsnetze verschiedener Länder, die National Security Agency (NSA) betreibt eine umfassende »Adversaries«-Datenbank; und das Joint Warfare Analysis Center ist mit ähnlichen Aufgaben befasst. [6] Die Arbeit grenzt oft an eine Sisyphos-Aufgabe.

Viele Staaten verwenden für sicherheitsreievante Aufgaben proprietäre Computersysteme, deren Funktionsweise ohne den Quellcode nicht erschlossen werden kann. Zudem ist dieser oft in exotischen oder speziell entwickelten Programmiersprachen geschrieben. Ein Pentagon-Mitarbeiter drückte dies sehr treffend aus: »Es gibt mehr als einhundert Ideen für Waffen des Informationskriegs da draußen, und ich würde sagen, dass für 98 Prozent von ihnen nicht die nötigen Aufklärungserkenntnisse vorliegen. Die Leute können nicht sagen, dass ein bestimmtes Land den Computercode > X< auf dem Computer > Y< laufen hat. Oft sind es dort entwickelte Computer mit vor Ort geschriebener Software. Weil es so schwierig ist, eine Computerumgebung zu klassifizieren und detailliert zu beschreiben, ist es ebenso schwer, eine Waffe zu definieren, die man dagegen verwenden kann.« [7]

Erschwerend kommt hinzu, dass zivile und militärische Ziele nicht klar getrennt werden können. Viele Streitkräfte nutzen Satellitenkapazitäten und Breitbandkabel, die von zivilen Telekommunikationsanbietern gemietet werden. Darüber hinaus sollen Computer angriffe nicht nur gegen andere Truppen, sondern auch gegen zivile Infrastrukturen, Terroristen oder als Gegenschlag gegen Cyber-Angreifer eingesetzt werden. Die US-Streitkräfte sind daher trotz Echelon-Überwachung und enger Zusammenarbeit mit den Geheimdiensten nicht in der Lage, alle möglichen in Frage kommenden Systeme elektronisch auszukundschaften. In der Praxis beschränkt man sich daher doch wieder auf die üblichen Verdächtigen: mögliche militärische Konkurrenten, »Schurkenstaaten« oder internationale Terroristen. Auch Hacktivisten können eine Herausforderung darstellen: Als 1998 das Electronic Disturbance Theater (EDT) die Webseite des Pentagon aus Protest gegen die Unterstützung der mexikanischen Regierung in Chiapas elektronisch besetzen wollte, schlugen die Hacker der Defense Information Systems Agency zurück: Sie hatten in der Seite ein Java-Applet eingebaut, welches das vom EDT verwendete Floodnet-Tool und damit den Web-Browser abstürzen ließ.

Die Auswahl von Angriffszielen und der dazu passenden Cyberwaffen ist nicht nur ein technisches Problem. Weil diese Art der Kriegführung nicht mit einer herkömmlichen Panzerschlacht oder strategischer Bombardierung verglichen werden kann, fehlt den Kommandeuren die praktische Erfahrung, die ihnen bei der Entscheidung zwischen einer herkömmlichen Bombe und einem Cyberangriff helfen könnte. Das Air Force Information Warfare Center (AFIWC) hat daher eine Reihe von Simulationshilfen für den Informationskrieg entwickelt, die von der 39th Information Operations Squadron in Hurlburt Field/Florida zu Ausbildungszwecken verwendet werden. An solchen Schulungen nehmen zum Beispiel die Stabsmitarbeiter des Combined Air Operations Center in Vicenza/Italien teil, die bis heute die NATO-Einsätze auf dem Balkan leiten. Weil man den Erfolg eines Cyberangriffs nicht wie einen Bombenkrater auf Satellitenfotos oder Flugzeugkameras sehen kann, arbeitet das AFIWC ebenfalls an Systemen, die eine Visualisierung der Effekte ermöglichen sollen. Eines davon ist SIMDAS, das es erlaubt, dem höchsten Befehlshaber die angenommenen Folgen von Cyberattacken und »Hard-Kill«-Maßnahmen zu präsentieren. Es wird vom Joint Information Operations Center (JIOC) verwendet, das wie das AFIWC auf dem Luftwaffenstützpunkt Kelly in San Antonio/Texas angesiedelt ist. Auch die Naval Information Warfare Activity (NIWA), die in der Zentrale der NSA in Fort Meade/Maryland angesiedelt ist, entwickelt ein Simulations- und Planungssystem zur Unterstützung der Kommandeure im Einsatzgebiet bei Angriffen auf die Kommandosysteme des Gegners. Verschiedene Einheiten entwickeln derzeit sogar weitergehende Werkzeuge, mit denen eine Liste von Angriffszielen automatisch erstellt werden kann, und ein Planungssystem der Luftwaffe soll bis Jahresende fertig sein. Diese Entwicklung ist natürlich heikel, denn wenn man nicht nur den Krieg in den Cyberspace

verlagert, sondern sich auch bei der Durchführung von Software leiten lässt, kann man schnell der Faszination der neuen Technologie erliegen und die realweltlichen und politischen Ziele des Kriegs aus den Augen verlieren. Im Endeffekt geht es bei jedem Krieg nämlich immer noch darum, ein Territorium zu besetzen und den dort ansässigen Machthabern oder Bevölkerungsgruppen seinen Willen aufzuzwingen. Dazu reicht der Cyberkrieg nicht aus, auch wenn seine Apologeten die schönsten Visionen vom »unblutigen elektronischen Krieg« malen.

Noch immer gelten Cyberangriffe als sehr riskante Waffen. Nicht nur, weil man die Kaskadierungseffekte in den attackierten Systemen nicht abschätzen kann und daher ein Angriff auf ein militärisches System unter Umständen doch Zivilisten in Mitleidenschaft zieht, sondern auch, weil international damit Präzedenzfälle geschaffen würden. Daher muss bislang der US-Präsident jeden einzelnen Einsatz von Computerattacken genehmigen, und diese werden stets im Alleingang, ohne Abstimmung etwa mit den Verbündeten in der NATO, durchgeführt. Bis die Cyberwaffen ein Standardelement der Air Tasking Order werden, der im Einzelfall abgestimmten Liste von Angriffszielen, dürfte es daher noch eine Weile dauern.

Die Waffen des Cyberkriegs

Welche Waffen sind es überhaupt, mit denen die Cyberkrieger der USA ausgerüstet sind? Als »Computernetzwerkattacken« bezeichnet das Pentagon »passive Abhörattacken« (Netzwerk-Monitoring oder Entschlüsselung), »aktive Netzwerkattacken« (Computereinbrüche und Angriffe mit »boshaftem Code«), »Insiderattacken« (mit oder ohne Absicht) sowie »Hardware-/Software-Distributionsattacken« (böswillige Modifikationen der Systeme beim Hersteller oder im Vertrieb). [8] Davon sind »Abhören« und »Insider« nichts wirklich Neues. Die weltweiten Abhöraktivitäten des von der NSA betriebenen Echelon-Systems sind hinlänglich bekannt, [9] sie fallen aber im Wesentlichen unter den klassischen Bereich der geheimdienstlichen Aufklärung. Auch eingeschleuste Agenten sind ein altes Mittel der Geheimdienstarbeit, ob sie nun mit der Mikrokamera geheime Dokumente kopieren oder dies per autorisiertem Passwort tun. Interessant sind daher vor allem die Bereiche »Netzwerkattacken« und »Distributionsattacken«. Letztere werden im Rahmen von Standardisierungsregelungen, Exportkontrollen oder durch die enge praktische Zusammenarbeit zwischen US-Computer firmen und der NSA durchgeführt und können an dieser Stelle nicht behandelt werden. Sie waren aber, so viel sei angemerkt, der Grund für die massive Nutzung und Forderung von Open-Source-Systemen sowohl in Russland und China als auch in einigen europäischen Staaten. Im Folgenden sollen vor allem die Netzwerkattacken, auch »Hackerkriegführung« genannt, behandelt werden.

Die Mittel dazu sind vielfältig und werden auch im zivilen Bereich von Hackern und Crackern vielfach verwendet: Computerviren, die sich an andere Programme anhängen; Würmer, die sich selbst verbreiten; »trojanische Pferde«, die als »normale« Programme im Hintergrund unerwünschte Aktivitäten starten; »logische Bomben«, die von Ferne elektronisch ausgelöst werden können. Dazu kommen diverse Skripte und Hilfsprogramme, die beim Überwinden der Sicherheitsvorkehrungen eines Computernetzes dienen. Eine weitere Möglichkeit sind Denial-of-Service-Attacken, die einen Computer so mit Anfragen bombardieren, dass er seine Dienste nicht mehr erledigen kann oder die Bandbreite der Netzwerkverbindung blockiert ist.

Die NSA, die auch für die Sicherheit der Computersysteme des nationalen Sicherheitsapparats der USA zuständig ist, beobachtet sehr aufmerksam die weltweiten Hackeraktivitäten und hält sich über neueste Tools und Tricks auf dem Laufenden. Bei dem an der NSA angesiedelten National Security Incident Response Center (NSIRC) wird eine zentrale Datenbank mit Informationen über Computersicherheitsprobleme gepflegt. Die NSIRC-Abteilung Network Intrusion Analysis Capability hat als Auftrag, ihre »Kunden« mit Detailwissen über Hackertechniken zu versorgen. [10] Dies dient offiziell nur der Abwehr von Angriffen, aber das Wissen kann selbstverständlich auch offensiv verwendet werden. Nicht zufällig haben die Einheiten der Streitkräfte, die mit Informationskriegführung befasst sind, enge Verbindungen zur NSA oder sind sogar dort angesiedelt. Seit 1997 besteht bei der NSA bereits das Information Operations Technical Center (IOTC), in dem Spezialabteilungen aus Geheimdiensten und Streitkräften zusammenarbeiten: die P42-Information Warfare Support Cell der NSA, die Critical Defense Technologies Division der CIA und die Abteilung J-33 »Special Technology Operations« des Pentagon. J-33 verwaltet Dutzende von »schwarzen Programmen« der US-Streitkräfte und rüstet Spezialteams für verdeckte Operationen aus. [11]

Man muss davon ausgehen, dass die Computerspezialisten der NSA in der Lage sind, mit den Standardmethoden der freien Hackerszene in allen weltweit zugänglichen Datennetzen Computereinbrüche zu verüben. Was dies allerdings um ein Vielfaches brisanter macht als die Freizeithacker, sind die immensen Ressourcen, die zur Unterstützung solcher Maßnahmen zur Verfügung stehen. Das gesammelte Wissen über alle bekannten Sicherheitslücken, verbunden mit technischen Informationen über weltweite Kommunikationssysteme aus der »Constant Web«-Datenbank, ungeheuren Rechenkapazitäten für Passwort-Tests und Entschlüsselungen sowie einer komfortablen Personaldecke macht die NSA weitaus gefährlicher als die wichtigtuerischen Script-Kiddies, die ahnungslose Politiker gerne für eine Bedrohung der nationalen Sicherheit halten.

Darüber hinaus ist bekannt, dass sich die US-Streitkräfte bereits seit dem Ende der 1980er Jahre an der Erforschung und Entwicklung von Computerviren beteiligen. Solche eher brutalen Methoden, ein gegnerisches Computersystem zu stören, werden heute allerdings ebenso wenig ernsthaft für den Einsatz vorgesehen wie Würmer oder DoS-Angriffe. Das Ziel der Cyberkrieger ist es, in die Netze einzudringen, ohne dass die Betroffenen es überhaupt bemerken. Vor allem Viren und Würmer sind militärisch kaum zu gebrauchen, weil ihre Ausbreitung kaum begrenzt werden kann. Dazu kommt, dass das Image des Cyberwar als unkontrollierbare elektronische Verwüstung Kommandeure und Politiker bislang davon abgehalten hat, solche Maßnahmen in größerem Umfang zu genehmigen. Die Cyberkrieger sind daher sehr darauf bedacht, ihre Technologien als Präzisionswaffen darzustellen. »Wenn man über Kriegführung in Computernetzen diskutiert, kann man vollständig aus der Bahn geraten und über Würmer und Viren und sich selbst verbreitende Programme reden, und jeder denkt, es ist so etwas wie unbeschränkte Massenvernichtungswaffen«, so Oberst David Kirk, stellvertretender Kommandeur des Joint Information Operations Center. Allerdings werden solche Szenarien durchaus geplant. Ein von den USA verursachter vollständiger Ausfall der Datennetze eines Landes könnte nach Aussagen von Pentagon-Mitarbeitern als elektronischer Warnschuss in einer zugespitzten Krisensituation dienen, um einen Staat doch noch zum Einlenken zu bewegen. [12]

Da Cyberattacken immer noch als Maßnahmen mit Spezialtechnologie gelten, müssen sie einzeln genehmigt werden. Dazu gehören auch genaue Angaben über Ziele, Mittel und

eventuelle Kollateralschäden. »Die nationalen Befehlshaber wollen sicher sein, dass man das System oder den Netzknoten genau identifiziert hat, gegen die man solche Technologien einsetzen will«, so Kirk. Das Ziel der derzeitigen Entwicklungen ist es, dass die Cyberkrieger ihren Kommandeuren in wenigen Jahren sagen können: »Ich kann Ihnen mit einem hohen Grad an Gewissheit versichern, dass das Risiko eines Kollateralschadens X, das Risiko, Technologien zu verraten Y, und das Risiko für US-Systeme Z ist.« Man versucht daher, Techniken zu entwickeln, die genau definierte Effekte hervorrufen. Bereits 1997 wurde im »Joint Warfighter Science and Technology Plan« beklagt, dass für die offensive Informationskriegführung vor allem noch zwei Fähigkeiten fehlen: schnell und automatisch Schwachpunkte in den Systemen des Gegners zu entdecken und flexible Angriffssysteme, die gegen verschiedenste Computersysteme eingesetzt werden können. Gefordert wurde daher die Entwicklung »eines Vorrats an neuen Waffen, darunter verschiedene, die auf verbesserten konventionellen Technologien der elektronischen Kriegführung basieren«. [13]

Genau dies wird auch bisher betrieben. Die bekannten Techniken der elektronischen Kriegführung, vor allem Störsender und Täuschkörper, werden ausgebaut und für die Computerkriegführung aufgerüstet. Dabei wird eine Vielzahl von Möglichkeiten ausprobiert. Allein das beim Air Force Information Warfare Center (AFIWC) in San Antonio angesiedelte Information Warfare Battlelab etwa hat seit seiner Gründung 1997 mehr als 270 Konzepte untersucht und prüft derzeit 37 von ihnen genauer.

Im »Army Science and Technology Master Plan« von 1997, dem letzten, der öffentlich zugänglich ist, findet man weitere Hinweise auf die geplanten Cyber-Angriffstechnologien. Unter den Projekttiteln III.F.07, III.F.09 und III.F.10p finden sich dort die geheimen Vorhaben für »elektronische Attacken auf digitale Kommunikation«, »Informationskriegsattacken und -schütz« und »Informationskrieg«. Seit Ende 1997 liegen laut diesem Plan bereits Prototypen vor, mit denen Angriffe auf die gängigen kommerziellen Netze durchgeführt werden können, und seit 1999 sollte die Army in der Lage sein, weitere kommerzielle Netzwerke zu unterbrechen. Bis 2002 will man in der Lage sein, ausgewählte Bereiche der Informationssysteme eines beliebigen Gegners lahm zu legen oder zu stören, und bis 2003 soll seine gezielte Beeinflussung durch elektronische Täuschungsmanöver und Datenmanipulationen möglich sein. Erst ab 2004 werden Technologien erwartet, die Informationssysteme elektronisch zerstören können. [14] Laut dem »Joint Warfighter Science and Technology Plan« sollen dann auch Systeme für die »integrierte offensive Informationskriegführung« bereitstehen.

Dies sieht sehr langsam aus, wenn man die vollmundigen Infowar-Reden, Artikel, Bücher und Strategiepapiere betrachtet, die nun seit zehn Jahren verfasst werden. Brigadegeneral John B. Baker, damals Direktor der Air Intelligence Agency und Chef des Joint Information Operations Center, sagte noch 1999: »Wenn es darum geht, jenseits des reinen Abhörens von Datenübertragungen die > Nullen und Einsen< wirklich zu manipulieren und auszunutzen, haben wir noch einen weiten Weg vor uns.« Man darf aber nicht vergessen, dass es sich gerade bei den Angriffen auf Datennetze um eine vollständig neue Waffengattung handelt und auch andere Rüstungsprojekte sich teilweise 15 Jahre und länger hinziehen. Ein ständiges Problem, das hier viel schärfer wirkt als bei anderen Waffenprojekten, ist allerdings die rasante Weiterentwicklung der Informationstechnologien gerade im zivilen Bereich. Einmal entwickelte Informationskriegssysteme können daher nur sehr kurz verwendet werden, bevor sie durch neue Schutzvorkehrungen und Upgrades bei den »Angriffszielen« wieder obsolet sind. Als weiteres Problem könnte auf die Cyberkrieger zukommen, dass ihre Techniken

nur begrenzt eingesetzt werden können: Wer einmal angegriffen wurde, kann seine Erfahrungen auswerten und mit etwas Fachkenntnis eine zweite Attacke abwehren.

Viele der Cyberkriegswaffen werden im Rahmen der lange geplanten Modernisierung bestehender Systeme zur elektronischen Kriegführung entwickelt. Kernstück des elektronischen Arsenals der Air Force ist eine modifizierte Version von Lockheeds Transportflugzeug C-130 »Hercules«. Die Spezialversion EC-130H mit der Bezeichnung »Compass Call« verfügt über einen mit Elektronik voll gestopften Laderaum und diverse Antennen, mit denen die Funkverbindungen der gegnerischen Truppen abgehört, ausgewertet und gezielt gestört werden können. Nomalerweise wird es gebraucht, um die integrierten Luftverteidigungssysteme zu stören und so den Weg frei zu machen für die Bomber der Air Force. Sein Herzstück ist eine alternde Empfangs- und Sendeeinheit mit drei Modulen für UHF-Frequenzen, einem für VHF, einem KY-58-Satellitensystem und zwei KY-75 HF-Modulen. [15]

Für die systematische Anwendung auch gegen technologisch hochgerüstetere Gegner oder gegen kommerzielle Datenverbindungen reicht das System, das ursprünglich für analoge Signale entwickelt wurde, aber nicht aus. Die weitere Entwicklung soll zweigleisig verlaufen: Einerseits wird in dem für 2007 geplanten »Common Sensor «-Flugzeug die Fähigkeit eingebaut, gegen digitale Signale systematisch vorzugehen und so aus der Luft wirkliche Cyberkriege führen zu können. Die Projekte »Information Warfare« und »Digital Communications Electronic Attack« aus dem »Science and Technology Master Plan« der Army werden unter anderem dafür ausgerichtet. Darüber hinaus sollen für die elektronische und digitale Kriegführung verstärkt unbemannte Flugkörper (»Drohnen«) verwendet werden, die Signale der anzugreifenden Systeme auffangen, automatisch auswerten und stören können. Sie werden von der »Compass Call« der Air Force oder vergleichbaren Flugzeugen der Army wie der RC-7 »Airborne Reconnaissance Low (ARL)«, der RC-135V/W » Rivet Joint« oder der RC-12 »Guardrail« gesteuert, deren Aufgabe später die 40 neuen »Common Sensor«-Systeme übernehmen soll. Die Air Force modernisiert dazu gerade ihre Aufklärungsdrohne »Global Hawk«, die Army entwickelt zum selben Zweck das »Tactical Unmanned Aerial Vehicie« (TUAV). Ein weiteres Modul für die elektronische Kriegführung soll eine kompakte Bodenstation zum Abhören und elektronischen Stören und Verfälschen gegnerischer Signale sein, die mit den flugzeuggestützten Systemen zusammenarbeiten und diese koordinieren kann. Sie wird auf einem Geländewagen mit Anhänger unterkommen und bequem in den Laderaum eines Transportflugzeugs passen. [16]

Manche der defensiven Systeme zum Schutz eigener Computer können auch offensiv verwendet werden. Das Air Force Information Warfare Center hat ein Programm, entwickelt, mit dem man verdächtigen Eindringlingen einen »Stempel« verpassen kann - damit wären die üblichen Tarnungstechniken wie ständiger Wechsel von Usernamen und Passwort unwirksam. Weil man die elektronische Spur des Hackers dann bis zu seinem Computer zurückverfolgen kann, muss man allerdings selber unter Umständen in fremde Netze eindringen. Dann einen Virus einzuschleusen oder Daten zu manipulieren, soll ebenfalls möglich sein.

Erste Einsätze

Schon seit Mitte der 1980er Jahre setzten die USA Hacker gegen die Computernetze des damaligen Warschauer Pakts ein. Mitarbeiter von CIA und NSA verzeichneten nach

eigenen Angaben »beachtliche Erfolge dabei, geheime militärische Computersysteme in der Sowjetunion und anderen Ländern zu penetrieren«. Dies diente allerdings überwiegend der Spionage. Die technologischen Anstrengungen konzentrierten sich damals noch auf die elektronische Kriegführung gegen Raketen und Kampfflugzeuge. Zum ersten Mal bei einer militärischen Operation eingesetzt wurden Computereinbrüche im Rahmen von »Uphold Democracy« in Haiti 1994, als die USA den gestürzten Präsidenten Bertrand Aristide wieder an die Macht brachten. Die Maßnahmen waren damals von Präsident Clinton persönlich genehmigt worden. Seitdem wurden im Rahmen von weiteren UN-Missionen einige »relativ unbedeutende« Computer angriffe durchgeführt, wie Angehörige der US-Streitkräfte der Washington Post erzählten. Viele davon dienten vor allem der Überwachung gegnerischer Datenflüsse. In vielen anderen Fällen wurden von der Pentagon-Abteilung für »Special Technical Operations« Vorschläge für den Verteidigungsminister und den Präsidenten entwickelt. Der Genehmigungsprozess dauerte aber so lange, dass sie nicht mehr umgesetzt werden konnten. [17]

Der Krieg der NATO gegen Serbien um das Kosovo 1999 gilt vielfach als der erste richtige Cyberkrieg. Diesen Namen hat er vor allem wegen der starken Beteiligung der Hacker-Szene auf beiden Seiten an der psychologischen und politischen Auseinandersetzung im Internet bekommen. Vielfach wurden Webseiten gecrackt und mit Stellungnahmen für oder gegen den Krieg versehen, nach der Bombardierung der chinesischen Botschaft in Belgrad beteiligten sich auch Computerfreaks aus der Volksrepublik an den virtuellen Auseinandersetzungen. Darüber hinaus wurden vor allem gegen die NATO Denial-of-Service-Attacken durchgeführt und der Mailserver mit virenverseuchten E-Mails bombardiert. Dies sollte jedoch eher als elektronische Form der politischen Randale bezeichnet werden als mit dem Wort »Krieg«. Weniger bekannt ist, dass die USA die serbischen Luftabwehrsysteme elektronisch angriffen und sie nicht nur störten, sondern auch gezielt manipulierten. Dazu wurden von der EC-130H »Compass Call« hochfrequente Mikrowellen-Übertragungen abgehört, modifiziert und mit einem stärkeren Sender wieder ausgestrahlt. Am Ende sahen die Operateure der Abwehrstellungen Ziele auf ihren Monitoren, die gar nicht existierten. Darüber hinaus wurde das serbische Telefonsystem angegriffen, um die Kommandeure in Belgrad zu zwingen, mit ihren Truppen im Kosovo mittels Mobiltelefonen zu kommunizieren. Diese sind leichter abzuhören, da man nicht direkt an die Verbindungskabel heran muss.

Im Kosovokrieg zeigten sich auch die Probleme, die das US-Militär immer noch mit der Cyberkriegführung hat: Die streng geheime Operation war vom Joint Information Warfare Center in Zusammenarbeit mit den Kommandeuren in Europa bereits vorbereitet worden, als sich die Ereignisse auf dem Balkan erst zuzuspitzen begannen. Politische Bedenken verhinderten aber einen Einsatz bei Kriegsbeginn am 24. März, und die Genehmigung aus Washington kam erst eine Weile später. Als die Cyberkrieger dann alle Informationen zusammen und die Systeme einsatzbereit hatten, war durch die Bombardierung bereits so viel am Boden zerstört worden, dass es schwer war abzuschätzen, welchen Einfluss die Cyberattacken wirklich hatten. Anschließende Auswertungen kamen zu dem Ergebnis, dass man mehr hätte erreichen können, wenn die Cyberwaffen systematischer genutzt worden wären. Von Insidern aus dem Pentagon wird geschätzt, dass vielleicht zehn Prozent der Möglichkeiten ausgeschöpft wurden. [18] In einem internen Entwurf für ein Briefing der Navy, der an die Presse durchsickerte, wurde sogar behauptet, dass der Krieg nur halb so lange hätte dauern müssen, wenn die Informationsangriffe besser und umfangreicher ausgeführt worden wären.

Dass es beim Informationskrieg nicht nur um Angriffe auf die militärischen Datennetze geht, zeigte eine Meldung von Newsweek im Mai 1999. Angeblich habe Bill Clinton die CIA ermächtigt, im Rahmen einer »special technical Operation« elektronisch in Banken in Russland, Zypern und Griechenland einzubrechen, um die Auslandskonten des jugoslawischen Präsidenten Milosevic zu leeren. Im Gegensatz zu den bisher genannten Aktionen, die sich direkt gegen die Streitkräfte einer Kriegspartei richteten, wären in diesem Fall die zivilen Systeme von unbeteiligten Staaten unter Beschuss der USA geraten. Sogar der NATO-Partner Griechenland hätte sich damit virtuellem »friendly fire« ausgesetzt gesehen. Nicht einmal die NATO-Verbündeten waren in die Pläne eingeweiht. [19] Später stellte sich zwar heraus, dass diese Aktion offenbar von den Juristen der US-Regierung gestoppt worden war, aber nach einem Bericht von United Press International sollen die USA inzwischen in die versteckten Konten des aktuellen Lieblingsfeindes Osama Bin Laden eingebrochen sein. Nachdem es den Geheimdiensten gelungen sei, das finanzielle Netzwerk des islamistischen Millionärs zu durchschauen, könnten nun die Hacker der USA in die Konten eindringen und das Geld löschen oder abfließen lassen. »Drei Tastenklicks, und es ist weg«, sagte ein US-Beamter gegenüber UPI. [20] Ob an dieser Geschichte wirklich etwas dran ist, darf bezweifelt werden, denn es bestehen enge Verbindungen zwischen UPI und der zwielichtigen Sicherheitsfirma iDefense, einem Subunternehmen von NSA und Pentagon. James Adams, ehemaliger UPI-Chef und heute Direktor von iDefense, ist schon mehrfach durch Falschmeldungen aufgefallen. Laut Aussagen des Chaos Computer Clubs ist es allerdings technisch möglich, über das internationale Bankensystem Swift Überweisungen zu fälschen. Geheimdienste wie die NSA seien dazu in der Lage.

Immerhin macht die Story auf eine reale Gefahr aufmerksam: Cyberangriffe können nicht mehr wie normale Kriege von Öffentlichkeit und Parlament überwacht werden, und zivile Ziele sind in den einschlägigen US-Doktrinen für den Informationskrieg durchaus vorgesehen. Mitglieder der Geheimdienstausschüsse von Senat und Repräsentantenhaus in den USA, die in einer geheimen Sitzung über die virtuellen Banküberfälle der CIA gegen Milosevic informiert worden waren, äußerten sich ebenfalls besorgt. Eine solche Aktion gegen ausländische Banken würde nicht nur gegen mehrere internationale Verträge verstoßen, sie könne auch die führende Rolle der USA im weitweiten Bankgeschäft untergraben. Außerdem sei dieser Bruch der Souveränität sogar von verbündeten Staaten ein gefährlicher Präzedenzfall und lade zur Nachahmung, also zu Angriffen auf US-Banken, geradezu ein. Übrigens würden die USA einen Hacker, der Ähnliches bei einer New Yorker Bank versucht, als »Cyberterroristen« bezeichnen.

Akzeptanz- und Personalprobleme

Jenseits solcher spektakulärer Einzelaktionen geht die Integration der Cyberkriegspläne in normale Militäreinsätze nur langsam voran. Das erwähnte Kosovo-Briefing der Navy war interessant, weil es die Ursachen dafür nannte. Der Autor bezeichnete das Personal der »Information Operations Gell« als »großartige Leute«, aber ergänzte: »Sie hatten zu niedrige Dienstgrade und kamen aus dem falschen Umfeld, als dass sie den nötigen Einfluss auf Planung und Durchführung [des Einsatzes] hätten haben können.« [21] Für viele Kommandeure sind die hauseigenen Hacker immer noch eine suspekte Gruppe, die mit den herkömmlichen physischen Belastungen der Kriegführung wenig anfangen kann. Eine Kriegführung per Mausklick oder durch Flugzeuge ohne Piloten und reale Waffen ist für

das von Heldenverehrung, körperlicher Disziplin und Einsatz des eigenen Lebens geprägte Militär noch immer eine ungewohnte, wenn nicht sogar unerfreuliche Angelegenheit. Die Herkunft der Cyberkriegführung aus den geheimen Apparaten der Aufklärungseinheiten trägt ebenfalls nicht dazu bei, dass die Informationswaffen als ein »weiterer Pfeil im Köcher« angesehen werden, wie es General Richard Myers, der bis Februar 2000 die Abteilung für Computerkriegführung am Space Command geleitet hatte, gerne formuliert. Oft stünden die Angriffspläne mit konventionellen Waffen bereits fest, wenn jemandem einfällt, dass die Geeks für Informationsangriffe ja auch noch gefragt werden könnten, so beklagen sich viele der mit Cyberkrieg befassten Militärs. Ein großer Teil der Arbeit des Air Force Information Warfare Center besteht daher momentan darin, innerhalb der Truppe für sein Know-how und seine Technologien zu werben.

Bislang fehlen auch immer noch klare Einsatzrichtlinien für Cyberangriffe. Da diese unter den weiten und bis heute unscharf definierten Bereich der »Informationsoperationen« fallen, tun sich die Planer des Pentagon sehr schwer damit, die Bedingungen und Verfahrensregeln für solche Einsätze festzulegen. Jedes Szenario, das eventuell einmal den Einsatz von Cyberwaffen erfordern könnte, muss einzeln entwickelt und genehmigt werden. Zur Zeit beschäftigen sich die Juristen der US-Streitkräfte damit, ob und unter welchen Umständen das Völkerrecht Derartiges überhaupt zulässt. Daneben wird an einer umfassenden Militärstrategie für den Informationskrieg gearbeitet, dem OPLAN 3600. Einen Termin für seine Fertigstellung gibt es aber noch nicht. [22]

Ein drängendes Problem ist auch die Personalknappheit. Dem Pentagon fehlen an allen Ecken und Enden die Computerexperten, die in der privaten Wirtschaft um ein Vielfaches lukrativere Jobs finden. Einige nehmen zwar auch den umgekehrten Weg, weil sie geregeltere Arbeitszeiten als im Silicon Valley schätzen oder der Versuchung erliegen, ohne Strafandrohung in fremde Rechner einbrechen zu dürfen. Dies reicht aber bei weitem nicht aus, den Bedarf zu decken. Teilweise verlassen frustrierte Softwareentwickler auch die Streitkräfte, weil ihre Ideen im zähen Apparat auf Granit stoßen. Ein Beispiel ist die heute zum Netzwerkgiganten Cisco Systems gehörende Wheel Group. Gegründet wurde sie von hoch qualifizierten Computerexperten des Air Force Information Warfare Center (AFIWC), die 1998 auch die Untersuchung nach den britischen Hackereinbrüchen in die Air Force Rome Laboratories und das Air Force Material Command geleitet hatten. Sie hatten damals einen Netsniffer namens »NetRanger« entwickelt. Dieser gefiel dem AFIWC nicht, weil dort ein anderes Produkt als das Richtige galt, und so verließen die Computerfreaks die Air Force und gründeten eine eigene Firma. Der dann kommerziell vermarktete NetRanger wurde später sogar von der 609th Information Warfare Squadron verwendet.

Um die dünne Personaldecke im IT-Bereich etwas aufzustocken, hat das Pentagon im Dezember 2000 begonnen, Reservisten mit Computerexpertise einzuberufen. Die insgesamt fünf geplanten Teams, so genannte »Joint Reserve Information Operations and Information Assurance Organizations«, sollen unter anderem bei der Sicherung der eigenen Netze, bei Abhörangelegenheiten, aber auch für Computerattacken eingesetzt werden. Bis 2007 sollen sechshundert Mann aufgestellt werden, die sogar per Telearbeit für die NSA oder das Joint Information Operations Center arbeiten dürfen.

Um kurzfristige Engpässe zu umgehen, war das Pentagon gezwungen, verstärkt private Firmen zu beauftragen. Dies wiederum treibt aber die Kosten in die Höhe. In der Grauzone zwischen Netzwerksicherheit, Risikostudien, Analysen und Computerattacken tummeln sich ohnehin viele Unternehmen, die de facto Cyber-Söldner für die Hackerkriege der USA stellen. Die Firma Sytex Inc. hilft zum Beispiel der Land Information Warfare Activity der

Army bei der »Analyse, Aufbereitung und Verteilung von informationskriegsrelevanten Daten« - im Klartext heißt das: Mitarbeit bei der Zielauswahl für Angriffe. Sytex war bereits in Bosnien dabei und hat aufgrund der wachsenden Nachfrage gerade ein Information Warfare Center of Excellence gegründet. Auch andere Firmen wie SAIC oder Veridian sind in diesem Bereich tätig. Veridian hat im Juli 1999 einen Auftrag über 38 Millionen Dollar erhalten, um der Infowar-Abteilung des Naval Air Warfare Center ein Komplettpaket für die Planung und Durchführung von Informationskriegen zu liefern. Die Syracuse Research Corporation bietet Schulungen in Informationsoperationen an, bei denen auch »Hacking« auf dem Programm steht. Neben verschiedenen Cyberkriegseinheiten der US-Streitkräfte gehören auch die CIA, die kanadischen Streitkräfte und Rüstungskonzerne wie Lockheed Martin zu den Kunden.

Ein neuer Rüstungswettlauf?

Innerhalb von zehn Jahren ist aus einer zunächst skeptisch aufgenommenen Expertendiskussion an den Militärakademien eine neue Waffengattung entstanden. Dies gilt es festzuhalten, wenn man über die politischen Folgen und Probleme der amerikanischen Cyberkriegspläne nachdenken will. Trotz einer noch immer sehr schwammigen Definition dessen, was ein »Informationskrieg« eigentlich ist, trotz unklarer Einsatzregeln und juristischer Probleme, trotz technischer Schwierigkeiten und mangelnder Akzeptanz in der Truppe: Der Cyberkrieg beginnt zu reifen. Er hat sich im Apparat festgesetzt mit eigenen Einheiten, Planungszellen, einer Militärdoktrin und einer kaum noch zu überblickenden theoretischen Literatur. Viele der noch offenen Fragen werden derzeit in der Militärbürokratie und in den Forschungslabors von Streitkräften und Rüstungsindustrie bearbeitet, und man muss davon ausgehen, dass sie in spätestens fünf Jahren zum großen Teil gelöst sind. Dies wirft die Frage nach einer politischen Kontrolle der bislang vor allem technologisch und militärstrategisch betriebenen Entwicklung auf. Wenn die Cyberkrieger der USA unentdeckt und unter Ausschluss von Parlament und Öffentlichkeit in beliebige Datennetze der Welt eindringen können, wenn dabei kommerzielle Netze ebenso als Angriffsziele gelten wie von Computern gesteuerte Infrastrukturen industrialisierter Gesellschaften, wenn zur Terroristenjagd internationale Banken geknackt werden, wenn dazu noch Überwachungstechniken verbessert und sogar Hintertüren in amerikanische Computerprodukte eingebaut werden, dann werden Datenschützer ebenso nervös wie Völkerrechtler oder ganze Wirtschaftszweige.

Dazu kommt die internationale Vorbildfunktion der USA. Viele Staaten haben die amerikanische Entwicklung aufmerksam verfolgt und beginnen nun, eigene Pläne für den Cyberkrieg zu schmieden. Als erste Kandidaten gelten China, Indien, Pakistan und Israel, einige europäische Staaten - darunter auch Deutschland - hocken in den Startlöchern. Mittlerweile warnen daher die Direktoren der US-Geheimdienste bei Kongressanhörungen vor dem »Volksinformationskrieg« aus China und fordern weitere Aufrüstungsanstrengungen der USA auf diesem Gebiet. Dem sicherheitspolitisch geschulten Beobachter zeigen sich darin die ersten Stufen eines klassischen Wettrüstens. Die Cyberkriegs-Vordenker wie John Arquilla oder Dan Kuehl machen sich daher bereits Sorgen, ob sie die von ihnen angestoßene Entwicklung noch kontrollieren können.

Auf großes Interesse stoßen daher in der akademischen Diskussion zur Zeit erste Ideen zur Cyber-Rüstungskontrolle, wie sie unter anderem von der deutsch-österreichischen Forschungsgruppe Informationsgesellschaft und Sicherheitspolitik (FoG:IS) oder vom

Information Assurance Advisory Council (IAAC) am Londoner King's College entwickelt worden sind. Erste Schritte zur Friedenssicherung im Cyberspace wären zum Beispiel ein »no first use«-Abkommen und der erklärte Verzicht auf Angriffe gegen zivile Ziele. Als mittelfristiges Ziel wird eine internationale Konvention zur friedlichen Nutzung des Cyberspace angestrebt. Die Zeit drängt. Im Februar 2001 wurde die Air Intelligence Agency, an der die meisten der mehreren tausend US-Cyberkrieger ihren Dienst tun, dem Air Combat Command unterstellt. Damit ist sie nun Teil der kämpfenden Truppe, und der erste Großeinsatz ihrer unsichtbaren Waffen rückt immer näher. Die Bundesregierung konnte hier ihr Koalitionsversprechen »rot-grüne Außenpolitik ist Friedenspolitik« auf zukunftsträchtige Art und Weise einlösen, indem sie die in der Friedensforschung, aber auch in der UN-Generalversammlung begonnenen Bemühungen zur Begrenzung eines elektronischen Wettrüstens unterstützt. Warum sollte hier nicht funktionieren, was bei der Freigabe von Kryptografie oder der Förderung von Open-Source-Software bereits geschehen ist - dass man in Deutschland weiter, aber vor allem ziviler denkt als in der Militärmacht USA?

Literatur

[1] Wichtige Schlüsseltexte der Debatte finden sich in John Arquilla / David Ronfeldt (Hrsg.), In Arhena's Camp. Preparing for Conflict in the Information Age, Santa Monica 1997

[2] Joint Chiefs of Staff, Joint Pub 3-13.1, Joint Doctrine for Command and Control Warfare, Washington, B.C., 7. 2. 1996

[3] Ralf Bendrath, Elektronisches Pearl Harbor oder Computerkriminalität? Die Reformulierung der Sicherheitspolitik in Zeiten globaler Datennetze, in: S+F, Vierteljahresschrift für Sicherheit und Frieden, Nr. 2/2000, S. 135-144

[4] Joint Chiefs of Staff, Joint Pub 3-13, Joint Doctrine for Information Operations, Washington, D.C., 9. 10. 1998

[5] Joint Chiefs of Staff, Joint Pub 3-51, Joint Doctrine for Electronic Warfare, Washington, D.C., 7, 4. 2000

[6] USAF Intelligence Targeting Guide, Air Force Pamphlet 14-210, Intelligence, Washington, D.C., 1. 2. 1998, Kapitel 11: Targeting in ehe Information Age, S. 88

[7] David A. Fulghum / Rober Wall: Cyber-Arsenal Needs Testing, in: Aviation Week & Space Technology, 26. 2. 2001

[8] John L. Woodward, Jr., Department of Defense Director for Command, Control, Communications and Computer Systems, Information Assurance through Defense in Depth, Washington, D.C., Februar 2000, S. 5

[9] Vgl. die laufende Berichterstattung in telepolis, http://www.heise.de/tp/deutsch/special/ech/default.htrnl

[10] William Clinton, Defending America's Cyberspace. National Plan for Information Systems Protection Version 1.0. An Invitation to a Dialogue, Washington, D.C., 7. 1. 2000, S, 49

[11] William M. Arkin: A Mouse That Roars?, washingtonpost.com, 7. 7. 1999

[12] David A. Fulghum / Robert Wall, Information Warfare Isn't What You Think, in: Aviation Week St Space Technology, 26. 2. 2001

[13] Office of Secretary of Defense, Joint Warfighter Science and Technology Plan, Washington, D.C., 1997, Kapitel IV.1 »Information Warfare«

[14] Department of the Army, Army Science and Technology Master Plan, Washington, D.C., 1997, Annex A: Science And Technology Objectives (STOs), Kapitel III.F.
[15] David A. Fulghum, Compass Call To Dominate Electronic, Info Warfare, in: Aviation Week & Space Technology; 18. 10. 1999
[16] David A. Fulghum, Army Hackers Go Airborne, in: Aviation Week & Space Technology, 18. 10. 1999
[17] William M. Arkin, The Cyber Bomb in Yugoslavia, washingtonpost.com, 25. 10.1999
[18] Lisa Hoffman, Special Report: U.S. opened cyber-war during Kosovo fight, in: Washington Times, 25. 10. 1999
[19] Gregory L. Vistica, Cyberwar and Sabotage, in: Newsweek, 31. 5. 1999, S. 22
[20] U.S. Makes Cyberwar on Bin Laden, United Press International, 9. 2. 2001
[21] Bob Brewin, Kosovo ushered in cyberwar, in: Federal Computer Week, 27. 9. 1999
[22] Ellen Messmer, U.S. Army kick-starts cyberwar machine, in: Network World, 20.11.2000

Ralf Bendrath, Dipl.Pol., promoviert an der Freien Universität Berlin zum Thema »Das Militär in der Informationsgesellschaft«. Daneben ist er Geschäftsführer der Forschungsgruppe Informationsgesellschaft und Sicherheitspolitik (FoG:IS), betreibt die Mailingliste Infowar.de und schreibt regelmäßig in telepolis zu diesem und anderen Themen. Weitere Informationen und Texte zum Thema gibt es unter http://userpage.fu-berlin.de/~bendrath.

Datenschutzwerkzeuge für anonyme und verschlüsselte Kommunikation sichern wertvolle Freiräume in einer zunehmend kontrollierten Informationslandschaft

Digitale Freihäfen

Christiane Schulzki-Haddouti

Im Privatleben ist die Trennung zwischen Öffentlichkeit und Privatheit recht einfach zu regeln: Hinter der Wohnungstür ist alles privat - davor ist man sich der Öffentlichkeit bewusst. Die Informationstechniken durchdringen die Wohnungstür jedoch mühelos - und nur die wenigsten Nutzer sind sich dessen bewusst. Der Angriff auf die Privatsphäre kann von unterschiedlichsten Seiten und mit unterschiedlichsten Motiven erfolgen: Kommerzielle Interessen, Strafverfolger und Geheimdienste, repressive politische Systeme, sie alle haben ein Interesse am Kommunikationsverhalten von Personen, Organisationen und Firmen. Obwohl man eigentlich annehmen sollte, dass zumindest in demokratischen Ländern auch die Regierungen ein Interesse daran haben, dass ihre Bürger elektronische Kommunikation frei und sicher nutzen können, wurde die Entwicklung entsprechender Tools durch die Debatte um Kryptopolitik um Jahre zurückgeworfen. Zugleich werden Polizei und Nachrichtendienste immer wieder mit Wunschlisten bei Gesetzgebern vorstellig, wonach jede Kommunikation im Prinzip abhörbar und Anonymität fast schon einem Verbrechen gleichgestellt werden soll. Mit den immer gleichen Argumenten - Kinderpornografie, politischer Extremismus und organisiertes Verbrechen - wird versucht, die Verbreitung von Tools, die eine sichere Kommunikation für jedermann ermöglichen, entweder zu verhindern oder gar illegal zu machen. Auf der anderen Seite arbeiten engagierte Individuen, akademische und kommerzielle Entwicklergruppen an Techniken, die als digitale Freihäfen dem Grundrecht auf private und unzensierte Kommunikation zum Durchbruch verhelfen sollen.

Die Datenschutzwerkzeuge arbeiten grundsätzlich nach zwei Prinzipien: Die Daten werden verschlüsselt - und sie werden so verteilt, dass eine zentrale Kontrolle unmöglich wird. Einen Generalversiegler gibt es nicht - aber je nach Bedarf sind verschiedene Werkzeuge auf dem Markt: Um E-Mails unter vier Augen lesen zu können helfen Verschlüsselungsprogramme wie Pretty Good Privacy, um sie unerkannt verschicken zu können stehen Remailer zur Verfügung. Anonymes Surfen ist auch ein Wunsch vieler Nutzer - angesichts von Cookie-Attacken und Webkäfern, die persönliche Daten ausspähen können. Andere Tools hingegen sollen Zensurversuche der verschiedensten Art umgehen helfen. Die meisten vorhandenen Tools stecken noch in den Kinderschuhen, sind entweder kompliziert zu verwenden oder garantieren nicht ausreichende Sicherheit. Doch enthusiastische Communities arbeiten mit Vehemenz an der Weiterentwicklung von Datenschutzwerkzeugen, von denen einige der wichtigsten hier vorgestellt werden.

Pretty Good Privacy

Alles was Nutzer lieber nicht per Postkarte mitteilen, sondern im Umschlag verschicken möchten, sollten sie im Internet verschlüsseln. Denn die E-Mail läuft über viele Rechner, bevor sie beim Computer des Empfängers ankommt. Auf jedem dieser Rechner kann die Nachricht gelesen und auch verändert werden - ohne dass der Absender oder der Empfänger es merken.

Als Programm zum Ver- und Entschlüsseln bietet sich hier PGP an, das es für fast alle Rechner-Plattformen gibt und für private Nutzung kostenlos ist. Die Abkürzung steht für Pretty Good Privacy oder »ziemlich gute Privatsphäre«. Diese Verschlüsselungssoftware gilt seit Jahren als De-facto-Standard für sichere Kommunikation im Internet - und half, das US-Kryptoexportverbot zu durchbrechen: Ihr Code wurde per Buch exportiert - und in Europa mühsam wieder eingescannt. Denn der Buchexport war nicht verboten.

Noch immer soll es Polizei und Nachrichtendiensten nicht möglich sein, PGP-verschlüsselte E-Mails abzuhören - vorausgesetzt, der Nutzer wendet es sauber an. Der Angriff auf das Endgerät, was nur mit dem »Großen Lauschangriff« möglich wäre, kann allerdings zum Erfolg führen, denn auf der Festplatte des PC befindet sich der geheime Schlüssel. Die Fahnder müssen deshalb nur noch das geheime Passwort herausfinden.

Von PGP gibt es inzwischen viele Versionen. Kritische Experten empfehlen die spartanische Version von PGP 2.6.3. Es ist im Netz zusammen mit der grafischen Oberfläche wie dem Programm MailPGP (für Windows 95, 98, NT) kostenlos erhältlich. [1] Egal welche Version verwendet wird - in einem ersten Schritt wird automatisch das eigene Schlüsselpaar erzeugt. Später kann man in der Schlüsselverwaltung einen neuen Schlüssel erzeugen. Dabei muss man aussuchen, mit welchem kryptografischen Verfahren der Schlüssel erzeugt wird: mit RSA oder Diffie-Hellman/DSS. Nutzer der 2.6x-Versionen können nur RSA-Schlüssel verwenden. Nutzer neuerer Versionen wählen in der Regel Diffie-Hellman/DSS, da man hier längere und somit sicherere Schlüssel erzeugen kann. Man kann auch zwei Schlüsselpaare erzeugen: zum Beispiel ein RSA-Schlüsselpaar mit einer Länge von 2048 Bits und mit unbegrenzter Haltbarkeit und ein zweites, das nur für zwei Monate gültig ist. Dies erhöht die Sicherheit.

Dann wird die so genannte Passphrase beziehungsweise das geheime Passwort eingegeben. Am sichersten ist eine willkürliche Folge von Buchstaben und Zahlen. Minimum sind acht Zeichen, die man sich möglichst auch ohne Spickzettel gut merken kann. Diese Zeichen müssen nämlich später bei jedem Entschlüsseln eingegeben werden. Schließlich wird das Schlüsselpaar generiert. Auf langsamen Rechnern kann dies einige Minuten dauern.

Danach kann man den öffentlichen Schlüssel per Mausklick an einen der so genannten Key-Server im Internet schicken. Das sind Datenbanken, die eine große Zahl öffentlicher Schlüssel zum Abruf gespeichert haben. In der Regel tauschen diese Rechner untereinander die Schlüssel aus. Oder aber man exportiert den Schlüssel per Mausklick in eine Datei, die man sowohl einzelnen Briefpartnern schicken als auch der Allgemeinheit auf der eigenen Homepage zur Verfügung stellen kann.

Prinzipiell funktioniert das Verschlüsseln so, dass die Briefpartner jeweils ein Schlüsselpaar aus einem öffentlichen und einem geheimen Schlüssel besitzen. Mit dem öffentlichen Schlüssel des Empfängers kann man den abzuschickenden Text verschlüsseln. Der Empfänger kann diesen aber nur mit seinem geheimen Schlüssel wieder entziffern.

Verschlüsselt werden können sowohl ganze Dateien als auch nur einzelne Textabschnitte. Mit Hilfe der PGP-Werkzeuge lassen sich die entsprechenden Dateien auswählen. Das Entschlüsseln erfolgt ganz ähnlich.

Es gibt allerdings auch Programme, die die geheimen Schlüssel auf der Festplatte ausspähen können. So existiert zum Beispiel ein in Word-Dokumenten enthaltenes Makro-Programm, das diese Schlüssel dann auch noch per Internet zu verschicken versucht. Mit den Angriffsprogrammen »Back Orifice« oder »Netbus« lässt sich die Datei, in der der geheime Schlüssel abgelegt ist, ebenfalls leicht ausspähen, auch wenn sie verschlüsselt und durch eine Passphrase geschützt ist. Vor allem einfache Passwörter lassen sich nämlich durch automatisches Ausprobieren ziemlich leicht herausfinden.

Es ist daher empfehlenswert, die Datei mit den geheimen Schlüsseln, die »secring.pgp«, nicht auf der Festplatte, sondern auf einer Diskette zu speichern. Noch sicherer wäre es, die geheimen Schlüssel auf Chipkarte oder auf einem sicheren mobilen Gadget zu speichern.

Remailer

Mix-Rechner, die ausschließlich E-Mails anonymisieren, heißen Remailer. Über einen Remailer kann man beispielsweise Nachrichten anonym in eine Usenet-Newsgruppe posten oder jemandem eine E-Mail schicken, ohne dass dem Empfänger Namen oder E-Mail-Adresse des Absenders bekannt sind. Lutz Donnerhacke betrieb noch bis vor kurzem in Jena einen anonymen Remailer, [2] den er jedoch wegen der hohen Arbeitsbelastung deaktivierte.

Pseudoanonyme Remailer sind im Netz inzwischen kaum noch verfügbar. Sie anonymisierten Nachrichten, indem sie einfach den Namen und die Adresse des Absenders durch andere Daten ersetzten. Positiv daran war, dass über diese Remailer auch Rückantworten erfolgreich ankamen. Negativ war, dass bei diesen Remailern Name und Pseudonym zentral zusammenliefen. 1996 erzwang Scientology per Gerichtsbeschluss die Beschlagnahmung der Protokolldaten des finnischen Remailers Penet. Angeblich hatte ein Penet-Nutzer eine aus Sicht von Scientology negative Äußerung über die Organisation über den Remailer anonymisiert ins Usenet verschickt. Auf diese Weise hatte die Polizei aber auch die Identität der 700.000 anderen Penet-Nutzer ermittelt. Der Betreiber, Johan Helsingius, schloss daraufhin seinen Dienst.

Für wirklich anonyme Remailer gibt es heute zwei technische Konzepte: Die »Cypherpunk«-Remailer benutzen PGP, der Mixmaster-Remailer von Lance Cottrell benutzt ein speziell für die Anonymisierung entwickeltes Datenformat. Die Mail-Inhalte werden mit Triple-DES chiffriert. Der Paket-Header sowie die Triple-DES-Schlüssel werden mit dem RSA-Algorithmus verschlüsselt.

Inzwischen gibt es für den anonymen Mailversand E-Mail-Clients oder Mixmaster-Frontends. Mit beiden Technologien arbeiten »Private Idaho« [3] und »Jack B. Nymble« [4] auf Windows-Betriebssystemen. Beide setzen voraus, dass der Nutzer PGP installiert hat. Aber auch im World Wide Web gibt es einige Homepages, Über die man direkt mit Hilfe von Cypherpunk oder Mixmaster Mails verschicken kann. So zum Beispiel das Remailer-Projekt Orange [5]. Positiv ist hier, dass der Nutzer selbst festlegen kann, über welche Remailer seine E-Mail verschickt werden soll. Damit kann er auch abschätzen, wie lange die E-Mail braucht, um zum Empfänger zu gelangen.

Safeweb

Die Netzsoftware Safeweb [6] verschlüsselt komplett den ganzen Web-Verkehr und schützt so den persönlichen Internetverkehr. Der britische Datenschutz-Guru Simon Davies zeigte sich angesichts von Safeweb enthusiastisch: »Diese Art von kostenloser Software wird wie auch Hushmail oder das Freedom-Netzwerk die Bemühungen der Regierung zunichte machen.« Allerdings läuft der Verkehr nur über den Rechner von Safeweb. Experten kritisieren, dass damit ein einziges Angriffsziel geboten ist,

Auch manche Regierungsbehörden können sich mit solchen Softwarewerkzeugen anfreunden. Vor allem Spione legten traditionellerweise schon immer höchsten Wert auf Anonymität: Im Herbst 2000 ging der Anonymisierdienst denn auch eine bemerkenswerte Allianz mit dem amerikanischen Geheimdienst CIA ein. Vor zwei Jahren startete die Behörde ihre eigene Venture-Kapital-Firma In-Q-Tel, um diese Art von Anonymisierungsdiensten zu untersuchen. Nun will die CIA Safeweb selbst benutzen, um die eigenen Bewegungen im Internet zu verschleiern.

Für viele Nutzer ist die Zusammenarbeit mit der CIA nicht unbedingt eine vertrauensbildende Maßnahme. Auch dem 34-jährigen Chef von Safeweb, Stephen Hsu, ist klar, »dass wir einen Rückschlag von fünf Prozent unserer paranoidesten Kunden hinnehmen müssen«. Der Beitrag von Safeweb bestünde jedoch nur darin, die Behörde mit einer angepassten Software zu versorgen. Die CIA selbst habe keinen Zugriff auf die Weh-Computer der Firma oder auf die Arbeitsweise der Software. Die bei Safeweb benutzte Technologie heißt Triangle Boy. Damit kann jeder PC in eine Art Web-Server verwandelt werden. Damit können Nutzer jede Website besuchen, ohne Spuren zu hinterlassen. Die Anfrage an die Zielwebsite wird an die Website von Safeweb weitergeleitet, die dann die Verbindung herstellt.

Die CIA könnte aber nicht nur ihre Surftouren im Internet verschleiern, sondern auch sichere Kommunikationsverbindungen für ihre Quellen herstellen, damit diese vertraulich mit dem CIA-Hauptquartier kommunizieren können. Die Safeweb-Technologie bietet sich auch an, um Informationen unentdeckt in andere Länder gelangen zu lassen. Genau diese Anwendungen hatte Stephen Hsu im Kopf, als er im letzten Jahr die CIA kontaktierte. Allerdings könnten nicht nur Propagandasendungen auf diese Weise verbreitet werden, sondern auch Cyber-Attacken gestartet werden, ohne dass der Ursprungsort erkannt werden könnte.

Man könnte nun darüber spekulieren, dass das wahre Interesse der CIA darin bestünde, Triangle Boy zu knacken und seinen Gebrauch in der Öffentlichkeit zu kompromittieren. Immerhin erschweren solche Techniken genauso wie kryptografische Methoden das eigentliche Geschäft der Geheimdienste: die elektronische Nachrichtenauswertung.

Allerdings könnte schon ein richterlicher Beschluss genügen, um Strafverfolgern Zugriff auf die Anonymisier-Rechner zu gewähren. Denn die Betreiber dieser Rechner können die Kommunikation sehr wohl einzelnen Nutzern zuordnen.

Anonymizer

Sehr bekannt ist der Anonymizer, der Safeweb sehr ähnlich ist. Über den einfachen Aufruf einer Webseite, in die der Nutzer eine Internetadresse eingibt, können anonym weitere Webseiten genutzt werden. Der Anonymizer arbeitet wie ein herkömmlicher Proxy-Rechner.

Doch er entfernt alle personenbezogenen Informationen wie Cookies oder IP-Adressen aus den Kopfzeilen [7] der Webanfragen.

Allerdings arbeitet der Anonymizer wie Safeweb nicht mit verschiedenen Rechnern. Es genügt also der Zugriff auf den Anonymizer-Rechner, um die Nutzer zurückverfolgen zu können. Eine technische Sicherheit gibt es nicht. Der Nutzer muss dem Betreiber des Anonymizer vertrauen, dass er keine Interessensdaten sammelt. Zudem könnte ein Angreifer die Kommunikation zwischen dem Anonymizer-Rechner und einem Nutzer abhören und auch Verkehrsanalysen machen. Auch dauern die Abrufe eine Weile länger als sonst - bei schnellen Internetverbindungen ist dies jedoch kaum noch zu spüren.

Crowds

Das Projekt wurde im Sommer 1997 erstmals vorgestellt. Bei Crowds geht es darum, Nutzerspuren im World Wide Web zu verstecken. Die Spuren eines Einzelnen sollen in den Spuren der Menge [8] untergehen: Der Nutzer mischt sich unter eine Nutzermenge. Seine Anfrage an einen Web-Server wird an ein zufälliges Mitglied der Menge weitergereicht. Dieses kann die Anfrage direkt an den Zielserver weiterreichen oder an ein weiteres, zufällig ausgewähltes Mitglied weitergeben. Wenn die Anfrage schließlich übermittelt wird, wird sie von einem zufällig ausgewählten Mitglied übermittelt. Der Server geht jedoch davon aus, es mit dem ursprünglich anfragenden Mitglied zu tun zu haben. Angeblich können sogar Mitglieder der Menge den Anfrager nicht identifizieren.

Experten kritisieren, dass ein Teilnehmer fälschlicherweise für den Absender einer Anfrage gehalten werden kann [9]. Andererseits kann dieser das natürlich immer mit gutem Grund abstreiten.

Mitlesen können Angreifer die Daten nicht, denn die Anfragen sind mit einem symmetrischen Kryptosystem verschlüsselt. Wenn der Angreifer Verkehrsanalysen durchführt, können die verschlüsselten Daten jedoch miteinander verkettet und beobachtet werden.

Sehr erfolgreich war das Projekt trotz sehr positiver Berichterstattung in der US-Presse nicht. Es wird nur selten genutzt. Bis Anfang 2000 verhinderten die US-Kryptoexportkontrollen [10], dass es in vollem Umfang in Europa genutzt wurde. Aber auch danach gab es Probleme, Crowds zu exportieren. Bis heute fand es wenig Unterstützung.

Bei Crowds werden die Anfragen über mehrere Rechner geschleust - und darin besteht seine Stärke. Damit greift Crowds das Erfolgsrezept des Internets auf: Noch vor wenigen Jahren hielten viele das Internet für unzensierbar. Schließlich war es dezentral organisiert worden, um die Kommunikation zwischen verschiedenen Punkten auch im Falle eines Atomkriegs aufrechterhalten zu können. Wenn jedoch die Kommunikation innerhalb eines Rechtssystems, also eines Staates, nur über einen zentralen Knoten läuft, lässt sie sich kontrollieren. Inzwischen gibt es mehrere Versuche, ein unzensierbares Netz zu erschaffen, in dem Dateien möglichst unkontrolliert ausgetauscht werden. Je dezentraler diese Systeme organisiert sind, desto resistenter sind sie gegenüber Manipulationsversuchen.

Napster

Die bekannteste Tauschbörse im Netz ist Napster. Es ermöglicht Nutzern, schnell und einfach Musikdateien über das Internet zu tauschen. Ob dabei urheberrechtlich geschützte Musikstücke betroffen sind, überprüfte das System vor der Übernahme durch Bertelsmann nicht. Das System wurde für »Fair Use« entworfen und verwendete keine Verschlüsselungsverfahren. Nachdem Bertelsmann nicht-lizenzierte, urheberrechtlich geschützte Songs blockierte, sank nach einer Untersuchung von Jupiter Media Metrix die Zahl der Anwender, die mit dem Napster-Client Songs tauschten, in den USA im März 2001 um gut 3 Millionen auf 12,1 Millionen. Im Februar waren es noch 15,2 Millionen individuelle US-Napster-Anwender.

Gnutella

Etwas schwieriger als Napster in den Griff zu bekommen ist Gnutella, da es dezentraler als Napster arbeitet. Bei Gnutella handelt es sich um eine Open-Source-Software zum Tauschen von Dateien. Das geschieht in einem Netzwerk aus Rechnern, die untereinander Suchanfragen austauschen. Startet der Nutzer eine Suchanfrage, wird diese an alle verbundenen Rechner weitergeleitet, Anfrage und Antwort laufen über mehrere Rechner und können nicht direkt einer bestimmten IP-Adresse zugeordnet werden. Die Antworten enthalten aber die IP-Adresse des Datei-Anbieters, der über den Provider ermittelbar ist. Anonymes Tauschen ist deshalb mit Gnutella nicht möglich. Für Gnutella gibt es verschiedene Anwendungsprogramme, so genannte Clients. Dazu gehören Gnotella oder Toadnode für Windows, Mactella für den Mac, MyGnut für BeOs, Hagelslag für Unix oder der Java-Client Furi.

Onion Routing

Onion Routing [11] ist nach Ansicht des überaus kritischen Dresdner Informatikprofessors Andreas Pfitzmann das derzeit einzige »akzeptable« funktionierende Konzept für anonymes Surfen. Es ist ebenfalls wie Napster und Gnutella für den Datentransfer, das Remote Login und andere verbindungsorientierte Dienste nutzbar. Bei Onion Routing können die Daten aber weitgehend anonym ausgetauscht werden.

Nicht nur ein einziger Rechner ist für die Anonymisierung zuständig. Die Kommunikation wird verschlüsselt. Verkehrsanalyse ist ebenfalls nur eingeschränkt möglich. Allerdings ist der Absender dem Empfänger bekannt. Insgesamt schützt Crowds gegen stärkere Angriffe als Anonymizer. Onion Routing bietet aber noch einen stärkeren Schutz als Crowds.

Das Forschungsprojekt wurde vom US-Verteidigungsministerium und der US-Forschungsschmiede DARPA [12] gesponsert. Der Prototyp bewies, dass das Konzept funktioniert. Pro Tag wurde das Netzwerk durchschnittlich mit 50.000 Hits in der Testphase fertig. Bis Anfang 2000 durfte die Software nicht aus den USA exportiert werden, da sie kryptografische Elemente beinhaltet. Seit dem 28. Januar 2000 ist der Prototyp offline und wartet auf weitere Einsätze. Ins Ausland soll er jedoch nicht exportiert werden - aufgrund seines militärischen Hintergrunds. Immerhin baute Ulf Möller an der Universität Hamburg einen Prototypen nach.

Beim Onion-Routing baut der Browser eine Verbindung zu einem ersten Onion-Routing-Proxy-Rechner auf. Dieser baut dann eine anonyme Route beziehungsweise Strecke durch verschiedene Onion-Router bis zum Zielserver auf. Dabei kennt ein Onion-Router nur die Strecke bis zum nächsten Rechner. Bevor die Daten auf die Reise geschickt werden, werden sie mehrfach verschlüsselt. Diese Verschlüsselung legt sich in Schichten um die Daten, wobei jede Schicht die Adresse des nächsten Onion-Routers trägt. Diese Schichten sind der Namensgeber für das Projekt, dessen Verschlüsselungskonzept einer Zwiebel [13] ähnelt.

Schutz vor Beobachtung bietet der so genannte Dummy Traffic oder Leerverkehr, der zwischen den Onion-Routern erzeugt wird. Wird der Dienst nur wenig benutzt, bietet das kaum Schutz. Denn dann können die Enden eines Kommunikationskanals allein über die ausgetauschte Datenmenge verkettet werden.

AN.ON

Richtig zufriedenstellend sind die bislang vorgestellten Möglichkeiten für anonymes Surfen nicht. Das Bundeswirtschaftsministerium fördert deshalb die Entwicklung des Anonymitätsdienstes. Das Projekt »AN.ON Anonymität im Internet« von der TU Dresden und dem unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein will einen Dienst entwickeln, dessen Basis auf vielen unabhängigen Netzknoten, so genannten Mix-Proxies, beruht, über die die Internetkommunikation verschlüsselt abläuft. Nicht nur Geheimdienste, selbst die Provider können so nicht herausfinden, wer was im Internet macht.

Jeder Nutzer kann selbst einen Mix-Proxy betreiben, wenn er über eine entsprechend breite Internetanbindung verfügt. Die im Projekt entwickelte Software soll künftig als Open-Source allen Nutzern offen gelegt und frei zugänglich gemacht werden, Das Bundeswirtschaftsministerium will vor allem, dass die bisherigen Hemmnisse für den E-Commerce abgebaut werden. Das Haupthindernis ist das fehlende Vertrauen der Verbraucher in das Netz.

Die Verbraucher sollen sich darauf verlassen können, dass sie beim Online-Shopping nicht automatisch eine breite Datenspur erzeugen. Kein Wunder: Die Zuwachsraten des Internethandels liegen weit hinter den Erwartungen der Wirtschaft. Ein entscheidender Punkt, so die Analysen von Marktforschungsunternehmen, liegt eben in den Sicherheitsbedenken der Verbraucher.

Hannes Federrath, Gastprofessor für Informatik an der Freien Universität Berlin, hat ein plastisches Beispiel zur Hand: »Stellen Sie sich vor, Sie suchen zufällig nach medizinischen Informationen im Netz, weil Freunde von Ihnen an einer schweren Krankheit leiden. Gleichzeitig informieren Sie sich auf der Website einer Lebensversicherung nach günstigen Tarifen. Beides ergibt ein Profil, das ausgewertet und an Interessenten verkauft wird. Vielleicht wird Ihnen dann nur ein ungünstiger Tarif angeboten.« [14]

Schon jetzt kostenlos verfügbar ist das Programm Java Anon Proxy (JAP) [15], das Federrath im Rahmen des Projekts AN.ON entwickelt hat. Wie eine virtuelle Tarnkappe arbeitet JAP: Es schickt die Kommunikationsverbindung nicht direkt an den Web-Server, sondern über eine so genannte Mix-Proxy-Kaskade. Dabei wird der Aufruf des JAP-Nutzers unter den Internetverbindungen der anderen JAP-Nutzer versteckt. Die Verbindung kann nicht mehr einem bestimmten Nutzer zugeordnet werden. Jeder Benutzer könnte der Urheber einer Verbindung gewesen sein. »Niemand, kein Außenstehender, kein anderer

Benutzer, nicht einmal der Betreiber des Anonymitätsdienstes kann herausbekommen, welche Verbindungen ein bestimmter Benutzer hat,« heißt es auf der Website.

In der Regel arbeiten in einer Kaskade mindestens drei Mix-Proxies, die von unabhängigen Institutionen betrieben werden. Sie erklären in einer Selbstverpflichtung, dass sie weder Log-Files über die transportierten Verbindungen speichern noch mit den anderen Mix-Proxy-Betreibern Daten austauschen, die dazu führen könnten, dass ein Benutzer enttarnt wird. Unabhängige Prüfstellen sollen garantieren, dass die Selbstverpflichtung tatsächlich eingehalten wird. Am idealsten wäre es, so Andreas Pfitzmann, wenn die Katholische Kirche einen Proxy, die PDS den nächsten, eine Universität den dritten und ein Kaufhaus den vierten Proxy betreiben würde - auch Proxies im Ausland würden zur weiteren Sicherheit beitragen. Denn den Nutzer kann man nur dann identifizieren, wenn alle Betreiber den Zugriff auf den Proxy erlauben.

Freenet

Noch radikaler als AN.ON ist Freenet [16]. Es etabliert ein paralleles Internet, das zensurresistent, anonym und effizient Informationen publizieren und abrufen lässt. Ziel ist die völlige Abschaffung von Urheberrechten und der freie Zugang zu allen Daten im Netz für jeden.

Derzeit arbeiten rund 400 Entwicklerinnen und Entwickler um den schottischen Studenten Ian Clarke [17] an dem Prototypen. In dem völlig dezentralen Netz darf es keine zentralen Kontrollpunkte mehr geben. Einfach ist dies nicht. Clarke und seine Entwickler haben mit Problemen der Skalierbarkeit, der Effizienz und der Netzlastverteilung zu kämpfen. Implementiert wird das System in Java, um Plattformunabhängigkeit zu erreichen.

Schon jetzt zeigen Simulationen, dass das Netz relativ stabil ist: Bis zu 20 Knoten können gezielt geschlossen werden und bis zu 30 Prozent zufällig ausfallen, ohne dass das Netz zusammenbricht. Nutzer können sich auf die Echtheit der empfangenen Daten verlassen: Der Inhalt einer Datei ist über eine Prüfsumme an ihren Namen gebunden. Allerdings lassen sich Dateien noch nicht gezielt suchen.

Peekabooty

Nicht auf der Netzebene, sondern am Client setzt folgendes vielversprechende Projekt an: Im Frühjahr 2001 kündigte die US-Hackergruppe »Cult of the Dead Cow« (CdC) die Veröffentlichung eines eigenen Browsers namens Peekabooty an. [18] Sie wollen ihn auf dem Hackerkongress DefCon im Juli 2001 vorstellen.

Peekabooty soll nicht nur den kompletten Datentransfer zwischen Server und Browser verschlüsseln und durch verteiltes Rechnen verhindern, dass die Nutzer identifiziert werden können. Nutzer können mit anderen Peekabooty-Nutzern Kontakt aufnehmen, womit ein eigenes Kommunikationsnetzwerk entstehen soll. Innerhalb dieses Netzes ist die komplette Kommunikation verschlüsselt - selbst E-Mails können die Peekabooty-Nutzer sicher verschicken. Damit könnten Peekabooty-Nutzer sogar Firewalls überwinden.

Peekabooty-Nutzer können aber auch Netzdaten abrufen. Ein Nutzer in China könnte mit Hilfe dieses Browsers an Internetinhalte gelangen, die von der chinesischen Regierung eigentlich zensiert wurden. Ein PeekaBooty-Rechner außerhalb Chinas würde zum

Gateway: Hierüber könnten die angeforderten Daten verschlüsselt an den chinesischen Dissidenten weitergeleitet werden.

Berühmt wurde die CdC, als sie die Software-Tools »Back Orifice« und »Back Orifice 2000« entwickelte, die einen nahezu unbeschränkten Zugang zu fremden Microsoft-Rechnern ermöglichten. Sie werden heute noch von Systemadministratoren als Fernwartungswerkzeug, aber auch von Hackern benutzt.

Literatur

[1] Das Programm ist für den privaten Einsatz lizenzfrei erhältlich und kann zum Beispiel über den PGP-Server ftp://ftp.de.pgpi.com/pub/pgp oder über Network Associates, Inc. (http://www.pgpinternational.com) bezogen werden. Hier finden sich auch Hinweise zur Installation und zur Bedienung des Programms.

[2] http://www.iks-jena.de/mitarb/lutz/anon/as-node.html

[3] http://www.itech.net.au/pi/, Download von »Private Idaho«

[4] http://www.skuz.net/potatoware/index.html, Downloadseite für »Potato« (DOS), »Jack B. Nymble« (Windows) und »Reliable« (Remailer-Server für Windows)

[5] http://www.remailer.cjb.net, Homepage des Orange-Projekts

[6] http://www.safeweb.com, Homepage von Safeweb

[7] engl. header

[8] engl. crowd

[9] Hannes Federrath, Kai Martius, Anonymität und Authentizität im World Wide Web, TU Dresden, http://www.inf .tu-dresden.de/~hf2/publ/1998/FeMa1_98itg/

[10] »Angelehnt an das Wassenaar-Abkomrnen vom Dezember 1998 wird es keine Exportkontrollen mehr für 64-Bit-Massenmarktprodukte, 56-Bit-Verschlüsselungskomponenten und 512-Bit-Schlüsselmanagement-Produkte geben.« Aus: Christiane Schulzki-Haddouti, Kontrollierte Liberalisierung, telepolis, 13.1. 2000, http://www.heise.de/tp/deutsch/inhalt/te/5683/1.html

[11] http://www.onion-router.net/, Homepage von Onion Routing

[12] Defense Advanced Research Projekts Agency (DARPA)

[13] engl. onion

[14] Unbeobachtetes Surfen. Gespräch mit Hannes Federrath, dem Entwickler des Java Anon Proxy. Burkhard Schröder in telepolis, 11. 4. 2001, http://www.heise.de/tp/deutsch/inhalt/te/7347/1.html

[15] http://anon.inf.-tu-dresden.de/

[16] http://freenet.sourceforge.net, Homepage von Freenet, »the free network project«

[17] http://www.sanity.ukunux.net, Homepage von Ian Clark

[18] Frank Patalong, »PeekaBooty«: Jetzt kommt der Hacker-Browser, SpiegelOnline, 8. 5.2001, http://www. spiegel.de/druckversion/0,1588,132661,00.html

Christiane Schulzki-Haddouti ist freie Journalistin und seit 1996 Telepolis-Korrespondentin. Als Herausgeberin betreute sie »Vom Ende der Anonymität -Die Globalisierung der Überwachung«, erschienen 2000 im Heise-Verlag.