Patrice Riemens
HEART — DON'T PANIC! HACK IT! (*)

Wenn Sie das erste Mal einem Hacker begegnen …

(*) Das war das Motto der Galactic Hacker's Party in Amsterdam, August 1989.

Passend zum diesjährigen Motto "InfoWar" veranstaltet die Ars Electronica im Rahmen des Festivals einen Hackertreff. Der Zeitpunkt ist richtig gewählt: Die Hacker sind wieder da. Und da das Informationszeitalter angeblich auch einen Wilden Westen hat, dürfen natürlich die Cowboys (oder Indianer!) nicht fehlen. Aber das Informationszeitalter, von Manuel Castells in seiner namensgebenden Trilogie so meisterhaft dekonstruiert, bedeutet für jeden Menschen und vor allem für jede Interessensgruppe etwas anderes. Und ähnlich geteilt sind auch die Meinungen über die Hacker — durchaus nicht immer zu ihrem und unserem Vorteil.

Erst einmal gilt es zu definieren, was ein Hacker eigentlich ist. Definitionen, ohnehin eine heikle Angelegenheit, sind in diesem Fall noch schwieriger. Die Ideale und das Selbstbild der Hacker und ihr häufig katastrophales Image in der Öffentlichkeit könnten nicht weiter auseinanderklaffen. Die Leichtgläubigkeit der Öffentlichkeit, Desinformation durch sensationslüsterne Medien und Manipulationen zugunsten von Regierungsinteressen haben zum schlechten Ruf der Hacker beigetragen. Im günstigsten Fall erscheinen sie als nervtötende Jugendliche, deren präpubertäre destruktive Triebe es im Zaum zu halten gilt. Man denke nur an das idiotische Affentheater rund um die Computer in den Schulen. Im schlimmsten Fall werden Hacker als enorm gefährliche Technoterroristen dämonisiert, die eine teuflische Macht über Maschinen haben und die ganze Gesellschaft in Gefahr bringen. Kevin Mitnick, gegen den die US-Regierung seit seiner Verhaftung vor mehr als zwei Jahren keine schlüssige Anklageschrift zustande gebracht hat, ist nur ein trauriges Beispiel dafür.

Was aber ist nun ein Hacker? Die Dinge werden leichter verständlich, wenn wir erst einmal das gewohnte Wort "Computer" vor dem "Hacker" weglassen, denn dann können wir auf den eleganten Satz von Eric Corley (aka Emmanuel Goldstein von "2600") zurückgreifen: "Ein Hacker ist eine neugierige Person." Diese minimalistische Beschreibung trifft den Kern der Sache genau. Beim "Hacken" geht es nicht um die Technologie als solche, auch wenn sie dessen eigentliches Terrain ist. "Hacken" hat mit einer bestimmten Geisteshaltung, einer Einstellung zu tun. Es geht dabei um Lernen und freies Forschen. Wir müssen uns aber der doppelten Kodierung des Wortes "Neugier" bewußt sein. Mag die offizielle Sprachregelung die Neugier als Motor für die Weiterentwicklung unseres Wissens betrachten, so hält es die Vox Populi eher mit dem französischen Sprichwort: "La curiosité est un vilain défaut." Neugier ist eine schreckliche Angewohnheit. Neugier bedeutet, seine Nase in fremde Angelegenheiten zu stecken, peinliche Fragen am falschen Ort und zum falschen Zeitpunkt zu stellen und sich ganz allgemein für Dinge zu interessieren, die "einen nichts angehen". Und genau diese Vorstellung bringt man leider auch mit Hackern in Verbindung.

Das Eindringen in fremde Computersysteme hat mit Wissen, d.h. mit Macht, zu tun. Beim Wissen aber geht es weniger um die Macht selbst, es stellt eher eine Bedrohung für sie dar. Hacker gefährden die Position der Mächtigen. Denn sie stellen auf einer peinlich praktischen Ebene die Behauptung in Frage, unsere Gesellschaft sei so komplex geworden, daß man ihre Steuerung am besten den eigens dafür abgestellten "Experten" überlasse. Wer diese Experten sind und in welchem Interesse sie handeln, bestimmt selbstverständlich, wer an den Schalthebeln der Macht sitzt. Der diesbezügliche Konsens ist allerdings etwas total Fabriziertes, das jeder Grundlage entbehrt. Die technischen oder sonstigen "Experten"

versagen immer wieder, und ihre Systeme sind weitaus unzuverlässiger und unsicherer, als sie jemals eingestehen würden. Das Aufdecken von Fehlern, in manchen Fällen sogar von richtiggehenden Betrügereien, hat so manchen Hacker und so manche Hackergruppe in den Mittelpunkt der (inter)nationalen Diskussion gestellt … oder auf die Anklagebank gebracht (die man als Erweiterung der Diskussion sehen kann). Das hat weitreichende politische Konsequenzen. Zum besseren Verständnis der politischen Auseinandersetzung als Ursache bzw. Folge des Hacking bedarf es einiger Ausführungen über die soziale Natur des Wissens.

Auch ohne in die Feinheiten der Erkenntnistheorie einzudringen, ist unmittelbar einsichtig, daß uns hier manche Elemente der sie konstituierenden Triade — Wissenschaftstheorie, Ideengeschichte und Wissenssoziologie — ein Stück weiterbringen können. Die Wissenschaftstheorie stellt sozusagen unser Bezugssystem dar, und die Ideengeschichte beleuchtet die Entwicklung des vorliegenden Problems über die Jahrhunderte hinweg, aber am meisten Aufmerksamkeit in diesem Zusammenhang verdient zweifellos die Wissenssoziologie. Die Wissenschaftstheorie lehrt (oder legt zumindest nahe), daß Wissen weder etwas Einfaches noch etwas Gegebenes ist und daß es insbesondere nicht etwas "außerhalb von uns" Existierendes ist. Die Ideengeschichte beleuchtet unter anderem die Zwänge, die rund um das Wissen in verschiedenen offenen und geschlossenen Systemen bestehen. (Den alten Ägyptern wird — um ein berühmtes Beispiel zu nennen — der Besitz eines umfangreichen "Geheimwissens" nachgesagt, das zum Aufkommen der "Hohepriester" führte.) Aber der Wissenssoziologie gebührt das Verdienst, die uralten Konflikte um die Schaffung und Verbreitung des menschlichen Wissens als sozialen Antagonismus — d. h. als "Klassenkampf" — erkannt zu haben. Einfach gesagt: Wer der bestehenden Hierarchie positiv gegenübersteht, bevorzugt "geschlossene", d. h. repressive (Wissens-)Systeme. Die Gegner des jeweiligen Systems hingegen fordern Offenheit, d.h. Freiheit — in allen Dingen. "Information will frei sein" ist demnach ein hochpolitisches Statement, das sich zum gegenwärtigen Zeitpunkt auch noch gegen die herrschende Meinung richtet.

Dies um so mehr, als die derzeitigen "globalen" Entwicklungen eigentlich nur eine Interpretation zulassen: Die besitzende Schicht ist dabei, ihre Privilegien weitgehend zurückzuerobern, egal, ob in puncto Wissen, Macht oder Einkommen — oder, wie üblich, in allen drei Bereichen. Diesem Trend liegt die Ideologie des sogenannten "freien" Marktes zugrunde. Tatsächlich entwickeln wir uns mit großer Geschwindigkeit von einer Marktwirtschaft zu einer Marktgesellschaft. (Der Ausdruck stammt von Friedrich Hayek, wurde aber von Zaki Laidi in einem Interview mit *Le Monde* vom 9. Juni 1998 auf brillante Weise neu formuliert.) Da sie die Aufrechterhaltung und Förderung dieses Zustandes sowohl in Wirtschaft als auch Politik ermöglicht, kommt der Technologie in diesem Prozeß eine entscheidende Rolle zu. Auf Unternehmerseite sehen wir uns mit enormen Anstrengungen konfrontiert, Wissen vollständig zum Eigentum zu erklären. Sowohl die Produktion von als auch der Zugang zu Wissen wird Marktprozessen unterworfen. Gleichzeitig wird die Non-Profit-Forschung, die sich nicht an der Nachfrage des Marktes orientiert, marginalisiert, abgelehnt, ja sogar unterdrückt. Auf Regierungsseite ist trotz allen Geredes vom Verschwinden des Staates eine gesteigerte Tendenz zum Erfassen und Sammeln von Daten und zur elektronischen Überwachung zu beobachten. Gleichzeitig wird die Verantwortung des Staates für das Wohlergehen seiner Bürger als unzeitgemäß abgelehnt. Alles zusammen läuft auf massive Angriffe von allen Seiten des politisch-wirtschaftlichen Spektrums auf den öffentlichen Raum hinaus. Und in allen Fällen haben wir es mit geschlossenen Wissens- und Kontrollsystemen zu tun, die sich dem Zugriff und der Überprüfung durch demokratisch konstituierte Einrichtungen oder Privatpersonen entziehen.

Geschlossene, den Spielregeln des Marktes unterworfene Informationssysteme, deren Zugang von "Bedarfs"-Kriterien kontrolliert und von Bezahlung — sprich: von "wirklicher Nachfrage" — abhängig gemacht wird, haben eine neue Kategorie "illegalen" Wissens entstehen lassen. Das ist das Reich der Hacker, die mit gutem Grund behaupten, daß ihr Tun vollkommen legitim sei. Denken wir nur an die jüngsten Entwicklungen in der Softwareindustrie. Auch wenn es wie eine Karikatur anmuten mag — der mittlerweile legendäre Aufstieg der Microsoft Corporation und ihres Über-Ich Bill Gates zu einem den ganzen Erdball beherrschenden, elektronischen Tyrannen ist nur das Resultat einer unkontrollierbar gewordenen Ideologie des "freien" Marktes. Aber die dadurch auf den Plan gerufenen Gegenkräfte — ob letzten Endes siegreich oder nicht — geben uns eine Vorstellung von der wichtigen Rolle der Hacker im Kampf gegen das Entstehen "neuer Mauern" an der Wissensfront. Die Freigabe des Netscape-Quellcodes im sogenannten "Browser-Krieg", allen Grundsätzen der "Wissen ist Eigentum"— Ideologie zum Hohn, war ein Sieg des Ethos und der Geschicklichkeit von Hackern innerhalb und außerhalb dieses Unternehmens. Daß Regierungen in Sachen Kryptographie zunehmend auf verlorenem Posten stehen, ist ein weiteres Beispiel. Die Hacker — in diesem Fall bezeichnen sie sich als "Cypherpunks" — haben eindeutig bewiesen, daß, wenn die Bereitschaft dazu besteht, der vollkommene Schutz der Privatsphäre in der (elektronischen) Kommunikation möglich ist. Das eröffnet Möglichkeiten zur Gestaltung der Zukunft, die die Regierungen nur durch den (hoffentlich) völlig inakzeptablen Einsatz von Gewalt verhindern könnten.

Wenn wir also unter InfoWar berechtigterweise auch den Kampf für und um Privatsphäre und freie Information in der bürgerlichen Gesellschaft verstehen, sind Hacker unsere Alliierten, nicht unsere Feinde. Wie so oft, wenn bisher gültige Wertsysteme und überkommene Wahrheiten ihren Sinn verlieren, erweist sich das scheinbar Bedrohliche als hilfreich, und unsere vorgeblichen Beschützer entpuppen sich als falsche Freunde. Schon die alten Römer waren sich dieses Dilemmas bewußt, als sie den Spruch prägten: "Quis custodiet ipsos custodes?" Die Antwort auf diese Frage stand auf einem T-Shirt der holländischen HackTic-Gruppe zu lesen: "Watching Them Watching Us".

Also: Be Curious! Don' t Panic! Hack It!

Dank an Barbara Strebel

Literaturhinweise

Das beste Buch zum Thema Hacker bleibt auch in den späten neunziger Jahren ein Klassiker aus der Mitte der achtziger Jahre: Hackers von Steven Levy. Seine Analysen des "Hacker-Ethos" und des "Hands-on-Imperartivs" sind unübertroffen.

Wenn Sie sich für aktuelle Informationen und solide politische Analysen interessieren, sehen Sie auf der Web-Site von "2600", The Hackers' Quarterly (www.2600.com) nach. Oder, noch besser, entscheiden Sie sich für ein Abonnement (für Bewohner der ehemaligen "Ostblockstaaten" kostenlos!).

Die besten Texte zur "Open Source"-Ideology stammen von Eric S. Raymond und sind unter folgender Adresse zu finden: bzw. unter