

## Die Randkultur der Hacker - Rebellen, Spione und Diebe

R. GIRTLER <sup>1</sup>

**Das Problem mit Hackern wird meist aus technischer - oder wegen der möglichen Schäden - aus wirtschaftlicher und politischer Sicht betrachtet. Der Autor behandelt im vorliegenden Artikel dieses Problemfeld aus der Sicht des beschreibenden Soziologen als eines von sozialen Randgruppen, die es immer schon gab, die sich aber mit den heute allgegenwärtigen Mitteln der Informationstechnologie in teilweiser neuer und vor allem globaler Weise bemerkbar machen. Die dabei verwendete, etwas ungewohnte Terminologie kann dabei helfen, das Hackerproblem von einer neuen Seite zu sehen und vielleicht auch besser zu verstehen.**

### 1. Die Hacker als Freibeuter auf dem Meer des Internets

Die Welt des Computers erinnert an Meer, Seefahrt, Freibeuterei und windiges Gleiten auf den Wellen. Auch mit den Wörtern „Surfen im Internet“ verbinden sich Gedanken an Wind und Meer.

Im großen Meer des Internets findet der Hacker gleich einem Freibeuter seine Heimat.

Von diesem Hacker, der einen denkbar schlechten Ruf besitzt, der aber auch eine gewisse gangsterhafte Romantik verbreitet, handeln meine Ausführungen. Allerdings, dies sei eingefügt, schreibe ich diesen Beitrag nicht als Computerspezialist, sondern eher als ein Laie in der Welt der Computer und als jemand, der sich seit Jahren mehr oder weniger intensiv mit Randkulturen beschäftigt. Und irgendwie faszinieren mich auch diese modernen Freibeuter, die geschickt und bewundernswert mit den modernen Techniken umzugehen wissen.

Unter „Hacker“ werde ich in dem vorliegenden Aufsatz also eine Person verstehen, die durch allerlei Kniffe versucht, gleich einem Schmuggler oder Freibeuter, ungesehen und unbelangt in fremde Häfen, also fremde Computersysteme, zu gelangen. Der Hacker sucht nach offenen Toren, die Hafenzufahrten gleichen, um sich in den Häusern und Lagerhallen anderer willkürlich zu bedienen. Der Hacker will zunächst ganz im Stile eines kriegerischen Piratenkapitäns durchlässige Stellen finden, die ihm helfen, Informationen über die feindliche Bastion einzuholen. Oft peilt er mehrere Häfen an, die so genannten IP-Adressen, um zu einem Erfolg in Form offener Tore – der Ports – zu kommen. Steht eine der Zufahrten offen, genügt dies als Ansatzpunkt. Jeder am weiten Meer gelegene Hafen, also jeder im Internet angeschlossene Rechner, hat geografisch seine eindeutige Adresse, bzw. IP-

---

<sup>1</sup> GIRTLER, Roland, ao. Univ.-Prof. Dr., Universität Wien, Institut für Soziologie, Rooseveltplatz 2, A-1090 Wien.  
(E-Mail: roland.girtler@univie.ac.at)  
In: e&i elektrotechnik und informationstechnik. Heft 7/8 Juli/Aug. 2003

Adresse, unter der er angefahren werden kann.

Dadurch finden die Schiffsladungen bzw. die Datenpakete immer an ihr Ziel. Mit einer so genannten „statischen IP“, dem festen Hafen im Internet, bleibt ein PC ständig unter der gleichen Identifikation erreichbar. Kennt der Freibeuter ebenso wie der Hacker den genauen Zugang zum Hafen, erleichtert ihm dies die Arbeit. Hacker finden Mittel und Wege, Rechner im Netz zu identifizieren, ganz im Stile schlauer Freibeuter, die nach verborgenen Zufahrtsstraßen im Meer suchen.

Die Kultur der Hacker ist typischer Weise eine Randkultur. Randkulturen entstehen überall dort, wo innerhalb einer Gesellschaft Menschen, deren Ruf ein schlechter ist, gemeinsame Strategien entwickeln, um einigermaßen zu überleben, um sich nicht erniedrigen zu lassen, um auf verbotene Weise zu Gewinn zu kommen oder um bewusst anderen zu schaden. In diesem Sinn habe ich vier Typen von Randkulturen erarbeitet:

- (1) Randkulturen des Überlebens
- (2) Randkulturen der Revolution und Rebellion
- (3) Randkulturen des kriminellen oder verpönten Geschäftes und
- (4) Randkulturen der gemeinsamen Herkunft (*Girtler, 1998*)

Die so genannten Hacker, die in freibeuterischer Weise die durch Computer eingeleitete Vernetzung der Menschen stören oder in Unordnung bringen, ordne ich grundsätzlich sowohl den Randkulturen der Rebellion als auch den Randkulturen des verpönten Geschäftes zu. In diesem Sinne werde ich im Folgenden verfahren.

## **2. Hacker als Rebellen**

Der klassische Hacker hat etwas von einem Rebellen an sich, er kämpft für freie Information<sup>2</sup>, für ihn soll der Zugang zu Computern frei sein. Die Freude am Programmieren und an der kreativen Nutzung der Technik steht im Mittelpunkt und gipfelt in dem Zitat: „Nicht das Hören einer MP3-Datei ist der Genuss, sondern das Hacken derselben.“ Zu den Rebellen unter den Hackern sind wohl jene Leute zu zählen, die sich im Chaos Computer Club - im Internet leicht erreichbar - zusammengetan haben (<http://vwww.ccc.de/hackerethics>). Charakteristisch für diesen rebellischen Club, der aus der modernen Jugendkultur, die zur „**Internetgeneration**“ wurde, zu kommen scheint, ist, dass er so etwas wie einen Ehrenkodex entwickelt hat, auf den ich jedoch erst etwas später eingehen will.

Die virtuellen „Robin Hoods“ sehen sich als edle Leute, obwohl ihnen klar ist, dass das unerlaubte Eindringen in fremde Rechner gegen das Gesetz verstößt. Aber gerade dies reizt.

Rebellisches Denken steckt, dessen bin ich mir sicher, hinter den Angriffen auf die Computersysteme der mächtigsten Institutionen dieser Welt, in denen es um Frieden und Krieg geht. So starteten Hacker im Februar 2000 eine Offensive auf das Pentagon, die immerhin bewirkte, dass das US-Verteidigungsministerium alle seine Rechner überprüfen ließ. Und im Mai 2001 legten Hacker die Webseite des Weißen Hauses für mehrere Stunden lahm. Die Rebellen bombardierten den Web-Server

---

<sup>2</sup> Vgl. Philosophy of the GNU Project: "... information wants to be free ...«[www.gnu.org/philosophy/philosophy.html](http://www.gnu.org/philosophy/philosophy.html)). Die „Open Software Foundation“ (OSF) kämpft um für jeden frei verfügbare Software. Hier stehen die Positionen proprietärer Software (vor allem Microsoft) und der OSF (vor allem Linux unter der GNU-Lizenz) einander als feindliche Ideologien gegenüber.

solange mit Datenmüll, bis dieser zusammenbrach (DoS = Denial of Service Attack). Von Rebellen dieser Art, die den Hochmut überschäumender Politiker und Machthaber durch Angriffe im Internet in Frage stellen, ist wohl in Zukunft noch einiges zu erwarten? <sup>3</sup>

### **3. Hacker als Spione, Schmuggler und Diebe**

Ein Hacker, der zum echten Kriminellen wird, wird für gewöhnlich als Cracker bezeichnet. Er bedient sich der Hackermethoden, um Daten zu stehlen, Systeme lahm zu legen oder mit spektakulären Aktionen zumindest kurzfristige Berühmtheit einzufahren.

Sobald ein Computer an das Internet angeschlossen ist - dies gleicht der Gründung eines Hafens - bietet er eine Angriffsfläche für Hacker. Durch verschiedene Maßnahmen wie etwa eine Firewall, regelmäßige Programm-Updates und sichere Passwörter lässt sich ein System zwar ganz gut abschotten, doch eine 100-prozentige Sicherheit ist nicht realisierbar.

#### **3.1 Das Erobern von Häfen (Ports)**

Ein Cracker dringt in erster Linie in zerstörerischer Absicht in Computersysteme ein. Er spioniert dort Daten und Passwörter aus, löscht Dateien und legt Systeme lahm. Cracker leben vor allem von der Fahrlässigkeit der Benutzer von Computern, die es unterlassen haben, ihren Hafen, den Port, entsprechend abzusichern und sorgfältige Hafenwächter aufzustellen, die nur jene passieren lassen, die das verwickelte Lösungswort kennen.

So etwas passierte im Jänner 2001. Der offene Port Nummer 1433 und ein unsicheres Passwort reichten aus, und die Hacker waren im System. Dieser Fehler des Systemadministrators hatte spektakuläre Auswirkungen, denn diesmal handelte es sich nicht um den Privat-PC der technisch unbedarften Familie XY, sondern um die Datenbank des Weltwirtschaftsforums in der Schweiz. Jene hoch exklusive Institution, die für die wirtschaftliche und damit auch die technologische Zukunft der Welt Mitverantwortlich ist, war selbst nicht in der Lage, die Daten ihrer prominenten Mitglieder zu schützen. Die Ausbeute war jedenfalls brisant. Die Hacker kopierten private Telefon- und Handynummern sowie Kreditkartennummern von hochrangigen Persönlichkeiten, darunter Bill Clinton, Palästinenserpräsident Yasser Arafat oder Südafrikas Staatspräsident Thabo Mbek.

Die Absicherung des Ports war hier schwach, und das nutzten die Cracker aus. Niemand löste Alarm aus. Die Angreifer erkannten bald, dass ein Microsoft-Server mit Windows 2000 betrieben wurde. Dazu war das Standard-Passwort der auf dem Server laufenden Microsoft-Datenbank nicht geändert worden - jeder frisch gelieferte SQL-Server vergibt mit dem Benutzernamen „sa“ und einem leeren Passwortfeld standardmäßig Administratorenrechte. Mehr war nicht nötig, und die heiklen Informationen lagen offen. Die Cracker hatten die Zugangswege zum neuen Hafen gefunden, in dem sich ein paradiesisches Leben ankündigte.

In diesem Sinn stahlen Hacker auch im November 2001 Kundeninformationen und Kreditkartennummern auf dem Internetportal von Playboy und versandten kurz

---

<sup>3</sup> Allerdings sollte man nicht übersehen, dass derartige Angriffe auf die Computernetze des Gegners heute normale militärische Angriffsstrategien sind. Auch die Geheimdienste aller Welt "hacken" professionell.

darauf die Informationen an die Playboy-Kunden. Die Nachrichten waren mit „ingreslock 1524“ unterzeichnet. Der Cracker behauptete, bereits seit drei Jahren Zugriff auf die Kundendaten gehabt zu haben. Diese persönlichen Daten kursieren derzeit in der Unterwelt, in anarchistischen Kreisen und unter Kreditkartenbetrügnern. Das Geschäft dürfte ein großes sein.

Gesetzlich verboten ist auch das Schnüffeln im Netz, nämlich das diebische Abhören fremder Computer. Die so genannten Sniffer-Tools überwachen alle ein- und ausgehenden Daten an bestimmten Stellen im Netzwerk. Im Internet erfolgt die Übertragung in einzelnen Datenpaketen. Der Sniffer fängt diese ab, protokolliert sie und ordnet sie nach zusammengehörigen Blöcken. Kann der Hacker diese Informationen richtig auswerten, sind E-Mails, unverschlüsselt übertragene Passwörter oder Chats auch schon in seiner Hand.

### **3.2 Das Ausspionieren von Passwörtern**

Zu den wichtigsten Sperren für sensible Daten zählen, wie schon angedeutet, Passwörter. Sie sind dann innerhalb kürzester Zeit zu knacken, wenn einfache und nahe liegende Passwörter verwendet werden, wie der Kosenamen der Angebeteten, der Vorname der Tochter oder der frühere Familienname der Frau. Und tatsächlich sind viele Kennwörter für einschlägige Programme kein Problem. Zu allererst wird der Hacker jedoch die gespeicherten Passwörter testen. Denn wenn der Anwender dies zulässt, merkt sich der Internet-Explorer die Eingaben bei der Anmeldung zu den diversen Internetdiensten, und auch die Einwahl ins DfÜ-Netzwerk bleibt der Bequemlichkeit halber gespeichert. Mit diesen Daten lässt sich einiges anfangen, und vielleicht ist darunter auch das Kennwort für die Bankverbindung oder für den PC am Arbeitsplatz. Eine weitere Methode zum Knacken von Passwörtern oder Verschlüsselungen ist die Brute-Force-Attacke. Dabei probiert ein Tool einfach alle Kombinationen von Buchstaben und Ziffern aus. Kurze Passwörter sind so leicht zu entschlüsseln, bei längeren ist die Rechenleistung ausschlaggebend. Andere Passwort-Cracker arbeiten mit Wörterbüchern. Hier sind die Kombinationsmöglichkeiten eingeschränkt, die Wahrscheinlichkeit eines Treffers bleibt dennoch hoch, da viele Kennwörter auf einem leicht zu merkenden Begriff in der jeweiligen Sprache basieren. Andere Suchmethoden setzen auf die Statistik. Statt wie bei Brute Force trifft das Tool eine Vorauswahl der Zeichenkombinationen aufgrund statistischer Wahrscheinlichkeiten.

Vergleichsweise leicht haben es die Cracker bei ZIP-Dateien, denn in einem Archiv befindet sich zumindest eine unkomprimierte Datei. Damit liegt neben der verschlüsselten Datei bereits das Gegenstück vor, und Tools wie etwa ZIP Key wissen, wonach sie suchen müssen. Das Knacken der Kennwörter ist erst gar nicht nötig, wenn im Hintergrund ein Keylogger-Programm läuft. Ein solches Tool zeichnet alle Tastatureingaben auf, und schon ist das Geheimnis gelüftet. Die Dateien werden entweder auf der Festplatte abgelegt oder direkt per Internet versandt.

### **3.3 Die Idee des Odysseus**

Die Gangster im Internet können auch bei Privat-PCs, die kleinen Jachthäfen gleichen und wenig anzubieten haben, Schaden anrichten.

Schon ein harmloser „Trojaner“ in Form von Weihnachtsgruß-Programmen kann den Rechner ausspionieren oder sich eine Tür für spätere Hacker-Angriffe offen halten. Auch dieser Name - Trojaner - erinnert an Meer und kriegerische Zerstörung einer

Hafenstadt, nämlich Trojas in Kleinasien. In dem Epos „Ilias“ des großen Homer, welches von der Eroberung Trojas durch die Griechen handelt, wird erzählt, wie nach der Idee des listenreichen Odysseus die Griechen ihre Krieger in einem riesigen hölzernen Pferd versteckten und dieses vor die Tore der belagerten Stadt stellten. Die Trojaner dachten, es sei ein Geschenk und brachten das Pferd in ihre Stadt. Als das große hölzerne Pferd in der Hafenstadt war, krochen aus diesem in der Nacht unbemerkt die griechischen Kriegshelden und richteten furchtbaren Schaden an - gleich den in ein Computersystem gelangten Viren. Auf die Geschichte mit dem Pferd zielt dieser klassische Spruch ab, der auch Computerbenutzern etwas sagen sollte:

„Timeo Danaos et dona ferentes“: Ich fürchte die Griechen (Danaer) auch (und besonders), wenn sie Geschenke bringen.

Also: Achtung vor eingeschleusten Pferden, die man in der Welt der Computer sinnig als Trojaner zu bezeichnen pflegt.

Solche Pferde, also die Trojaner, können furchtbar gefährlich werden. Die Trojaner gelangen meist über E-Mail-Anhänge, zweifelhafte Webseiten oder File-Sharing auf die Rechner.

Dies erfolgte auch auf spektakuläre Weise im Oktober 2000: Ein Eindringling bewegte sich geraume Zeit durch das Microsoft-Netzwerk und verschaffte sich unter anderem Zugriff auf den Source Code von künftigen Microsoft-Produkten. Nach und nach wird bekannt, wie die Sicherheitsmaßnahmen des Software-Riesen umgangen wurden: Ein Trojaner auf dem Rechner eines Mitarbeiters versorgte den Hacker mit den nötigen Informationen und Passwörtern, so dass er bald einige Rechte auf diesem Computer bekam. Von da aus war es nicht mehr weit zum Zugriff auf das Microsoft-interne Netzwerk.

Zu den gefährlichsten Hackertricks, bei denen Trojaner-Pferde eingesetzt werden, gehören die so genannten Backdoors (Hintertüren). Dabei wird ein kleines Programm - als Trojaner - auf den fremden Rechner geschleust, um eine Verbindung zu einem Remote Access Tool (RAT) zu ermöglichen.

Durch so genannte Backdoor-Programme kann ein Eindringling den fremden Computer beinahe gänzlich ausspionieren (wie ferngesteuert). Er hat aber auch die Möglichkeit, diesen Computer als „Zeitbombe“ zu nutzen, wodurch eine große Menge von Computern synchronisiert einen Angriff durchführen kann.

Gespeicherte Passwörter werden ausgelesen, E-Mails und Instant-Messenger-Chats protokolliert oder sogar die einzelnen Tastatureingaben via Keylogger mitverfolgt. Hier kann der Schaden beträchtlich sein. Freunde im Chat können verärgert werden, bei der Behörde können via Internet Eingaben gemacht oder der Briefwechsel mit der Krankenversicherung eingesehen werden.

Trotz neuer Techniken, die derartige Eindringlinge verhindern sollen, entwickeln die Cracker immer wieder neue Tricks, um die Sicherheitswälle zu durchsegeln und Trojaner einzuschleusen.

Auf der letztjährigen Jahrestagung des Chaos Computer Clubs stellten die Hacker ihre Visionen für die künftigen Herausforderungen vor:

Es war auch von programmierten Kühlschränken die Rede, die dann plötzlich 4000 Liter Milch statt zwei bestellen oder von Handys mit „schicken Betriebssystemen“, die eine Telefonrechnung in Schwindel erregende Höhen schnellen lassen (<http://www.ccc.de/hackerethics>).

#### **4. Hacker als Spaßmacher**

Die Hacker sind oftmals verspielt und werden vielfach durch Berichte über große Hackerattacken in den Medien angespornt. Durch Probieren oder mit Hilfe von Anleitungen versuchen sie diese nachzuvollziehen und sind sich der Tragweite ihrer Taten oft nicht bewusst. Hacker dieser Art, man nennt sie auch Whacker, wollen lediglich spielen und andere eher auf harmlose Weise ärgern.

Solche „Spaßmacher“ waren am 23. Februar 2003 am Nachmittag um 13 Uhr 55 im Computermeer der großen Handelsfirma Billa unterwegs. Der Kunde, der auf der Billa-Home-page (<http://www.billa.at>) nach Angeboten aus der Käsecke, nach den Preisen von Bananen oder nach dem Trockensortiment suchte, wurde zu seiner großen Überraschung, die manchen vielleicht mit Freude erfüllte, mit Pornowerbung begrüßt. So las er von „Anna (20) - privat und unzensiert“, die zum Besuch ihrer Homepage einlud. Links waren manipuliert worden, um Werbung für Pornosites zu machen.

In einer Stellungnahme betonte Billa, dass man die „Situation sehr ernst genommen und prompt auf den Angriff reagiert“ habe. In einer „groß angelegten Aktion über Nacht sei der größte Schaden“ behoben worden.

Es hatten sich also Hacker den Spaß gemacht, das Publikum von Billa, das über Internet etwas für ihre Mittagseinkäufe erfahren wollte, lustvoll zu schocken.

Einen Spaß machten sich im November 1984 auch Steffen Wernery und Wau Holland vom Chaos Computer Club in Deutschland. Sie entdeckten eine Sicherheitslücke im Bildschirmtext (BTX) der Bundespost und buchten an einem Wochenende über 130000 D-Mark um. Am Montag Morgen riefen sie bei der betroffenen Bank an und verkündeten einem verschreckten Sachbearbeiter sinngemäß: Bei Ihnen fehlen über 100000 Mark. Aber machen Sie sich keine Sorgen, wir wollen das Geld gar nicht!

#### **5. Die Gaunerehre der Hacker**

Dort, wo es Gauner gibt, gibt es auch so etwas wie Gaunerehre, nämlich einen Kodex, der dem wahren Ganoven, der etwas auf sich hält, angibt, dass gewisse Handlungen seiner Ehre widersprechen. So ist es im Sinne der Gaunerehre, dass ein echter Dieb armen Leuten nichts wegnimmt oder dass Wildschützen im Gebirge nicht auf Jäger schießen. Im Laufe der Zeit entstand nun auch eine spezielle Hackerethik. Anschaulich erfasst ist sie bei den Chaos Computer Clubs. Hier sind es folgende Regeln, die dem Hacker heilig sein sollen: <sup>4</sup>

- (1) Der Zugang zu Computern und allem, was einem zeigen kann, wie diese Welt funktioniert, sollte unbegrenzt und vollständig sein.
- (2) Alle Informationen müssen frei sein.
- (3) Misstraue Autoritäten - fördere Dezentralisierung.
- (4) Beurteile einen Hacker nach dem, was er tut und nicht nach üblichen Kriterien wie Aussehen, Alter, Rasse, Geschlecht

---

<sup>4</sup> Ähnlich gibt es auch für „normale“ Nutzer einen ungeschriebenen Verhaltenscodex, die so genannte „Netiquette“. Bei deren Verletzung kann durch massenhafte kritische E-Mails (das so genannte „flaming“) der Briefkasten des Nutzers blockiert werden, so dass er von den Kommunikation ausgeschlossen, sozusagen „exkommuniziert“ wird.

oder gesellschaftliche Stellung.

(5) Man kann mit einem Computer Kunst und Schönheit schaffen.

(6) Computer können dein Leben zum Besseren verändern.

(7) Mülle nicht in den Daten anderer Leute.

(8) Öffentliche Daten nützen, private Daten schützen.

Die Hackerethik ist nur bedingt einheitlich definiert. Es gibt eine ursprüngliche Version aus dem Buch „Hackers“ von Steven Levy (*Levy, 2001*). Unstrittig ist insofern, dass die ursprüngliche Version aus dem MIT-Eisenbahnerclub (Tech Model Railroad Club) kommt und insofern aus einer Zeit stammt, in der sich verhältnismäßig viele Leute wenige Computer teilen mussten und entsprechende Überlegungen zum Umgang miteinander und der Materie sinnvoll waren.

Die letzten beiden Punkte sind Ergänzungen des Chaos Computer Clubs aus den achtziger Jahren. Nachdem einige mehr oder weniger „Durchgeknallte“ aus der Hackerszene bzw. aus deren Umfeld auf die Idee kamen, ihr „Hack-Know-how“ dem KGB anzubieten, gab es heftige Diskussionen, weil Geheimdienste eher konträr zur Förderung freier Information stehen. Aber auch Eingriffe in die Systeme fremder Betreiber werden zunehmend als kontraproduktiv erkannt.

Um den Schutz der Privatsphäre des Einzelnen mit der Förderung von Informationsfreiheit für Informationen, die die Öffentlichkeit betreffen, zu verbinden, wurde schließlich der bislang letzte Punkt angefügt.

Die Hackerethik befindet sich allerdings - genauso wie die übrige Welt - in ständiger Weiterentwicklung und Diskussion.

Im Rahmen des 15. Chaos Communication Congress (Berlin, 27. bis 29. 12. 1998) fand ein Workshop statt, der noch andere Aspekte hervorgebracht hat, die bisher noch nicht eingearbeitet wurden. Das dort diskutierte Modell teilt sich in die Kategorien „Glaube“ und „Moral“, das ja bereits in der Kirche einige Jahrhunderte erfolgreich praktiziert wurde. Glaube (z. B. an eine Verbesserung der Lage durch Förderung von Informationsfreiheit und Transparenz) steht - wie auch in der Kirche - vor Moral (z. B. an den Regeln, mit fremden Systemen sorgsam umzugehen).

Es heißt da: „Bevor wir jetzt allerdings anstreben, eine Kirche zu werden und dann auch gleich konsequenten Ablasshandel u. Ä. zu betreiben, überlegen wir uns das nochmal gründlich. Dabei dürfen natürlich alle mitdenken.“

## **6. Abschließende Gedanken**

Es ist eine bunte Welt, die sich dem auf den Wellen des Internets freibeuterisch bewegenden Hacker bietet. Ein Meer mit vielen Häfen tut sich ihm auf. Er betrachtet es als seine Kunst, auf verbotenen Wegen in diese Häfen zu gelangen und aus diesen jene Dinge zu holen, die ihn erfreuen. Ähnlich wie die alten Piraten ist auch der rebellische Hacker daran interessiert, den Frieden des braven Bürgers zu stören und ihn zu verunsichern. Hierin liegt seine Macht, aber auch seine Freude. Als Rebell vermag der Hacker aber auch Gutes, wenn er den Mächtigen dieser Welt vor Augen führt, wie zerbrechlich ihre Wahrheiten sind. Es ist noch viel zu erwarten von diesen neuen Hacker-Helden und Cracker-Verbrechern.

**Danksagung**

für Gespräche mit Herren der Computerszene, vor allem mit Herrn Ingenieur Karl Gängelmayer.

**Literatur**

Girtler, Roland (2003): **Randkulturen, Theorie der Unanständigkeit**. 4. Aufl. Wien: Böhlau.  
Levy, Steven (2001): Hackers. New York: Penguin.