HACKERLAND

http://kickme.to/tiger/

Hackerland

Denis Moschitto, geb. 1977, und **Evrim Sen,** geb. 1975, kennen sich seit der 6. Schulklasse, als sie beide von der Idee besessen waren, Mitglieder der (Hacker)-'Szene' zu werden. Von ihrem Taschengeld kauften sie sich zu diesem Zweck 1990 die ersten Modems, die damals noch völlig unbekannt waren und gründeten ihre eigene Mailbox 'Skywards', die in Köln und Umgebung berüchtigt war. Dadurch kamen sie schon im Alter von 13 und 15 Jahren in Kontakt mit legendären Szenegruppen wie 'Skid Row' und 'Paranoimia'. Später waren sie selbst als Musiker Mitglieder bekannter Gruppen wie 'Scoopex' und 'Shining-8'. Zur Zeit sind sie Mitglieder von 'Nuance', einer reinen Demogruppe, die nur im legalen Bereich der Szene agiert. Sie leben nach dem Motto 'Einmal Szene, immer Szene' als Schauspieler und Student in Köln, schreiben für ein Computermagazin und organisieren jährlich die Szene-Party 'Cologne Conference'.

Denis Moschitto / Evrim Sen

HACKERLAND

Das Logbuch der Szene

Die Hacker-Hymne

Chesire Catalyst

Zu singen nach der Melodie:

'Put another nickel in'

Put another password in,
Bomb it out and try again,
Try to get past logging in,
We're hacking, hacking, hacking.
Try his first wife's maiden name.
This is more than just a game.
It's real fun, it is the same,
It's hacking, hacking, hacking.
Sys-call, let's try a sys-call.
Remember the great bug from v3,
Or RSX, it's here! Whoppee!

Put another sys-call in,
Run those passwords out and then,
Dial back up, we're logging in,
We're hacking, hacking, hacking!

Softwarepiraterie

Mailboxsysteme

Der Phreaker

Die Szene und das Gesetz

Die Kunst des Hackens

Hauptsache Spaß

In Kontakt mit der Szene

Vorwort

Durch das stetig wachsende Interesse an Computern ist der Begriff 'Hacker' auch für Nicht-Computerbesitzer längst kein Fremdwort mehr. Berichte über Computerfreaks, die sich in Staatsbanken hacken und für die selbst die Supercomputer der Geheimdienste kein Hindernis mehr sind, klingen vertraut. Es gibt ausführliche Reportagen in Zeitung und Fernsehen, und schon des öfteren haben sich Filmemacher dieses Themas angenommen. Man hört von Fällen, in denen sich Hacker angeblich per Knopfdruck die Bankkonten bequem von zu Hause aus füllen und Telefonate auf Kosten ihrer ahnungslosen Nachbarn führen.

Vieles davon ist tatsächlich geschehen. Im letzten Jahrzehnt gab es kaum eine Grenze, die ein Hacker nicht übertreten hätte. Doch entsprechen Berichte über derartige Vorfälle nicht immer ganz der Wahrheit. Vieles ist Legende oder bewußte Fehlinformation, so daß die eigentliche Welt der Hacker im Verborgenen bleibt. Kaum jemand weiß etwa, daß viele Hacker Mitglied einer geheimen, aber nicht unbedingt kriminellen Organisation sind.

Bisher ist nur wenig über diese Organisation an die Öffentlichkeit gedrungen; zu geschickt wurde sie von ihren Mitgliedern getarnt. Hin und wieder melden sich vermeintliche Insider, schreiben Bücher mit Titeln wie 'Ein Hacker packt aus' und verdienen dabei ein kleines Vermögen. Doch war bis heute niemand imstande, ein wahrheitsgetreues Bild dieser Organisation zu zeichnen, die sich schlicht und einfach die 'Szene' nennt.

Der Begriff 'Szene' scheint für eine derartige Vereinigung gänzlich ungeeignet, aber über die Jahre hat er sich auch im Kreise ihrer Mitglieder etabliert. Sie selbst nennen sich auch 'Scene Members' oder 'Sceners' und gehören einem Zusammenschluß an, der nicht nur aus Hackern, sondern auch aus Geschäftsleuten und Softwareproduzenten besteht. Die Szene ist eine wohldefinierte Organisation. Es existieren Listen, in denen jedes Mitglied mit einem Pseudonym erfaßt ist.

Die Szene teilt sich in zwei Sektionen auf: die legale und die illegale Sektion. Der illegale Teil der Szene verbreitet Raubkopien und betreibt andere strafbare Aktivitäten, während sich die legale Szene auf die Produktion von Software spezialisiert hat. Da die legale Szene der illegalen entsprungen ist, gehören beide derselben Organisation an. Um jedoch die Grenze zwischen den Mitgliedern der beiden Sektionen zu markieren, haben sich viele Szenegruppen in zwei Teile gespalten, obwohl sie denselben Gruppennamen tragen. Die Kooperation zwischen den zwei Teilen bleibt aber weiterhin gewährleistet. Jedes Szenemitglied, ob von der legalen oder der illegalen Sektion, wird als volles Mitglied anerkannt.

Wer einmal Mitglied der Szene war, wird ihr nur schwer den Rücken zukehren können, und auch wir wollen es mit diesem Buch nicht tun. Sicherlich werden wir einigen Leuten auf die Füße treten, aber das ist bei einer derartigen Veröffentlichung unvermeidlich. Wirklichen Schaden kann man kaum anrichten, dafür ist die Szene zu gut organisiert.

Zum Schutz vor Außenstehenden wird in der Szene ein sich ständig ändernder Jargon benutzt. Da sprachliches Verstehen eine beiderseitige Übereinkunft voraussetzt, macht es die Szenesprache einem Laien völlig unmöglich, Einsicht in ihre Vorgänge zu gewinnen. Zum Teil existieren für verschiedene Begriffe der Szene im normalen Sprachgebrauch keine Pendants, was eine direkte Übersetzung von vornherein ausschließt. Wir haben in unserem Buch versucht, Vorgänge der Szene ohne Fachbegriffe anschaulich zu machen. Hilfe bietet auch ein ausführliches Lexikon mit Redewendungen und szenespezifischen Begriffen im Anhang.
Einige der in diesem Buch enthaltenen Informationen sind noch nie veröffentlicht worden und bedürfen zum Teil weiterer Beweise, die wir nicht erbringen wollen. Mehr, als mit unserem Namen für die Korrektheit der Informationen zu bürgen, können wir nicht. Ein Großteil unserer Informationen beruht auf Geschehnissen und Geheimnissen, die eigentlich nicht für die Öffentlichkeit bestimmt waren, an denen wir aber aufgrund unserer langjährigen Mitgliedschaft in der Szene teilhaben konnten.

Köln, Februar 1999

Denis Moschitto, Evrim Sen

Softwarepiraterie

Die ersten Raubkopierer

Wenn man sich mit Begriffen wie Softwarepiraterie oder Softwarekriminalität auseinandersetzen will, bedarf es eines kleinen Rückblicks auf die Anfänge des Computerzeitalters. Softwarekriminalität entstand zu einer Zeit, in der Computer noch riesige Maschinen waren, die mit Lochkarten als Datenträgem gefüttert wurden. Eine Szene in der organisierten Form wie heute gab es damals noch nicht. Meist waren es Einzelgänger in kleineren Firmen, die Software klauten oder manipulierten. Von diesen gingen wohl auch die ersten Hackversuche in fremde Computersysteme aus, um beispielsweise an neue Softwareprodukte zu gelangen: Industriespionage auf EDV-Ebene. Manche erinnern sich bestimmt noch an Walt Disneys legendären Film 'Tron', in dem ein bösartiger Geschäftsführer Software von einem jungen, nichtsahnenden Computerprogrammierer stiehlt, um damit selbst auf den Markt zu kommen.

Richtig begonnen hat die Softwarepiraterie Anfang der 80er Jahre mit dem ersten Videospieleboom in den Vereinigten Staaten. In den Anfängen des neuen Computerspiel-Zeitalters bildeten sich Gruppen, die auf elektronischem Gebiet gezielt rechtswidrig aktiv wurden. Als dann die ersten Spielautomaten in Computerform Einzug in die privaten Haushalte fanden, brach das Zeitalter der Heimcomputer an. Nutzer der ersten Stunde werden sich an den weltweit verbreiteten Commodore 64 **(C64)** erinnern, der sich damals als meistverkaufter Computer zur Nummer Eins entwickelte. Der C64 war einer der ersten Computer, der trotz seiner Effizienz einigermaßen preiswert war.

Zu dieser Zeit hatte sich bereits ein Markt für Computerspiele etabliert. Private Benutzer konnten ihre Software von Softwareanbietern legal erstehen. Aber auch hier gab es schwarze Schafe unter den Anwendern. Einige Benutzer stellten Kopien dieser oftmals sehr teuren Datenträger her. Das war nicht sonderlich schwer, unterschied doch nur der Name 'Datasette' den Datenträger von einer herkömmlichen Musikkassette. Der Raubkopierer sparte durch die Kopie das Geld, das er für ein oft überteuertes Original ausgegeben hätte. Mit dem flächendeckenden Vertrieb von Computersoftware begann auch das Zeitalter der Raubkopierer. Die Softwareunternehmen beklagen seit jeher die angeblichen Schäden, die ihnen durch Softwarepiraten entstanden seien.

Softwarefirmen begannen sich bald gegen die ständig größer werdende Zahl der Raubkopierer zur Wehr zu setzen. Sie beauftragten und beauftragen noch heute Patentämter und Rechtsanwälte, Softwarepiraten Einhalt zu gebieten. Die Vorgehensweise der Ermittler in solchen Fällen wird später in diesem Buch näher behandelt werden.

Auch suchten die Programmierer nach besseren Wegen, um die damals noch unorganisierten und einzeln agierenden Raubkopierer zu stoppen. Sie bauten mit Hilfe komplexer Programmroutinen einen Kopierschutz in ihre Spiele ein. Damit wollten die Programmierer zumindest den gemeinen Raubkopierer daran hindern, Software zu vervielfältigen. Doch konnten sie zu dieser Zeit noch nicht vorausahnen, daß genau diese Maßnahme eine neue Ära des organisierten Computerverbrechens einleiten sollte.

Einige Softwarepiraten, die zunächst als Einzelgänger auftraten, fingen an, hobbymäßig Software zu **cracken,** also den Kopierschutz zu entfernen. Nachdem sie dann ein Programm **(Prog)** gecrackt hatten, gaben sie das Softwareprodukt an Raubkopierer weiter. Oft waren das Leute aus dem eigenen Freundeskreis. Später bildeten sich kleinere Gruppen, die es sich zur Aufgabe machten, Software kontinuierlich zu cracken und in Umlauf zu bringen. Die ersten **Cracker**gruppen**,** die so etwas schafften, versahen das Softwareprodukt mit ihrem Gruppennamen und sorgten für flächendeckende Verbreitung.

Es dauerte nicht lange, bis sich schließlich alle Crackergruppen vereinten. Ziel dieses Bündnisses war es, eine internationale, im Untergrund operierende illegale Organisation zu bilden, die in nur wenigen Jahren ein gigantisches Netz quer über den Globus spannen sollte. Gruppen- und Mitgliedernamen wurden in Listen festgehalten und weltweit durch Personen, die speziell für diesen Aufgabenbereich eingeteilt waren, verteilt. Computerfreaks

und Hacker aus aller Welt erkannten die Vorzüge einer Mitgliedschaft und traten den ersten Szenegruppen bei, um bei dieser neuen illegalen Vereinigung aktiv mitzuwirken. Das weltweite Netz steckte zwar noch in den Kinderschuhen, doch das Fundament stand. Obwohl die Entstehung dieser Clique ursprünglich den Crackern zu verdanken war, kamen nun viele andere Aufgaben auf jedes Mitglied dieses einzigartigen Kollektivs zu. Die 'Szene' war geboren.

Der Cracker

Heute gibt es Hunderte von illegalen Gruppen in der Szene, die kopiergeschützte Software cracken und verbreiten. Je besser der Kopierschutz in einem Programm ist, desto schwieriger wird es für einen Cracken dies zu entschlüsseln. Die Gruppen der Szene, die sich speziell dem Cracken von Software gewidmet haben, brauchen einen Lieferanten. Dieser wird in ihren Kreisen **Supplier** genannt.

Ein Supplier ist jemand, der für seine Gruppe Originalsoftware beschafft, oft noch bevor sie auf den Markt kommt. Große Crackergruppen haben durch Kontakte und finanzielle Mittel häufig einen Supplier direkt in den Softwarefirmen selbst. Dies sind Angestellte in den unterschiedlichsten Positionen, die die Software noch während der Entwicklungsphase vom Arbeitstisch stehlen, um sie an Cracker weiterzuleiten. Derartige Dienste werden natürlich honoriert und sind für den Supplier äußerst rentabel. Bei großen Softwarefirmen mit Hunderten von Mitarbeitern scheint es so gut wie unmöglich, einen Spion dingfest zu machen. Wirklich kompliziert wird die Angelegenheit dann, wenn Firmenbosse selbst einmal in der Szene waren und Software an ihre ehemalige Crackergruppe weitergeben. Wie auch immer ein Softwareprodukt in die Szene gelangt, eines ist sicher: Software wird so oder so, früher oder später und unabhängig von der Art des Produktes gecrackt und als Raubkopie **(NONPD)** in Umlauf gebracht. Dies kann niemand verhindern.

Auch kleinere Softwarefirmen, deren Mitarbeiter nicht unbedingt in Kontakt mit der Szene stehen, weisen Sicherheitslücken auf, durch die Software in die Hände von Crackergruppen fällt. Eine für die Szene ganz wichtige Schwachstelle bilden die sogenannten Betatester. Software, die sich noch in der Entwicklungsphase befindet, muß verständlicherweise vor ihrer Veröffentlichung getestet werden. Für solche Aufgaben werden die unveröffentlichten Programme an Betatester weitergeleitet, welche die Software nach Fehlern untersuchen und überprüfen. Betatester sind meist ganz gewöhnliche Benutzer, die in einem freien Arbeitsverhältnis mit den Softwareproduzenten stehen. Und tatsächlich gibt es immer wieder Testen die das in sie gesetzte Vertrauen mißbrauchen und noch nicht fertiggestellte Produkt an eine Crackergruppe weitergeben oder verkaufen.

Eine weitere Schwachstelle bilden die Medien. Eine Softwarefirma muß, wenn sie mit ihrem Produkt erfolgreich sein will, vor der Veröffentlichung stehende Software an verschiedene Pressestellen senden, um ihr schon vor dem Erscheinungstermin verkaufsträchtige Besprechungen zu sichern. Die Mitarbeiter einer Computerzeitschrift bekommen auf diesem Wege schon im Vorfeld Softwareprogramme verschiedenster Art zu sehen, lange bevor der Privatanwender die Möglichkeit hat, das Produkt zu kaufen. Auch hier, wie sollte es anders sein, haben Crackergruppen ihre Kontakte und erhalten vom Praktikanten bis zum Chefredakteur unveröffentlichte Software aller Kategorien.

Crackergruppen sind meist sehr gut organisiert und arbeiten systematisch. In einer Crackergruppe gibt es Mitglieder, die verschiedenen Aufgabenbereichen **(Sections)** zugeteilt sind. Der Leiter **(Leader)** der Gruppe kennt Supplier, ohne die eine Crackergruppe in der Szene nicht erfolgreich sein kann. Zu den Aufgaben eines Leiters gehört es auch, zu bestimmen, wer der Gruppe beitreten darf **(join)** und wer sie wieder verlassen muß **(kick).** Der sogenannte **Trader** in der Gruppe sorgt für die weltweite Verbreitung der Software. Er hat internationale Beziehungen zu Szenemailboxen **(Boards),** zu denen er täglichen Kontakt pflegt, um gecrackte Software zu verteilen. Der Telefonhacker **(Phreaker)** beliefert den 'Tader mit für ihn wichtigen Daten und Arbeitsmaterial. Die Versorgung reicht von gestohlenen Calling-Card-Nummern bis hin zu Kreditkarten, damit die Verbreitung der Software reibungslos und vor allem kostenfrei erfolgen kann. Der Musiker produziert dann die Computermusik **(Cracktune)** für einen von der Crackergruppe angefertigten Vorspann **(Cracktro),** der von einem Programmierer **(Coder)** ausgeführt wird. Der Vorspann erscheint vor jedem gecrackten Programm und präsentiert den Namen der Crackergruppe. Ist beispielsweise ein raubkopiertes Spiel, das man an seinem Computer startet, von einer Gruppe namens 'Shining-8' gecrackt worden, erscheint beim Start auf dem Bildschirm die Meldung: 'Cracked by Shining-8'.

Es gibt Szenegruppen und Szenemitglieder **(Scener),** die weltweit bekannt wurden. Das liegt zum Teil daran,

daß ihre gecrackte Software in fast jedem Land der Welt zu finden ist. Das Cracken von Programmen ist in der Szene zu einem routinierten Vorgang geworden und wird permanent betrieben. Um die Gruppe oder den eigenen Namen bekannt zu machen, kann die Veröffentlichung von Raubkopien äußerst hilfreich sein, jedoch ist dies nicht einfach. Jeder Cracker bringt daher langjährige Programmiererfahrung mit, die ohne eine gewisse programmiertechnische Kreativität nicht wirklich von Nutzen wäre.

Hand in Hand: Softwarefirmen und Raubkopierer

In der Regel ist die Szene selbst nicht sonderlich daran interessiert, welche Software sie crackt, solange diese als Neuheit in Insiderkreisen für Aufmerksamkeit sorgt und funktioniert. Viele Programme wurden in den vergangenen Jahren gestohlen, gecrackt und anschließend in Umlauf gebracht, ohne daß auch nur ein einziges Szenemitglied sie genutzt hätte. Die Szene sieht sich nun einmal nicht als Verbraucher. Aus diesem Grund ist es ihr egal, ob nun jemand das gecrackte Programm wirklich benötigt oder ob es etwas taugt. Denn gecrackte Software dient in erster Linie als Werbewand für den eigenen Namen.

Einige Softwarefirmen mit Szenewissen nutzten dies und schlossen geheime Deals mit verschiedenen Gruppen ab, um die Szene auf eine falsche Fährte zu locken. Das Angebot klang für Eingeweihte völlig verrückt, aber dennoch verlockend: Die angesprochenen Gruppen bekamen von den Herstellern die 'neueste Software'; diese sollte gecrackt und möglichst gezielt in der Szene verbreitet werden - und das auch noch für Geld. Das ganze schien zunächst sinnlos, da sich die Softwarefirmen damit offensichtlich selbst schadeten.

Selbstverständlich war dem nicht so. Bei den Softwareprodukten, die in die Szene geschleust wurden, handelte es sich häufig um gefälschte oder stark fehlerhafte Versionen des Originals, die zum Teil nicht funktionierten **(Fakes).** Die Idee, die hinter dieser Aktion steckte, basiert auf einem alten Szenekodex. Es ist ein ungeschriebenes Szenegesetz, daß kein Programm zweimal gecrackt werden darf **(Dupe).** Die Gruppe, die es als erste schafft, ein Softwareprodukt zu cracken, erntet den Ruhm, und die Software wird damit schlagartig für jede andere Szenegruppe uninteressant. Da sich in der Szene allerdings kaum jemand wirklich um den Inhalt einer Software kümmert, verging einige Zeit, bis man den Schwindel bemerkte. Damit blieb der Softwarefirma genügend Zeit, ihr Produkt ohne Druck durch Raubkopierer auf den Markt zu bringen.

Software kontrolliert an Raubkopierer zu verteilen, kann für eine Softwarefirma noch weiteren Nutzen haben. Denn ein schlechtes Computerspiel, das auf dem Markt keine Chancen hat, kann durch die Szene über die ganze Welt verteilt werden. Da Szeneleute keine Softwarekritiker sind, wird das Programm keine inhaltliche Kritik in der Szene selbst hervorrufen. Doch der Name der Softwarefirma wird auf diesem Weg ohne eigenes Zutun weltweit bekannt. Was könnte sich eine Firma mehr wünschen als Imagewerbung, die kostenlos und darüber hinaus noch zuverlässig ist? So einfach wird aus einer weltweiten kriminellen Vereinigung die größte Litfaßsäule der Welt.

Derartige Fälle haben Crackergruppen in der Vergangenheit in Verruf gebracht. Die bloße Anschuldigung, mit einer Softwarefirma unter einer Decke zu stecken, konnte große Crackergnzppen zerstören. So gab es Gerüchte, daß eine Gruppe dem Hersteller Factor 5 versprochen hatte, Software nur in fehlerhaften Versionen in Umlauf zu bringen. Dafür bekam die Gruppe dann die Software vor dem eigentlichen Erscheinungstermin. Oft werden solche Gruppen auch heute noch geächtet, ihnen werden kommerzielle Absichten vorgeworfen. Die Mitglieder werden aus Szenemailboxen verbannt und Phreaker bieten ihnen keine Unterstützung mehr an. In manchen Fällen geht es sogar so weit, daß eine ausgestoßene Gruppe, die versucht, mit guten Raubkopieangeboten erneut Anschluß an die Szene zu finden, von dieser an die Polizei verraten wird.

Um sich vor Mißverständnissen und gefälschten Raubkopien zu schützen, wird heute nahezu jedes Softwareprodukt, das vor dem Erscheinungstermin in der Szene zu haben ist, am Tag der Veröffentlichung in der neuen Version ein zweites Mal gecrackt.

Der Schwarzhandel mit CDs

Wer allerdings glaubt, daß alle Mitglieder der illegalen Szene nur ihr Hobby ausleben wollen, der irrt. Einige Leute in der Szene haben einen guten Geschäftssinn. Viele Softwareprogramme, die gecrackt werden, sind zum Verkauf bestimmt. Teure Programme werden auf CDs gepreßt und von der Szene günstiger angeboten. Die von der Szene zusammengestellten CD-Pakete kosten nur einen Bruchteil der Originalsoftware, deren Preis sich beim Kauf im Fachhandel auf mehrere tausend Mark belaufen würde.

Die Szene macht durch diesen Verkauf von illegal hergestellten CDs einen riesigen Profit. Die dabei erzielten Gewinne liegen im fünfstelligen Bereich. Mehrere gecrackte Programme werden auf eine CD gepackt und in großer Anzahl, häufig bis zu dreißigtausend Stück pro Auflage, gepreßt. Frisch aus den Preßanlagen der CD-Massenproduktion werden dann bis zu tausend CDs an den ersten Zwischenhändler verkauft. Der wiederum gibt die Ware an den nächsten Kunden für bis zu vierzig Mark pro Exemplar weiter, meist in kleineren Mengen zwischen dreißig und dreihundert Stück. Dieser liefert dann die CDs an den Endverbraucher, der für ein professionell gepreßtes Stück bis zu hundert Mark ausgibt.

Alle Programme, die sich auf einer solchen CD befinden, sind 'cracked and registered', das heißt, daß die Software in Form von Vollversionen vorliegt, sofort installierbar und ohne Einschränkungen nutzbar ist. Die polizeilichen Ermittlungen in diesem Bereich sind sehr schwierig, denn illegal gepreßte CDs sehen wie kommerzielle Produkte aus. Darüber hinaus haben diese CDs keine Seriennummer, und so wird es fast unmöglich, ihre genaue Herkunft zu bestimmen. Die meisten Schwarz-CDs werden in Holland gepreßt. Dort gibt es Massenanfertiger, die für ein paar Mark mehr nicht so genau darauf achten, was sie pressen und auch mal gerne auf die Seriennummer verzichten. Die fertigen CDs werden per PKW risikolos von Holland nach Österreich geliefert und von dort aus unter anderem nach Deutschland versandt. Bestellungen dieser CDs laufen über den gewöhnlichen Postweg. Kleinere Stückzahlen (bis hundert CDs) werden sicher verpackt per Nachnahme an den Empfänger gesendet. je nach Vereinbarung können größere Stückzahlen auch persönlich abgeholt werden. Wenn man als Mitglied der Szene die richtigen Beziehungen hat, ist es leicht, an raubkopierte CDs heranzukommen.

Die eigentlichen Köpfe der CD-Piraten sind Leiter der Szenegruppen, die schon an den Anfängen der Szene ihre ersten illegalen Geschäfte abgewickelt haben. Wenn man tiefer in die Szene involviert ist, laufen einem solche Leute ständig über den Weg. Man trifft sie bei Freunden oder auf Szeneveranstaltungen jeglicher Art. Die Namen derer, die durch ihre illegalen Tätigkeiten bekannt wurden, werden in der Szene mit großem Respekt genannt. Für jemanden mit den nötigen Referenzen **(Ref**s) ist es nicht sonderlich schwer, in das boomende CD-Geschäft einzusteigen. Andere müssen sich jedoch gegen eine Mauer der Arroganz durchsetzen, die bisher nur wenige durchbrochen haben. Denn die richtige **Elite** der Szene gibt sich nicht mit Neulingen **(Lamer)** ab - schon gar nicht mit denen, die die alten Werte der Szene nicht kennen und respektieren.

Raubkopien im Internet

Das Internet bietet neben vielen mittlerweile bekannt gewordenen Angeboten wie dem 'World Wide Web' (WWW) oder dem 'File Transfer Prototoll' (FTP) noch eine weitere Offerte: Das Tnternet Relay Chat' **(IRC).**

Das IRC bietet dem Internetnutzer auf hunderten von Kanälen die Möglichkeit, mit Benutzern aus aller Welt 'live via Tastatur' zu kommunizieren. Auch die Szene nutzt diesen Service des Internets und hat eigene Chatkanäle eingerichtet, in denen sich die Mitglieder ungestört miteinander unterhalten können. Was viele nicht wissen, ist, daß der Datentransfer über IRC genauso möglich ist wie über FTP oder WWW.

Der Austausch von Daten zwischen zwei Benutzern in einem der Chatkanäle erfolgt durch das Internetprotokoll DCC. Wenn die Internetprogramme zweier Nutzer DCC-fähig sind, kann der eine dem anderen eine Datei schicken, ohne daß ein Außenstehender etwas davon mitbekommt. Das liegt daran, daß die DCC-Verbindung nur zwischen diesen beiden Benutzern besteht. Selbst ein zugriffsberechtigter Administrator könnte diesen Transfer nicht mitverfolgen. Anders als bei Telefongesprächen ist ein Mitschnitt dieser Übertragung nicht möglich. Sobald sich jemand in diese Übertragung einmischen würde, hätte dies eine Verbindungsstörung zur Folge. Die Szene hat hier also absolut freie Hand, ihre Waren ohne große Umwege an den Mann zu bringen. Und dies, anders als bei statischen Mailboxen oder Boards, völlig ohne Risiko.

Wie bereits erwähnt, kennt man sich in der Szene untereinander und weiß, mit wem man Ware tauschen kann und mit wem besser nicht. Zwielichtige Personen werden, wie in den Szenemailboxen, sofort aus dem Kanal geworfen oder sogar verbannt. Bei einer Verbannung aus einem Kanal wird immer ein Grund angegeben, der dann einfach lautet: 'Wir haben nie etwas von Dir gehört', oder 'Komm wieder, wenn Du einen Namen hast'. Betritt jedoch ein bekannter Trader den Chatkanal, also jemand, der in der Szene durch die Verbreitung von Raubkopien Ruhm erlangt hat, wird er freundlich begrüßt und in die Runde aufgenommen.

Im Grunde beruht der Tausch von Raubkopien auf Gegenseitigkeit. Nicht die Größe einer Datei ist ausschlaggebend, sondern nur die Datei selbst. Für jede gesendete Datei **(Upload)** kann man eine andere herunterladen **(Download).** Stimmt die Qualität der Datei, wird der Vorgang wiederholt. Sobald einer der Empfänger feststellt, daß sein Gegenüber keine vernünftige Ware gesendet hat, wird der jeweilige Übeltäter entweder aus dem Kanal verbannt oder mit Internethacks, sogenannten 'Scripts'*, aus seiner Verbindung herauskatapultiert.

Allgemeine Anfragen nach bestimmter Software sind zugelassen. Es ist üblich, daß derjenige, der nach einem Softwareprodukt sucht, frei in die Runde fragen darf. Ist er beispielsweise auf der Suche nach einer raubkopierten Version von Windows, so stellt er die öffentliche und damit für alle Anwesenden lesbare Frage: 'Lookin' 4 Windowz sb help me plz' (Ich suche Windows, wer kann mir bitte helfen?) und muß nur noch abwarten. Entweder jemand schreibt ihn an und kommt seinem Wunsch entgegen, oder der Benutzer muß seine Anfrage einige Zeit später wiederholen. Eine wichtige Verhaltensregel ist dabei, nicht unnötig lästig zu werden, indem man den Chatkanal durch ständige Anfragen nach Software belastet.

Manchmal kommt es auch vor, daß man sich völlig überraschend in einem Gespräch mit einer anderen Person befindet und über alles mögliche ausgefragt wird. Dieses Frage- und Antwortspiel, auch 'Wordswapping' genannt, ist schon aus den Szenemailboxen bekannt und dient zur Abschreckung von Außenseitern. Häufig wird nach

Referenzen gefragt, und daher kann so etwas für Nicht-Mitglieder der Szene unangenehm werden. Da es oft zu Besuchen von Außenseitern kommt, ist die Szene sehr vorsichtig. Falls sich jemand als Lügner entpuppt und nicht der Szene angehört, wird er ebenfalls aus dem Chatkanal geworfen und auf eine Ignorier-Liste gesetzt. Danach kann er nie wieder jemanden aus dem Kanal ansprechen.

Wer seinen Internetzugriff riskieren und in einen der bekannten Szene-Chatkanäle hineinschnuppern möchte, kann der illegalen Szene mit einem IRC-Programm über den folgenden Server einen Besuch abstatten: **irc.funet.fi (#amielite, #warez).**

Manchmal kommt es auch vor, daß sich ein Mitglied der legalen Szene auf der Suche nach Software befindet und in einen der illegalen Chatkanäle der Szene hineinplatzt. Ihm wird in der Regel ohne Gegenleistung geholfen. Die illegale Szene weiß, daß jemand aus der legalen Szene kein Cracker oderTrader sein kann und somit keinen Handel mit Raubkopien betreibt. Doch ist es üblich, die legale Szene zu unterstützen und jeden Suchenden zuvorkommend mit Software zu versorgen. Schließlich ist ein legales Szenemitglied auch ein wichtiges Mitglied der Familie.

Scripts: Der IRC-Zugriff (Chatkanäle) im Internet findet meist unter den Betriebssystemen Unix, Linux oder Solaris statt. Im IRC hat man nur begrenzte Funktionen zur Verfügung. Einige Benutzer haben jedoch direkten Zugriff auf das Betriebssystem und steuern IRC-Funktionen von dort. Dieser Zugriff auf das Betriebssystem kann mit einem einfachen Script erfolgen, den einige Benutzer unter dem Betriebssystem des Anbieters starten können. Diese Scripts sind in der Regel verboten und werden, falls möglich, von den Administratoren abgefangen. Einige Scripts können das System bremsen, komplizierte Hackscripts können Provider sogar komplett zum Absturz bringen. Scripts werden von Unix-Fachleuten programmiert. Viele sind daher auch in der Szene in Umlauf und dienen unter anderem dazu, Benutzer aus dem Intemet zu werfen oder auf andere Art Systeme oder Benutzerzugriffe zu zerstören.

'The Chaos versus Order War' has been
raging on, ever since Time first got it on
with Space and created the Universe.

The KLF (Kopyright Liberation Front)

Mailboxsysteme

Was ist *eine* Mailbox?

Das Wort **Mailbox** ist den meisten Computeranwendern mittlerweile geläufig. Eine Mailbox ist im Prinzip nichts anderes als ein privates oder kommerzielles System, das Nachrichten speichert und den Zugriff von außerhalb ermöglicht. Auch der Anrufbeantworter eines Mobiltelefons wird daher Mailbox genannt. Auf der Computerebene versteht man unter dem Begriff Mailbox ein Computersystem, das den Zugriff auf interne Daten von außerhalb mit Hilfe eines **Modems** ermöglicht.

Neben unzähligen Privatanwendern eröffneten Anfang der 9oer Jahre auch renommierte Firmen kommerzielle Mailboxen und boten sie ihren Kunden als freie Informationsquellen an. So bestand beispielsweise mit dem Modem die Möglichkeit, bequem von zu Hause aus an Updates von Software oder Installations- und Hilfsprogramme heranzukommen und sich damit den Weg zum Händler zu ersparen. Mit der zunehmenden Verbreitung des Internets und der Websites (WWW) haben die Besucherzahlen kommerzieller Mailboxen nachgelassen. Dennoch sind viele weiterhin in Betrieb. Anders als in den kommerziellen Mailboxen von Firmen kann man sich in öffentlichen Mailboxen, die auch von Privatpersonen angeboten werden, an Diskussionsrunden über Themen aller denkbaren Bereiche beteiligen. Hier steht das Gespräch mit den anderen Systembenutzern im Vordergrund.

Szenemitglieder geben sich mit öffentlichen Mailboxen in der Regel nicht zufrieden. In einer öffentlichen Mailbox wird man dementsprechend nur höchst selten ein Szenemitglied antreffen. Die gewöhnliche Computergemeinde ist für ein Szenemitglied uninteressant und vor allem auch unter seinem vermeintlichen Niveau. Die Szene hat für ihre Zwecke eigene Mailboxsysteme geschaffen, die nur Mitgliedern den Zugang ermöglichen: das **Bulletin Board System,** abgekürzt **BBS** - von der Szene einfach nur als 'Board' bezeichnet.

Illegal pur: Boards

Die Szene selbst nutzt Mailboxen hauptsächlich zur weltweiten Verbreitung von Raubkopien. Die bekanntesten und am meisten verwendeten Mailboxprogramme in der Szene sind **Ami-Express (/X)** und **Farne.** Diese Programme sind ausschließlich zur Handhabung von Software entwickelt worden und unterscheiden sich daher im Aufbau stark von gewöhnlichen Mailboxprogrammen. Eine Szenemailbox bedient sich weder einer leichten Menüführung noch einer standardisierten Benutzeroberfläche, wie man es von einem herkömmlichen Mailboxsystem gewohnt ist. Zusätzlich verwirrt ein Board szeneunerfahrene Besucher durch seinen höchst komplexen Aufbau, und auch von seiten des Systembetreibers **(Sysop)** wird meist jegliche Hilfestellung unterlassen.

Auf diese Weise versuchen Besitzer von Boards, Außenstehenden, die es trotz aller Sicherheitsvorkehrungen geschafft haben, in das System zu gelangen, die Benutzung unmöglich zu machen. Selbst der kleinste Eingabefehler kann zur unverzüglichen Verbindungsunterbrechung führen, und der Besuch endet so schnell, wie er begonnen hat. Boards sind so aufgebaut, daß interne Diskussionen nicht direkt möglich sind. Schließlich ist ein Board keine Anlaufstelle für hilfsbedürftige Computerneueinsteiger, vielmehr gilt hier die Devise: 'Raubkopien tauschen, was das Zeug hält'.

Wettrennen um Raubkopien

Szenemitglieder selbst werden in den Boards nur solange geduldet, wie sie neue Software **(Warez)** senden können. Für ein neues Board ist es von enormer Wichtigkeit, Anerkennung in der Szene zu gewinnen. Bis es sich vollständig etabliert und einen Namen gemacht hat, dem man mit Respekt begegnet, kann viel Zeit vergehen. Der Weg zu diesem Ziel ist für die Systembetreiber steinig und gefährlich.

Wenn die Szene über ein Board spricht, wird häufig das englische Wort **fast** (zu deutsch: 'schnell') als Bewertung für die Qualität des Boards benutzt. Unter einem schnellen Board versteht man ein System, das in kürzester Zeit Software-Neuerscheinungen im eigenen Sortiment anbieten kann. Für besonders schnelle, also gute Boards, ist es üblich, daß Software bereits am Tag der offiziellen Erscheinung als gecrackte Version erhältlich ist. Im Szenejargon nennt man dies **0-Day-Warez,** was heißt, daß der Crack noch keinen Tag alt ist.

Da der Zugriff **(axs)** auf ein Board über mehrere Leitungen **(Nodes)** läuft, wird die Software mit immenser Geschwindigkeit von einem Board zum anderen verbreitet. So ist es nicht unüblich, daß ein Softwareprodukt am Tag der Neuerscheinung schon gegen Mittag gecrackt und am Abend in allen Boards der Welt verfügbar ist. Das Datum des Cracks gibt an, welche Software alt und welche neu ist. Meist ist das Erscheinen des Cracks zeitgleich mit dem Erscheinen der Software auf dem offiziellen Markt. Oft kann man sogar beobachten, daß Software durch die Szene verbreitet wird, noch bevor sie auf den Markt kommt. Ein Spruch in der Szene besagt, daß die erste Raubkopie dem Original vorausging.

Jedes Szenemitglied in einem Board ist dazu verpflichtet, in regelmäßigen Abständen neue Ware in Form von gecrackter Software zu liefern. Ist dem Mitglied des Boards der Zugang (**acc**) wichtig, wird es sich in jedem Fall an diese Regel halten. Die Belieferung eines Boards wird belohnt. Jeder, der aktuelle Software sendet, kann sich dafür den entsprechenden Teil aus dem Board zurücknehmen. Wer 'alte' Software verschickt, was bedeutet, daß das Produkt erst 24 Stunden nach der Szene-Veröffentlichung (**Major, Release**) geliefert worden ist, den kann ein besonders strenger Systembetreiber durchaus mit sofortiger Verbannung aus dem System bestrafen.

Interne Angelegenheiten

Neben der Distribution von Raubkopien haben Boards noch eine weitere essentielle Aufgabe: die Verbreitung von internen Szeneinformationen durch die sogenannten **Infofiles.** Diese Infofiles können sowohl Texte als auch Bilder enthalten, die nur für die Szene bestimmt sind. Ein Board bietet die ideale Oberfläche für derartige Insider-Informationen. Durch die in einem Board herrschenden strengen Kontrollen ist gewährleistet, daß nur die Personen an Szeneinformationen gelangen, die auch zur Szene gehören. So werden beispielsweise detaillierte Angaben über Personen, die der Szene feindlich gesonnen sind, in nur wenigen Stunden über die ganze Welt gestreut, ohne daß Außenstehende etwas davon mitbekommen.

Infofiles enthalten darüber hinaus vermischte Informationen über Mitglieder von legalen und illegalen Gruppen der Szene. Jede Mitgliedsänderung innerhalb einer der Szene bekannten Gruppe wird, scheint sie auch noch so unwichtig, in den Infofiles vermerkt. Die Leiter der Szenegruppen sehen so beispielsweise, welche Szenemitglieder eine Gruppe verlassen haben und können diese dann für die eigene Gruppe oder bestimmte Projekte anwerben.

Der Systembetreiber eines Boards ist in der Regel selbst Mitglied einer Szenegruppe und führt das Board im Namen seines Teams. Je nach Popularität und Größe des Boards wird es von einer Gruppe als World, European, oder einfach nur als Local **Headquarter** (Hauptquartier) genutzt. Im Headquarter können Mitglieder einer Gruppe virtuelle Konferenzräume **(Conferences)** als Treff- und Sammelpunkte nutzen, die nur für die eigene Gruppe bestimmt und zugänglich sind. Selbstverständlich ermöglicht der Systembetreiber eines Boards den Mitgliedern der eigenen Gruppe einen privilegierten Zugriff auf sein System.

Die absolute Elite

Obwohl Boards eindeutig der illegalen Szene zuzuordnen sind, findet man dort auch hin und wieder Angehörige des legalen Arms, die sich für kurze Zeit der weißen Weste entledigen, um die eigene Softwaresammlung aufzufrischen. Diese Kurzbesucher werden von den Systembetreibern meist ohne Gegenleistungen geduldet, dies hängt jedoch immer vom jeweiligen Systembetreiber und dessen Stimmung ab.

In jedem Fall sind es die Trader, die Tauschhändler der Szene, die dafür Sorge tragen müssen, daß ein Board schnellstmöglich mit der neuesten Software versorgt wird. Abgesehen von dieser Tätigkeit sind sie dazu verpflichtet, neue Produkte der eigenen Gruppe zu verbreiten. Da bei vielen Gruppierungen die Grenzen von Legalität und Illegalität fließend sind, kann neben der Verbreitung von Infofiles und Cracks genausogut der Vertrieb legaler Eigenproduktionen zum Aufgabenbereich eines Traders gehören. Oft werden Trader auch schlicht und einfach damit beauftragt, gezielt nach Software Ausschau zu halten, wenn diese im Rahmen der eigenen Gruppe oder für eine einzelne Person notwendig geworden ist.

Der Job des Traders zählt in der Szene zu den riskantesten überhaupt. Ein durchschnittlich erfolgreicher Trader ist meist weltweit in Boards aktiv. Dadurch entsteht für ihn das Risiko, daß sein Name eines Tages bei einer Hausdurchsuchung auf der Mitgliederliste eines hochgenommenen Boards auftaucht. Außerdem müssen Trader mit astronomisch hohen Telefongebühren rechnen, die durch die ständigen Anrufe rund um den Globus anfallen. Um Kosten zu sparen, sind Trader auf die Phreaker angewiesen. Ein Phreaker versorgt Trader mit gestohlenen Calling-Card-Nummern und sucht ständig nach neuen Methoden kostenfrei zu telefonieren (» 3. Eintrag) Hierbei sind beide, sowohl Phreaker als auch Trader, dem hohen Risiko ausgesetzt, von der Polizei entdeckt zu werden. Diese Szenemitglieder verkörpern das organisierte Computerverbrechen in seiner höchsten Form und bezeichnen sich daher in der Board-Gemeinde als die absolute und unantastbare Elite. Jeder, der nicht einen bestimmten Bekanntheitsgrad innerhalb der Szene erlangt hat, wird von der Elite zu einem Unbekannten, ja sogar zu einem Niemand erklärt. Eine gewisse Arroganz kann man dieser Haltung nicht absprechen.
Zugleich bildet dieses Verhalten jedoch einen Schutzwall, der für einen Elite-Systembetreiber unverzichtbar ist. Wenn man sich den Aufwand und die Kosten, ein Board zu führen, bewußt macht, wird der Druck, unter dem die Betreiber stehen, nachvollziehbar. Ein gutes Beispiel dafür war 'Philtrust', der Betreiber der 'New Central Europe', der wegen der Größe seines Boardes ständig damit leben mußte, daß ihm die Polizei auf die Schliche kommt. Daher zog er in Nürnberg unzählige Male mit seinem Board um, und nahm den ständigen Transport seines Equipments in Kauf. Nur so blieb er von einer Konfrontation mit den Hütern des Gesetzes verschont. Er schloß die Pforten von 'New Central Europe' erst, als ihm die Lust umzuziehen verging.

Systembetreiber der selbsternannten Elite verbannen Mitglieder der Szene oft auf unverschämteste Weise aus ihren Boards, wenn diese nicht ausreichend Erfahrung und Kompetenz in Sachen Piraterie mitbringen. Selbst bei Mißverständnissen und eigenen Fehlern gibt es für viele Systembetreiber keine Diskussion. Wer einmal aus einem Board verbannt wurde, kann diesem nie wieder beitreten.

Wie wird man Mitglied?

Die Telefonnummer eines Boards wird von den Mitgliedern und dem Systembetreiber geheimgehalten. Normalerweise werden solche Telefonnummern nur an Gruppen- und Szenemitglieder weitergegeben, die man persönlich kennt. Viele Systembetreiber lassen überdies noch die Nummern ihres Boards von der Telefongesellschaft in regelmäßigen Abständen ändern. Hat man über Beziehungen die aktuelle Telefonnummer eines Boards bekommen, kann man sich mit einem handelsüblichen Modem einwählen. Dort wartet aber auch schon das erste Hindernis auf den Besucher: denn der Eintritt in ein Board ist insofern es kein gesperrtes System **(closed System)** ist und einen Neueintrag erlaubt - nur durch die korrekte Eingabe eines Systempaßworts **(SYSPW)** möglich, das vom Systemleiter innerhalb von kurzen Zeitabständen geändert wird. Die Abfrage des Systempaßworts erfolgt sofort nach dem Aufbau der Verbindung zu einem Board. Bei dreimaliger falscher Eingabe des Paßworts wird die Verbindung automatisch unterbrochen, und der kleine Ausflug in die Welt der illegalen Szene endet, wie so oft, sehr schnell.

Sollte einem Benutzer, der sich ganz neu in ein Board eintragen möchte, das obligatorische Systempaßwort bekannt sein, erfolgt vom System die zweite Paßwortabfrage nach dem sogenannten 'New User Password', abgekürtzt **NUP.** Bei dieser zweiten Paßwortabfrage scheitern Neulinge meist endgültig. Das NUP wird nur dann verlangt, wenn der Benutzer nach der Eingabe des Systempaßworts keine gültige Zugangsberechtigung vorweisen kann, die aus dem Benutzernamen **(Handle)** und einem individuellen Paßwort besteht. Das System erkennt also automatisch, ob es sich um einen Neuling handelt, der damit gezwungen ist, einen komplett neuen Antrag auf Mitgliedschaft zu stellen.

Die eingetragenen Benutzer kennen zwar das Systempaßwort, aber sie kennen nicht das NUP, da sie als eingetragene Benutzer nicht mehr danach gefragt werden. Selbst wenn einem also jemand das Systempaßwort eines Boards verraten würde, könnte man nur schwer das zusätzlich erforderliche NUP in Erfahrung bringen. Das NUP wird in der Regel unabhängig vom Systempaßwort in regelmäßigen Abständen geändert, damit es nur vom Systembetreiber selbst an ausgesuchte Personen weitergegeben werden kann.

Falls jemand durch eine erfolgreiche Eingabe des Paßworts beide Sicherheitsbarrieren passiert haben sollte, steht dem Eindringling noch eine nicht weniger schwere Aufgabe bevor. Zuerst erfolgt eine automatisierte Abfrage über realen Namen, komplette Anschrift und Telefonnummer. Danach werden Fragen zur Gruppenzugehörigkeit und Aufgabenbereich gestellt, den man in der Szene abdeckt. Auch werden an den Neuling allgemeine Fragen über die Szene gerichtet. Meistens wird die Eingabe von Abkürzungen aus dem Szenejargon verlangt, die zum größten Teil nur von der illegalen Szene genutzt werden. Üblich sind Fragen wie: 'Was ist **CC**?', 'Was bedeutet **SCX**?', 'Wofür steht **TRSI**?' Am Schluß muß der Antragsteller noch drei Bürgen nennen, die eingetragene Mitglieder des Boards sein müssen und drei Namen von weiteren Boards angeben, in denen er eingetragenes Mitglied ist.

Der Eintrag in das allererste Board wird damit erkennbar schwierig, eine Rezept-Lösung für dieses Problem gibt es nicht. Selbst die erfolgreiche Beantwortung der Fragen ist einem Systembetreiber noch nicht Beweis genug, daß der Antragsteller ein erfahrenes Szenemitglied ist. Deshalb wird die Verbindung nach dem Antrag kurzerhand mit der Aufforderung unterbrochen, sich nach zwei Wochen wieder zu melden. Der Systembetreiber nutzt diese Zeit, um alle Angaben des Antragstellers auf ihre Richtigkeit zu prüfen.

Für einen hartgesottenen Trader, der sich durch seine ständigen Touren von Board zu Board genügend Szenewissen angeeignet hat und die nötigen Referenzen locker aus dem Ärmel schüttelt, ist ein Antrag auf Mitgliedschaft innerhalb weniger Minuten erledigt. Die Aufnahme in das Board seiner Wahl ist für ihn so gut wie sicher, und schon nach zwei Wochen kann er sich zu den ordentlichen Mitgliedern des Boards zählen.

Bereits eingetragene Mitglieder eines Boards haben es durch die ständig wechselnden Paßwortabfragen nicht leicht, dabei zu bleiben. Hat man sich eine gewisse Zeit nicht mehr gemeldet, wird sich das Systempaßwort ge-

ändert haben, in der Regel alle drei Wochen bis drei Monate. Danach gibt es keine direkte Möglichkeit mehr, in das System hineinzugelangen. Gewöhnlich erfolgt sogar nach vierwöchigem Nicht-Melden der automatische Rauswurf. So schützt sich ein Board vor Personen, die ihre Mitgliedschaft nicht ernst genug nehmen oder nur aus Prestigegründen eingetragene Mitglieder des Boards sind. Beides stört den reibungslosen Softwareverkehr und wird von keinem Systembetreiber geduldet.

Schwarze Schafe

Der größten Gefahr sind Boards dann ausgesetzt, wenn jemand aus den eigenen Reihen im Auftrag einer Anwaltskanzlei herumspioniert. Diese Leute werden in der Szene **Buster** genannt und sind der größte Feind der illegalen Szene. Es sind vor allem die jüngeren Systembetreiber, die durch ihre Naivität eher von der Polizei erwischt werden als andere. Ertappte Systembetreiber geben oft aus Angst vor einer zu hohen Strafe nach und verraten Boards in ihrem Umkreis. Von dieser Art Deal versprechen sich viele, denen ein Prozess droht, mildernde Umstände.

In der Regel wird der gebustete Systembetreiber eines Boards unverzüglich aus allen Boards der Welt, in denen er Mitglied war, ausgetragen. Dabei interessiert es kaum jemanden, ob der Systembetreiber der Polizei nun etwas verraten hat oder nicht. Verständlicherweise möchte sich keiner einem erhöhten Risiko aussetzen, und deswegen geht ein Systembetreiber immer vom Schlimmsten aus.

Nachdem ein Board lahmgelegt worden ist, verbreiten sich innerhalb weniger Stunden Gerüchte über bestimmte Personen, die diesen Vorfall verursacht haben könnten. Denn die Szene verfügt über sehr gute Beziehungen und ermittelt immer selbst. Letzten Endes kommt sie meistens an die erforderlichen Informationen, um den Verräter zu entlarven - entweder durch Bestechung oder durch Freunde in hohen Positionen. Es kann sogar vorkommen, daß ein Systembetreiber schon Wochen, bevor die Polizei selbst davon weiß, mit einer Hausdurchsuchung rechnet. So etwas ist natürlich nur dann möglich, wenn die Szene Informanten direkt in einer Anwaltskanzlei hat, die in dieser Angelegenheit ermittelt.

Es ist ein gefährliches Unterfangen, ein Board zu führen, doch kann es der erste große Schritt einer ruhmreichen Szene-Karriere sein. Wer ein Board richtig führt, kann Mitglieder aus allen Ländern der Welt gewinnen, was der beste Weg ist, den Namen des eigenen Boards populär zu machen. Doch nicht jedes Szenemitglied kann das eigene Board lange erfolgreich führen. Häufig sind die Konkurrenzkämpfe zwischen den Boards zu heftig und zwingen auch erfahrene Systembetreiber aufzuhören, denn in der Szene gilt das Gesetz des Stärkeren. Jeder, der im Kampf um Geschwindigkeit und Software nicht standhalten kann, ist es nicht wert, ein Board im Namen seiner Gruppe, geschweige denn im Namen der Szene, zu führen. Durch verschiedene Tricks und Hacks versuchen Systembetreiber, Boards von Neueinsteigern lahmzulegen - und das oft mit Erfolg. Sollten jedoch alle Maßnahmen nicht weiterhelfen, scheuen viele Szenemitglieder auch nicht davor zurück, ihre Konkurrenz der Polizei auszuliefern.

'Hallo, ist dort Mr. Wilson?'
‚Ja !?'
'Wir haben hier ein Gespräch von einer Mrs. Wilson. Akzeptieren Sie es als R-Gespräch?'
'Eh, ja, natürlich.'

(Knacken in der Leitung)

'Oh, hören Sie, wir haben Probleme mit Ihrer Leitung. Wären Sie auch einverstanden, das Gespräch über eine Calling Card abzurechnen?'

'Na ja, wenn es sein muß.'

'Es tut uns leid, es geht nicht anders. Wie lautet Ihre Nummer?'

Der Phreaker

Das Prinzip des kostenfreien Telefonierens

Der Begriff Phreaker ist eine Verknüpfung der beiden Wörter 'Phone' (Telefon) und 'Freak' (Fanatiker). Die Bezeichnung Phreaker ist in der Szene fast schon eine Ehrenauszeichnung für jemanden, der seine Arbeit voll und ganz auf kostenfreies Telefonieren konzentriert. Das Zeitalter der Phreaker begann mit der Entwicklung des **Akustikkopplers** - ein Gerät, das die Verbindung zwischen Computer und Telefon herstellte. Später wurde ein neues und besseres Gerät entwickelt, das sich zwar von der Funktion her nicht von seinem Vorläufer unterscheidet, aber schneller und praktikabler ist: das Modem.

Als die ersten Modems auf den Markt kamen, hatte die Szene nicht nur ein neues Spielzeug bekommen. Die Einführung und Normung dieses Geräts verbesserte die Kommunikation in der Szene entscheidend. Die unsichere und zeitraubende Methode, Software über den Postweg in alle Welt zu verschicken **(swapping),** hatte mit der Einführung des Modems ausgedient. Szenegruppen erkannten, daß ihre gecrackte Software über ein Modem viel schneller an die entsprechenden Stellen weitergeleitet werden konnte. Doch die Kosten, die zwangsläufig durch das ununterbrochene Telefonieren und die im Vergleich zu heute erheblich längeren Übertragungsraten entstanden, waren für den Einzelnen nicht zu tragen. Sicherlich wäre es naheliegend gewesen, die anfallenden Kosten zu teilen. Doch diese Lösung wäre nicht szenetypisch gewesen.
Normalerweise beginnt die Lösung eines Problems in der Szene nicht erst, wenn jemand darauf aufmerksam macht. Hacker haben oft nichts besseres zu tun, als Probleme der Szene zu lösen, die noch gar keine sind. Anders war es mit den Phreakern, die erst auf den Plan traten, als ein Problem bereits akkut war. Obwohl sich die Szene-Kontakte wegen der günstigeren Tarife hauptsächlich auf die Nachtzeiten verlegten, trafen schon bald die ersten astronomisch hohen Telefonrechnungen ein. Es herrschte Aufbruchsstimmung in der illegalen Szene, und jeder Szenehacker wußte, was zu tun war. Da mit einem Entgegenkommen der Telefongesellschaften kaum zu rechnen war, galt es, in kürzester Zeit einen Weg zu finden, Telefongebühren ganz zu umgehen - keine schwierige Aufgabe, wie sich herausstellen sollte.

Manipulieren der Telefonleitung: Blue Boxing

Um die Entstehung des kostenfreien Telefonierens in Form des **Blue Boxing** nachvollziehen zu können, sollte man im Groben wissen, wie eine Telefonverbindung von der Zentralstelle aus gesteuert wurde.

Vermittlungscomputer analoger Leitungen werden hauptsächlich durch Tonsignale gesteuert. Wenn man den Hörer nach Beendigung eines Telefonats auf die Gabel legt, wird die Verbindung nur indirekt unterbrochen. Durch das Auflegen wird ein akustisches Signal erzeugt, das durch die stehende Leitung zur örtlichen Vermittlungsstelle geschickt wird. Der Zentralcomputer erkennt diesen Ton als Unterbrechungssignal und trennt erst dann die Verbindung.

Einer, der es auf äußerst ungewöhnliche Weise schaffte, kostenfrei zu telefonieren, war 'Cap'n Crunch'. Eines Morgens rief ihn ein blinder Freund an, und machte ihn auf eine Cornflakespackung namens 'Cap'n Crunch' aufmerksam. In dieser befand sich eine kleine Spielzeugpfeife, mit der man angeblich Töne erzeugen konnte, auf die der Computer der amerikanischen Telefongesellschaft 'Ma Bell' reagierte. Nach zahlreichen Versuchen fand Cap'n Crunch die spezifischen Frequenzen, mit denen man den Vermittlungscomputer zu einer Unterbrechung der Gebührenübermittlung brachte. Ein Gespräch konnte weitergeführt werden, ohne daß Kosten entstanden. Ein einfacher Gimmick in einer Cornflakespackung ermöglichte ihm so die Täuschung eines riesigen Vermittlungscomputers. Damit hatte er nicht nur seinen Namen gefunden, sondern auch das sogenannte Blue Boxing **(BB)** ins Leben gerufen. Die Geschichte von Cap'n Crunch wird wie eine Legende von Phreaker zu Phreaker weitererzählt - und die Methode funktioniert noch heute.

Durch diese Geschichte erkannte die Szene, daß es möglich ist, über Tonsignale in die Funktionen des Zentralcomputers der Telefonvermittlung einzugreifen und den Gebührenzähler zu stoppen. Um die Signale zur Manipulation des Vermittlungscomputers zu ermitteln, begaben sich Hacker der Szene daran, durch endloses Ausprobieren verschiedenster, oft selbstgebastelter Geräte **(Dialer),** brauchbare Pfeiftöne zu erzeugen. Ein besonders cleverer Hacker fand jedoch eine bessere und vor allem einfachere Lösung. Er schrieb die Telefongesellschaft an und bat höflich um die Steuersignale. Die damals noch völlig unvoreingenommene Telefongesellschaft war so freundlich und übersandte dem netten und interessierten Kunden die Liste völlig kostenlos und unverbindlich.

Immer mehr Szenemitglieder wurden mit der Zeit eingeweiht und nutzten diese Technik, auch um privat kostenfrei zu telefonieren. Damit jedes Szenemitglied in den Genuß des kostenfreien Telefonierens kommen konnte, wurde eine Liste mit Steuersignalen und den dazugehörigen Programmen zur Erzeugung der Töne in den Szenemailboxen verteilt. Eine große Welle des Blue Boxings brach über die Telefongesellschaften herein. Szenemitglieder aus aller Welt nutzten diese Methode, um kostenfrei zu telefonieren. Das Blue Boxing entwickelte sich zu einer gängigen und für die Szene unverzichtbaren Technik. Den Telefongesellschaften entstanden innerhalb kürzester Zeit Verluste von Hunderten Millionen Dollar. Das Problem, mit dem sie sich nun auseinanderzusetzen hatten, war für sie völlig neu.

Schnell wurde den Telefongesellschaften klar, daß diesem Zustand ein Ende bereitet werden mußte. Die drei größten amerikanischen Unternehmen AT&T, MCI und Sprint suchten mit Hilfe von Fachleuten nach Wegen, die Szene am Mißbrauch ihrer Steuersignale zu hindern. Der erste Schritt bestand darin, die Steuersignale in unregelmäßigen Abständen zu ändern und geheimzuhalten. Die Phreaker konnten nun nicht mehr die alten Signallisten verwenden und standen vor einem neuen Problem.
Als Antwort der Szene wurden Programme entwickelt, die die aktuellen Signale ausfindig machen sollten. Es ging sogar so weit, daß Geräte mit eigenen Chips hergestellt wurden, die speziell zum Auskundschaften der Signale dienten. Diese Geräte, Blue Boxes genannt, wurden direkt ans Telefon angeschlossen. Sobald die Bauanleitungen in der Szene verteilt waren, machten sich die Phreaker auf die Jagd nach den Signalen. Jedesmal, wenn die Telefongesellschaften nun die Signale änderten, durchkämmten tausende von Phreakern die Telefonleitungen nach akustischen Codes.

Das führte zu einer immensen Belastung der Telefonleitungen, wodurch es zu ständigen Ausfällen in den zentralen Vermittlungsstellen kam. Die Programme wurden in der Szene so schnell weiterentwickelt, daß das Auskundschaften der Signale schon nach kurzer Zeit kein allzugroßes Problem mehr darstellte. Nach jeder Steuersignaländerung dauerte es nur wenige Stunden, bis eine neue Liste mit den aktuellen Signalen in den Szenemailboxen zu finden war. Daraufhin mußten die Telefongesellschaften einsehen, daß jede technische Blockade nur eine neue Herausforderung für die Szene darstellen würde. In den USA schlugen die Unternehmen als erste andere Wege zur Bekämpfung des illegalen Telefonierens ein.

Als äußerst wirksam erwies es sich, die illegal belegten Leitungen gemeinsam mit der Polizei zurückzuverfolgen. Da das FBI bis heute keine Befugnis hat, strafrechtliche Schritte in Deutschland einzuleiten, war das Blue Boxing von hier aus noch möglich, als in Amerika bereits einigen Phreakern schwere Strafen drohten. Die staatliche deutsche Telefongesellschaft, damals noch Deutsche Bundespost, wollte von all dem solange nichts wissen, bis ihr von amerikanischer Seite massiv gedroht wurde. Die amerikanischen Telefongesellschaften stellten damals ein Ultimatum: innerhalb kürzester Zeit mußte die Telekom alle Phreaker ausschalten. Die Telekom tat ihr Bestes, um das Problem zu lösen. Unermüdlich präsentierten Techniker Konzepte, die die Phreaker und damit die Szene zu Fall bringen sollten. Die oft sehr teuren und aufwendigen Gerätschaften, sogenannte 'Filter', die unterscheiden sollten, ob ein fremdes Signal gesendet wurde, hielten die Szene nur leider nicht davon ab, weiterhin Blue Boxing zu betreiben.

Die Telekom erkannte schließlich die Sinnlosigkeit ihres Unterfangens, allein gegen die Szene vorzugehen und tat es den amerikanischen Telefongesellschaften gleich. Mit Hilfe der Landespolizei und dem Rat des FBI gelang es, die Leitungen der Phreaker anzuzapfen und in der Zentralstelle festzuhalten. So konnten diese die Verbindung nicht mehr unterbrechen und eine Standleitung zum jeweiligen Gesprächspartner blieb bestehen, bis die Polizei vor Ort eintraf, um Beweise des Telefonbetrugs aufzunehmen.
Das Zurückverfolgen der Verbindung, in Szenekreisen **Tracing** genannt, ist auch heute noch die einzig wirksame Abschreckung gegen das Blue Boxing. Durch Fangschaltungen unterschiedlichster Art gelang es derTelekom endgültig, die Blue-Box-Aktivitäten auch in Deutschland fast völlig zu stoppen. Hunderte von Szenemitgliedem konnten unschädlich gemacht werden. Blue Boxing wurde sehr riskant, und nach einiger Zeit erklärte die Szene diese Methode des kostenfreien Telefonierens für zu gefährlich. Eine neue Methode mußte her, und die ließ nicht lange auf sich warten.

Gestohlene Nummern: Calling Cards

Der Sinn und Zweck einer Calling Card besteht darin, bargeldloses Telefonieren von jedem Punkt der Welt aus möglich zu machen, und zwar überall zum gleichen Tarif. Dies ist besonders für Firmen und Unternehmen attraktiv, die auch Mitarbeiter im Ausland beschäftigen. Anders als in Deutschland ist in Amerika der Calling-CardService, der von den Telefongesellschaften AT&T und MCI angeboten wird, etwas völlig Übliches. Zwar bietet die Deutsche Telekom mit ihrer T Card einen ähnlichen Service an, doch wurde dieser von deutschen Firmen noch nicht richtig angenommen.

Zum Telefonieren mit einer Calling Card ist die Karte selbst nicht zwangsläufig nötig. Man braucht nur die vierzehnstellige Nummer der Karte zu wissen. Ein Mitarbeiter einer amerikanischen Firma in Deutschland kann mit der Nummer seiner Calling Card sämtliche Gespräche, seien sie beruflich oder privat, von jedem Telefon aus bargeldlos führen. Dazu muß er nur den entsprechenden kostenlosen Calling-Card-Service (in Deutschland: 0130/0010) anrufen und die Nummer seiner Karte durchgeben. Der Operator oder ein Computer verbindet den Kunden dann mit dem gewünschten Gesprächsteilnehmer. Die Telefongebühren werden automatisch von seinem Konto abgebucht.

Irgendwann fiel einem Phreaker auf, daß die vierzehnstellige Nummer einer Calling Card nach einem bestimmten Algorithmus aufgebaut ist. Durch diese Entdeckung war es den Phreakern möglich, eigene Calling Cards herzustellen. Die Nummern wurden nun eine nach der anderen auf dem Computer der Telefongesellschaft AT&T ausprobiert. Da die Verbindung zum AT&T-Calling-Card-Service kostenlos ist und der AT&T-Computer keine Fragen stellt, kann ein Phreaker tagelang ungestört herumprobieren, bis er eine existierende Nummer gefunden hat. Aber eine zufällig gefundene Calling-Card-Nummer ist natürlich nicht unbegrenzt gültig. Spätestens wenn die Abrechnung der Calling Card erfolgt, wird dem Besitzer klar, daß er nicht der einzige gewesen sein kann, der mit seiner Karte telefoniert hat. Die Karte wird dann sofort gesperrt und ist für den Phreaker wertlos.

Dem Einfallsreichtum der Phreaker, an Calling-Card-Nummern heranzukommen, sind keine Grenzen gesetzt. Eine andere beliebte Methode nennt sich in Szenekreisen **Social Engineering.** Ein Phreaker ruft einfach einen Calling-Card-Besitzer, also einen gewöhnlichen Kunden an, gibt sich als AT&T oder MCI-Mitarbeiter aus und fragt den Kunden höflich nach seiner Calling-Card-Nummer. Man sollte es kaum für möglich halten, aber Tausende von Calling Cards werden auf diesem Weg von der Szene genutzt.

Ein Phreaker erhackt in der Regel mehr Karten, als er selbst benötigt. Der Überschuß wird dann einfach an die Szene verkauft. Der Preis liegt etwa bei fünf bis fünfzehn Dollar pro Stück. Obwohl niemand garantieren kann, wie lange gehackte Calling-Card-Nummern gültig sind, werden sie den Phreakern geradezu aus den Händen gerissen. Viele verdienten durch den Verkauf von illegal erworbenen Calling-Card-Nummern ein kleines Vermögen.

Schließlich entdeckte ein Phreaker einen gravierenden Fehler der Kommunikationsgesellschaft MCI. MCI hatte Tausende von Calling-Card-Nummern, die von keinem Kunden aktuell genutzt wurden, in einem Computer reserviert. Mit Hackversuchen gelang es der Szene, Zugang zu diesen Kartennummern zu bekommen. In der Szene nannte man diesen höchst willkommenen Fehler den '**MCI-Bug**'.

Durch den MCI-Bug sind mehrere tausend Calling-Card-Nummern in die Szene gelangt. Nie zuvor hatte es so einen Überschuß an Calling-Card-Nummern gegeben. An jeder Ecke konnte man plötzlich illegal Nummern erwerben, und dies sogar in ungewöhnlich großen Mengen. Dadurch explodierte die Szene förmlich. Denn durch die plötzlich rapide gestiegene Zahl der illegal in die Szene gelangten Calling-Card-Nummern gab es Szenemailboxen mit Raubkopien wie Sand am Meer. MCI bemerkte erst nach einiger Zeit, was vor sich ging, und es dauerte nur wenige Tage, bis der Fehler behoben war. Alle Kartennummern, die durch den MCI-Bug in Umlauf gekommen waren, wurden ungültig. Die Szene mußte sich wieder einmal etwas einfallen lassen.

Kurze Zeit später hatten Phreaker aus der Szene einen V-Mann in der amerikanischen Telefongesellschaft MCI,

der sie mit Kartennummern versorgte. Daraufhin hatten die Telefongesellschaften endgültig genug. Ein Exempel mußte statuiert werden, damit die Aktivitäten der Phreaker aufhörten. Es folgten einige schwere Schläge gegen die Szene. Mitte 1994 verhaftete das FBI ein Szenemitglied, das an der Quelle zu Calling-Card-Nummern saß. Das Mitglied hatte in regelmäßigen Abständen große Pakete mit bis zu tausend Kartennummern an die Szene weiterverkauft. Mehr als fünfeinhalb Jahre mußte der Betroffene dafür ins Gefängnis. Die Hintermänner wurden natürlich nicht geschnappt.

Dem deutschen 'Calling-Card-König' Kim Schmitz (Pseudonym: Kimble) erging es ähnlich. Kimble, damals gerade erst zwanzig Jahre alt, war wohl einer der wichtigsten und größten deutschen Phreaker, die es je in der Szene gegeben hatte. Er verkaufte Calling-Card-Nummem im großen Stil und wurde zu einem der Hauptlieferanten der weltweiten Szene. Daneben handelte er auch mit gefälschten Kreditkarten. Man schnappte Kimble zwar, allerdings konnte man ihn bis heute nicht verurteilen. Das Verfahren dauert zur Zeit noch an.

Die Verhaftungswelle löste damals in der Szene einen Schock aus. Noch bevor Kimbles Festnahme durch die Medien an die Öffentlichkeit gelangte, konnte man in jeder Szenemailbox rund um den Globus Informationen zu diesen Vorfall einholen. Speziell dieses Ereignis sorgte in der Szene für viel Wirbel und ist bis heute ein abschreckendes Beispiel für alle Phreaker geblieben. trotzdem ist das Prinzip des kostenfreien Telefonierens mit Hilfe von Calling Cards immer noch mit dem kleinsten Risiko verbunden.

Telefonkartenbetrug

Fernsehberichte haben in letzter Zeit versucht, die Aufmerksamkeit auf Chipkartenbetrüger zu lenken. Mit einem Chipkartengerät, das schreiben und lesen kann, ist es demnach angeblich möglich, Krankenkassenkarten und ähnliches zu kopieren. Diese Information ist soweit richtig. Denn mit einem handelsüblichen Gerät, das für unter dreihundert Mark zu erwerben ist, kann inzwischen durchaus eine Krankenkassenkarte ausgelesen, kopiert und auf einer Blanko-Karte gespeichert werden. Abgesehen davon, daß es illegal ist, wird jedoch schnell deutlich, wie unspektakulär es eigentlich ist, Krankenkassenkarten zu kopieren.

Um das Thema ein wenig interessanter zu machen, gehen einige Fernsehberichte noch einen Schritt weiter und behaupten neuerdings, dieselbe Methode mache es auch möglich, Telefonkarten zu kopieren. Dies ist aber nur teilweise richtig. Der Code auf einer Telefonkarte ist zunächst einmal geschützt, so daß eine Kopie nicht direkt möglich ist. Dennoch schaffen es einige Hacker, diese Zeichen auszulesen. Doch damit ist es noch lange nicht getan. Um nun auch mit dieser Karte telefonieren zu können, ohne daß nach einer Minute eine Polizeistreife auftaucht, bedarf es einer Methode, die unseres Wissens nach bislang noch von keinem Hacker der Welt entdeckt worden ist.

Hält man eine Telefonkarte schräg gegen das Licht, kann man meistens am Rande eine kaum lesbare Seriennummer erkennen. jede Telefonkarte hat eine solche Seriennummer, die zusätzlich auf dem Chip gespeichert ist. Diese wird von der Telefonzelle, von der aus die Telefonkarte benutzt wird, an die Zentralstelle der Telefongesellschaft gesendet. Dort wird die Karte überprüft. Da man davon ausgehen kann, daß jede Telefonkarte im Zentralcomputer der jeweiligen Telefongesellschaft registriert ist, würde der Computer sofort Alarm schlagen, wenn eine Karte plötzlich doppelt auftaucht. Keine Chance also für Telefonkartenfälscher.

In Berlin wurden vor knapp einem Jahr bei einem Großeinsatz der Polizei 191 Menschen wegen Betrugs mit Telefonkarten festgenommen. Seit den Anfängen des Telefonkartenbetrugs um 1995 häufen sich derartige Verhaftungen. Dies zeigt, daß selbst organisierte Gruppen außerhalb der Szene mit Telefonkartenbetrug nicht sehr weit kommen.

Bislang ist in der Szene nicht bekannt geworden, daß ein Phreaker mit einer Telefonkarte erfolgreich kostenfrei telefonieren konnte. Das liegt daran, daß die Szene weiß, wie riskant es ist. Diese Variante des kostenfreien Telefonierens würde in der Szene als Rückschritt betrachtet werden und stand daher nie ernsthaft zur Debatte.

» Der Zugang zu Computern und allem, was einem zeigen kann, wie diese Welt funktioniert, sollte unbegrenzt und vollständig sein.
» Alle Informationen müssen frei sein.
» Mißtraue Autoritäten - fördere Dezentralisierung.
» Beurteile einen Hacker nach dem, was er tut und nicht nach üblichen Kriterien wie Aussehen, Alter, Rasse, Geschlecht oder gesellschaftliche Stellung.
» Man kann mit einem Computer Kunst und Schönheit schaffen.
» Computer können dein Leben zum Besseren verändern.

Hackerethik

Die Szene und das Gesetz

Polizei, Gesetz und Gravenreuth

In der amerikanischen Szene hört man immer öfter von Fällen, bei denen selbst höhere Instanzen, wie das FBI, durch zeitaufwendige Ermittlungsarbeit illegale Szenemailboxen aufdecken. In Europa ist dies ähnlich. Es gibt Sonderkommissionen, die sich speziell mit der Softwarepiraterie beschäftigen. Das Thema wird im allgemeinen auch in Europa inzwischen sehr ernst genommen, denn der Schaden, der in den letzten Jahren durch Raubkopierer entstanden ist, geht laut Firmenangaben in die Millionen.
Deshalb haben sich viele größere Softwarefirmen dazu entschlossen, die Softwarekriminalität aktiv zu bekämpfen und holten sich die Unterstützung rechtschaffender Anwälte. Einer der bekanntesten auf dem Gebiet der Softwarekriminalität ist der Münchener Rechtsanwalt Günter Freiherr von Gravenreuth, der schon seit den Anfängen der Szene auf der Jagd nach Raubkopierern ist.

Wenn es um die Verfolgung von Raubkopierern geht, ist er der kompetenteste Mann. Das liegt wohl auch daran, daß ihm jedes Mittel Recht zu sein scheint. In den 8oer Jahren versuchte von Gravenreuth unter dem Decknamen 'Tanja', Raubkopierer durch Tauschangebote in Kleinanzeigenteilen verschiedener Zeitschriften anzulocken. So mancher fiel auf diesen Trick herein und wurde wegen Verbreitung urheberrechtlich geschützter Software angeklagt. Es ist verständlich, daß der Münchener Anwalt der illegalen Szene nicht gerade sympathisch ist. Besonders durch seine umstrittenen Lockvogel-Aktionen hat er sich auch in anderen Kreisen wenig Freunde gemacht.

Anfang 1996 konnte von Gravenreuth die holländische Firma 'Tricon Engineering B.V' als Mandanten gewinnen und erreichte durch richterlichen Beschluß, daß dieser Name verwechslungsfähig mit 'Triton' (Standard Motherboard Chipsatz) sei. Kaum hatten PC-Händler von diesem Beschluß gehört, begann eine Welle von Abmahnungen. Fast alle Händler warben, natürlich völlig unwissend, in Prospekten und Schaufenstern mit dem Namen 'Triton' weiter. Jeder, der heute noch mit dem Namen 'Triton' wirbt, muß seitdem mit einer Abmahnung von ca. 1300 Mark rechnen. Mit dieser Aktion sorgte der Anwalt für Furore, und seither ist sein Name auch außerhalb der Szene für viele ein Begriff.

Überall in der Szene hat von Gravenreuth seine Spitzel. Diese Leute sind häufig ehemalige Szenemitglieder, die sich in der Szene auskennen und entsprechende Beziehungen haben. Dadurch kommt er an Telefonnummern und Paßwörter von Mailboxen und Boards heran, die illegal Software vertreiben und kann dann bei der Staatsanwaltschaft einen Durchsuchungsbefehl erwirken. Ehemalige Szenemitglieder, die mit ihm kollaborieren, sind in der Szene noch verhaßter als er selbst. Sie gelten als Verräter, und wenn jemand als solcher entlarvt wird, hat er nie wieder die Möglichkeit, der Szene beizutreten.

Jedem Mitglied der Szene ist das Pseudonym 'Kimble' bekannt (» 3. Eintrag). Die Verhaftung von Kim Schmitz war das Resultat einer aufwendigen Kooperation des Bayerischen Landeskriminalamtes, der Telekom und der Münchener Kriminalpolizei. Ihm wurde Telefonbetrug vorgeworfen und ein Schaden von mindestens 20 Millionen Mark zur Last gelegt. Der Münchener Anwalt von Gravenreuth, der großes Interesse an Kimble hatte, stand diesem in vielen Angelegenheiten zur Seite. Nicht ohne Grund, wie sich herausstellen sollte, denn Kim Schmitz erwies sich als besonders kooperativ, und durch seine Tips kamen weitere Szenemitglieder in hohen Positionen in unangenehmen Kontakt mit der Polizei. Die Szene war empört, und man ging sogar so weit, ein Kopfgeld auf Kimble auszusetzen. Glücklicherweise nahm das keiner allzu ernst.

Der Fall Kim Schmitz war ein besonders schwerer Schlag für die illegale Szene. Manch einer behauptet, daß man die Nachwirkungen der damaligen Aufdeckungswelle noch heute in der Szene spüren kann. trotzdem sind Leute wie Kim Schmitz in der Szene keine Seltenheit. Immer wieder tauchen Gerüchte über Leute auf, die angeblich mit der Polizei kollaborieren.

Die Szene ist entsprechend vorsichtiger geworden. Sollte jemand in Verdacht stehen, mit von Gravenreuth oder der Polizei gemeinsame Sache zu machen, wird er überprüft und überwacht. Wenn sich der Verdacht erhärtet

oder sogar bestätigt, sind die Folgen für den Überläufer verheerend. Innerhalb von vierundzwanzig Stunden ist die gesamte illegale Szene durch Infofiles über den Buster informiert. Ein Szenemitglied müßte sich schon im Keller einsperren, um diese Information zu verpassen. jemand in einer führenden Position könnte es durchaus schaffen, die komplette Szene in nur wenigen Tagen zu enthaupten. Auf Tausende von Mitgliedern würden dann enorme Geldbußen oder sogar Gefängnisstrafen zukommen.

Es ist daher verständlich, daß die Szene Augen und Ohren offenhält, damit so etwas niemals geschieht. Die Methoden, einem Buster den Kopf zurechtzurücken, sind nicht selten rüde, und aus diesem Grund bemüht sich von Gravenreuth, seine Informanten verdeckt zu halten. Außerdem ist ein Buster, der in der Szene schon als solcher entlarvt wurde, völlig unbrauchbar.

Agent provocateur

Die Mitarbeiter des Münchener Anwalts von Gravenreuth sind meist Selbständige, die unter der Berufsbezeichnung 'Testbesteller' beim jeweiligen Finanzamt eingetragen sind. Die eigentliche Aufgabe eines Testbestellers ist es, an Material heranzukommen, das Verstöße gegen das Urheberrecht beweisen kann. Doch die Arbeit eines Testbestellers ist noch um einiges vielseitiger. So kann sich ein Testbesteller auch intensiv mit der Szene beschäftigen und illegale Mailboxen auffliegen lassen.

Dazu muß er eine Mailbox ausfindig machen, die Raubkopien verbreitet. Eine solche Mailbox zu erkennen ist nicht sonderlich schwer, denn in fast allen Szenemailboxen sind Raubkopien zu finden. In ein solches System einzudringen ist schon eine andere Sache: Szenemailboxen sind gegen Eindringlinge gut geschützt (» 2. Eintrag). Hin und wieder gibt es Testbesteller mit Hackerfahrung. Diese haben dann natürlich mehr Möglichkeiten, in ein System einzudringen. Hat ein Testbesteller einmal Zugriff zu einer Mailbox bekommen, wird er sich sofort nach raubkopierter Software umsehen und sich diese aneignen. Eine Liste der Software, die in dem System zu holen ist, wird erstellt und zusammen mit den Paßwörtern, die den Zugriff auf die Mailbox ermöglichen, an die Kanzlei geschickt. Ist die Beweislage sicher, wird alles erforderliche Material an die Staatsanwaltschaft weitergeleitet. Diese kann dann einen Durchsuchungsbefehl erlassen.

Neben diesen vielseitigen und komplizierten Ermittlungstätigkeiten kann ein Testbesteller noch andere Aufgaben übernehmen, zum Beispiel Videotheken ausfindig machen, die Spiele von Softwarefirmen ohne Erlaubnis vermieten. Oft durchstöbern Testbesteller auch Flohmärkte, um festzustellen, ob dort Raubkopien vertrieben werden.

Speziell in solchen Fällen arbeiten die Testbesteller mit der örtlichen Polizei zusammen, die ebenfalls in Kontakt mit von Gravenreuth steht. Ein Anruf des Testbestellers genügt, um mehrere Polizeistreifen zum Ort der kriminellen Handlung zu bewegen.

Die größte Arbeit jedoch haben Testbesteller im Fall 'Triton' geleistet. Hier war es ihre Aufgabe, nach dem gewinnbringenden Wort zu suchen. Die Testbesteller gingen sogar so weit, daß sie Verkäufer mit drastischen Methoden dazu brachten, den Begriff 'Triton' in Rechnungen oder Kostenvoranschlägen zu vermerken. Diese moralisch äußerst fragwürdige Methode hatte sich nach einiger Zeit herumgesprochen und sorgt auch heute noch für Gesprächsstoff.

Im Kreuzfeuer der Softwarefirmen

Szenemitglieder lassen sich von Polizei und Rechtsanwälten nicht unbedingt abschrecken. Vor allem bei Massenanfertigungen von raubkopierten CDs haben die illegalen Hersteller das Risiko bereits einkalkuliert. Sobald eine bestimmte Menge an CDs verkauft worden ist, kann man mit einer polizeilichen Ermittlung leben. Bei sehr großen Mengen verkaufter CDs sind die Gewinne enorm. Keine Softwarefirma kann die Summe des angeblich verursachten Schadens zurückbekommen.

Ein überführter Raubkopierer kann nur in den seltensten Fällen für den Schaden, den er angerichtet hat, aufkommen, und so kommt es häufig zu Deals zwischen Softwarepiraten und den ermittelnden Rechtsanwälten. Man einigt sich auf eine für den Angeklagten annehmbare Summe, frei nach der Devise: 'Lieber weniger als gar nichts.' Die Anklage wird fallengelassen. Nur so ist für jeden, sei es Softwarefirma, Rechtsanwalt oder Softwarepirat, etwas drin.

Die Hersteller haben seit den Anfängen der Softwareindustrie mit Softwarepiraterie zu kämpfen. Das Problem scheint unlösbar, und solange die Nachfrage nach Raubkopien besteht, wird in der Szene auch weiterhin Software gecrackt und verteilt werden. Mittlerweile ist der Tausch von Software auch unter gewöhnlichen User üblich. Viele geben gern und ohne schlechtes Gewissen Kopien an Freunde und Bekannte weiter. Daß damit eine Straftat begangen wird, ist vielen zwar bewußt, aber doch eher egal.

Es ist völlig unbestritten, daß Schäden durch Raubkopierer entstehen können. Ausnahmen zeigen jedoch, daß Firmen nicht unbedingt daran zu Grunde gehen müssen. Man erinnere sich zum Beispiel an die bekannte Softwarefirma 'Factor 5', die Ende der 8oer Jahre das noch bekanntere Computerspiel 'Turrican' auf den Markt brachte. Jedem Computerbesitzer war dieser Titel ein Begriff, und Unzählige besaßen es. Das Problem jedoch war, daß angeblich niemand diesen Titel käuflich erworben, sondern von Freunden bekommen hatte. Die Softwarefirma Factor 5 gab dazu einen offenen Brief an die Szene weiter, mit der Bitte, ihn als Infofile in verschiedenen Boards zu verbreiten.

So etwas war zu jener Zeit genau so schwer bis unmöglich wie heute. Denn die illegale Szene hätte einer Softwarefirma niemals Gehör geschenkt. Doch Factor 5 bestand zum Teil aus ehemaligen Szenemitgliedem, die ihre Beziehungen spielen lassen konnten, um das Schreiben zu veröffentlichen. Darin klärte die damals noch junge Firma über den entstandenen Schaden und den Verlust auf, den sie durch die Szene erlitten hatte. Die Szene wurde aufgefordert, den Schaden wieder gutzumachen. Ferner kündigte Factor 5 an, keine weiteren Spiele für den Amiga-Computer zu produzieren, weil die Szene dort am aktivsten wäre. Factor 5 behauptete in diesem Brief weiter, durch die Szene an den Rand des Ruins getrieben worden zu sein. Das Magazin 'Aktueller Spiele Markt' (ASM) schrieb damals, daß 'Turrican' weltweit nur in einer lächerlichen Stückzahl verkauft worden sei. Und in der Tat: Factor 5 schaffte es, zumindest einen kleinen Stein ins Rollen zu bringen. In der Szene wurden Stimmen laut, die für eine kontrolliertere Verbreitung von Raubkopien plädierten, denn schließlich sei es ja nicht ihre Absicht, gute Softwarefirmen zu zerstören.

Geändert hat sich jedoch nicht sehr viel. Hin und wieder konnte man bei einem gecrackten Spiel die absurde Aufforderung lesen, sich das Original zu kaufen, wenn einem die Kopie zusage: 'A game worth playing is a game worth buying.' (zu deutsch: Ein Spiel, das es wert ist gespielt zu werden, ist es auch wert gekauft zu werden.) Aber immerhin, Factor 5 hatte es tatsächlich geschafft, Hunderte von Szenemitglieder zum Nachdenken zu bringen. Heutzutage wäre das nicht mehr möglich.

Factor 5 überlebte auch ohne die Hilfe der Szene, und das nicht ohne Erfolg. 'Turrican 2' kam bald auf den Markt und wurde ein Verkaufsschlager. Die Szene fühlte sich hintergangen und wunderte sich über die rasche Genesung der Firma. Wie konnte ein Unternehmen, das angeblich so nah am Abgrund stand, weiterhin so gute Software produzieren? War der Brief an die Szene vielleicht nur eine clevere Marketingstrategie? Wer weiß! Tatsache ist jedenfalls, daß Factor 5 zeitweilig einer der größten Softwarehersteller in Europa war. Mittlerweile ist der

Firmensitz nach San Francisco verlegt worden, wo in noch größerem Rahmen Software produziert wird.

Es mag sich vielleicht seltsam anhören, aber Softwarefirmen verdienen auch durch Raubkopierer Geld. Bei erfolgreichen Ermittlungen gegen eine große Anzahl illegaler Mailboxen erzielt eine Softwarefirma durch Schadensanteile manchmal sogar Gewinne, auch wenn ihr Produkt größtenteils nicht regulär über den Ladentisch geht. Sie verdient so an Interessenten, die sich das Original niemals gekauft hätten.

Das Strafverfahren

Die finanziellen Schäden, die Szenemitgliedern vor Gericht vorgeworfen werden, sind astronomisch hoch und in vielen Fällen kaum wiedergutzumachen. Würde die Klägerpartei auf einen richterlichen Beschluß bestehen, müßte der Angeklagte mit einer Freiheitsstrafe rechnen. Doch eine Freiheitsstrafe würde dem Straftäter kein Bußgeld abverlangen und liegt somit nicht im Interesse der Softwarefirma. Abgesehen davon sind die Umstände oft äußerst kompliziert, so daß Klagen dieser Art nicht immer durchgesetzt werden können. Deshalb werden fast neunzig Prozent der Anklagen gegen Szenemitglieder im Bereich Softwarekriminalität fallengelassen. Die Parteien einigen sich dann auf eine Summe, die der Angeklagte tragen kann in manchen Fällen bis zu achttausend Mark -, und damit ist die Angelegenheit für alle erledigt. Der Beschuldigte ist noch einmal mit dem Schrecken davongekommen, die Softwarefirma samt ihrer gesetzlichen Vertreter hat ihr Geld, und alle sind glücklich und zufrieden.

Viele Neueinsteiger in der Szene haben den Fehler gemacht, dem falschen Personenkreis zu vertrauen. Unvorsichtige Frischlinge, die sich durch die Verbreitung illegal kopierter Software einen Namen machen wollten, wurden schon öfters erwischt und verhaftet, bevor auch nur einer ihren Namen aussprechen konnte. Die Szene arbeitet heute nach strengen Regeln: Clevere Geschäftsleute sind der Motor der Szene und entscheiden, was heute kommt und morgen wieder verschwindet. Daher ist die illegale Szene keine Spielwiese für Jugendliche, sondern eine kriminelle Vereinigung und eine ziemlich gut organisierte dazu.

Find vom Chef die Freundin raus
Probiere ihren Namen aus
Tast dich ran mit Ruh im Nu
Zum Hacken, Hacken, Hacken.

Hackerhymne

Die Kunst des Hackens

Der Mythos Hacker

Gerade in Zeiten des Internets, in denen sich die Medien besonders auf Mitglieder der Szene fixiert haben, ist es notwendig geworden, den Mythos Hacker zu entwirren und ein klares Bild davon zu entwerfen, was ein Hacker eigentlich ist. Verfolgt man die Berichterstattung des Fernsehens und der Printmedien genauer, scheint der Hacker heute gefährlicher denn je, und keiner ist vor ihm sicher. Es gibt Zeiten, da fühlt sich die gesamte Boulevardpresse der Welt dafür verantwortlich, auf die Gefahren aufmerksam zu machen, die von einem Hacker ausgehen und vor ihm zu warnen.

Die Kölner Boulevardzeitung 'Express' beispielsweise veröffentlichte 1995 eine Serie mit dem Titel: 'Der Hacker vom Rhein'. Die Aufmachung der Reportage verriet die Intention des Journalisten: er wollte durch Horrorvisionen bestehende Vorurteile gegen Hacker oder Computerfreaks schüren. Ursache einer gewissen Skepsis gegenüber neuen Technologien und ihren Schöpfern ist sicherlich die rasante Entwicklung im Computerbereich. Die damit einhergehende Unüberschaubarkeit macht vielen Menschen Angst. Ein Zitat aus dem genannten Artikel dokumentiert, wie dies ausgenutzt wird. Der Bericht läßt die Person des Hackers Reiner G. wie ein unterkühltes Wesen aus einer gefährlichen fremden Welt erscheinen: 'Ich schaue in seine stahlblauen Augen und sie machen mir Angst, große Angst.' Ein Foto dieser 'angsteinflößenden' Augen unterstreicht neben der Headline den 'gefährlichen Gesamteindruck' des Superhirns.

Was aber weder dem Journalisten noch den Lesern damals klar war und nur Eingeweihte wissen konnten: Dieser angebliche Hacker war in der Kölner Mailboxszene eher berüchtigt als berühmt. Hinter dem Pseudonym 'Antivirus' versteckte sich ein notorischer Lügner, der mit der Szene nicht den geringsten Kontakt hatte und nie Mitglied irgendeiner Gruppe war. Die Tatsache jedoch, daß dieser angebliche Hacker nun schon die Medien übers Ohr hauen konnte, machte eines deutlich: Die Figur des Hackers wird auch in Zukunft Gesprächsstoff liefern, egal, ob die Geschichten der Informanten der Wahrheit entsprechen oder nicht.

Der typische Hacker ist nicht immer sonderlich zielstrebig und gut organisiert. Oft handelt es sich um einen gelangweilten Computerfreak, der seine Kenntnisse mißbraucht und eigentlich nichts weiter ist als ein undisziplinierter User. Unter dem Begriff 'hacken' versteht man in der Regel das Eindringen in elektronische Systeme, Netzwerke oder Mailboxen. Häufig findet nach dem erfolgreichen elektronischen Einbruch ein Akt der Verwüstung und Zerstörung durch den Hacker statt. Andere Hacker, wie sie zum Beispiel im Chaos Computer Club organisiert sind, legen Wert darauf, daß sie zwar in Systeme eindringen, dies allerdings nur tun, um Sicherheitslücken aufzudecken.

Anwender, die sich als Hacker bezeichnen, sammeln ihre Hackerfahrung hauptsächlich in der Szene. Fast alle Hacker sind oder waren einmal Szenemitglieder und gehören oder gehörten einer illegalen Gruppe der Szene an. Nur so ist es einem Hacker überhaupt möglich, die verschiedenen Varianten und Methoden des Hackens kennenzulernen und sie innerhalb der Szene weiterzuentwickeln. Der Austausch von Hardwarebauplänen, Hacksoftware und verschiedenen Tips und Tricks findet in Konferenzräumen der Szenemailboxen, im Internet und auf Veranstaltungen statt, zu denen nur Mitglieder der Szene Zugang haben. Die Informationen, die auf diese Weise verteilt werden, beruhen auf jahrelanger Erfahrung unterschiedlichster Hacker. Ein Computerfreak, der keine Kontakte in der Szene hat, kann kaum ein richtiger Hacker werden. Nur durch die Hilfe der Szene kann er mit seinen Aktivitäten Erfolg haben.

Elektronischer Hausfriedensbruch

Ein Einbrecher benutzt meistens die Tür, um in ein Gebäude einzudringen und nur selten das Fenster. Nie aber geht er durch die Wand. Die Tür entspricht in einem Computersystem der Paßwortabfrage, und Fenster gibt es so gut wie keine. Auch ein Hacker kommt nicht um diese Paßwortabfrage herum.

In der Regel hat man bei einer Paßwortabfrage drei Versuche, ein korrektes Paßwort einzugeben. Danach erfolgt der direkte Rauswurf aus dem System, und es muß erneut angewählt werden. Hat der Hacker kein gültiges Paßwort, wird er versuchen, es zu erraten. Bei drei Versuchen pro Anlauf sieht jeder ein, wie aussichtslos ein solches Unterfangen ist. Selbst wenn ein Hacker kostenfrei telefonieren kann, scheint es sinnlos, tagelang Wörter und Zeichen einzugeben. Wenn auf diese Weise trotzdem ein Hackversuch gelingt, kann man mit hoher Wahrscheinlichkeit davon ausgehen, daß der Hacker den Systembetreiber oder einen anderen Systembenutzer mit gültiger Zugangsberechtigung persönlich kennt. Es ist zwar nicht immer möglich, ein Paßwort durch eine Charakteranalyse zu ermitteln, doch kann man die ungefähre Richtung ausmachen und verringert so die Zahl der notwendigen Versuche deutlich. So mancher Systembesitzer ist immer noch blauäugig genug, den Namen der Freundin oder des Freundes als Zugangspaßwort zu benutzen.

Die meisten Systeme erleichtern dem Hacker die Arbeit, indem sie einen eingeschränkten Zugriff auch ohne Paßwort zulassen. Der sogennante 'Gast-ZugrifF ermöglicht es dem Benutzer, sich erst einmal in einem System umzusehen. Bei Unix-Betriebssystemen, die meist von Internetanbietern genutzt werden, wird dieser zusätzliche Service sehr häufig angeboten (Anonymous-Login).

Maden im Internet

Komplexe Betriebssysteme wie zum Beispiel Unix neigen auch dazu, komplexe Fehler zu haben. Und genau das sucht ein Hacker: den Fehler im System.

Viele Rechenzentren von Universitäten, die unter dem Betriebssystem Unix laufen und ihren Studenten, zumindest in Deutschland, kostenlosen Zugriff aufs Internet bieten, sind beliebte Ziele für Hacker. Betriebssysteme, die hauptsächlich für Netzwerke konzipiert worden sind, bieten in einigen Fällen jedem Interessierten die Zugriffsdaten völlig frei und fast unverschlossen an. Der einzige Schutz für die Paßwortdaten ist die Verschlüsselung durch einen mathematischen Algorithmus. Dessen Entschlüsselung bereitet jedoch nicht einmal Mathematikstudenten in niedrigen Semestern Schwierigkeiten. Ein Hacker, der nicht über diese mathematischen Kenntnisse verfügt, braucht nur der nächstbesten Internetseite, die eine Softwarelösung zur Entschlüsselung von Zugangsdaten bietet, einen Besuch abzustatten. Die gängigsten Programme zur Defragmentierung von Paßwörtern in Unix-Systemen sind 'CrackerJack' und 'Crack' von Alec Muffet. Allein mit deren Hilfe können sich unzählige Hacker kostenfreien Zugang zum Internet beschaffen, der eigentlich nur für eingeschriebenen Studenten der Universitäten gilt.

Ein Internetnutzer, der bemerkt hat, daß sein Zugriff ebenfalls von einem Hacker genutzt wird, kann dem Spuk ein Ende setzen, indem er den Systembetreiber auf den Mißstand aufmerksam macht. Dieser wird versuchen, das Problem schnellstmöglich zu beheben, oder dem Internetnutzer eine neue Zugangsberechtigung zukommen zu lassen.

Um an neue Zugangsberechtigungen zu gelangen, schleusen Hacker hin und wieder sogenannte **trojanische Pferde** in ein System ein. Dies sind intelligente virusähnliche Programme, die sich wie eine Spinne im System versteckt halten und sich von Zeit zu Zeit unmerklich Zugriffsdaten und Paßwörter schnappen, um diese dann vollautomatisch per EMail an den Hacker zu versenden. Das Rechenzentrum der Kölner Universität **(http://www.uni-koeln.de)** hatte fünf Jahre lang ein trojanisches Pferd im System, das mehrere Hacker mit Paßwörtern versorgte. Kein Systembetreiber ist während dieser Zeit dahintergekommen. Das Ende des Parasiten, der all die Jahre versteckt und unentdeckt im System schlummerte, wurde durch die zufällige Neukonfigurierung des Betriebssystems seitens der Systembetreiber besiegelt.

Bombenanschläge via EMail

Hacker mögen es, im Internet für Unruhe zu sorgen. Eine bei Hackern besonders beliebte und sehr unfeine Art des Terrors ist **Mailbombing.** Von der Szene eingerichtete Systeme, die ebenfalls dem Internet angeschlossen sind, geben ihren Mitgliedern und damit auch Hackern die Möglichkeit, EMail-Adressen von beliebigen Personen mit Daten zu bombardieren.

Ein besonders beliebtes Anwenderprogramm zur Bombardierung von EMail-Adressen ist unter anderem 'Kaboom', das man völlig legal aus dem Internet beziehen kann. Ein Mailpaket einer Größe bis zu einem Gigabyte wird der EMail-Adresse des Opfers mehrmals am Tage von einer anonymen Stelle aus zugesandt. Da kaum ein Internetanbieter diese riesigen Mengen an Datenmüll verkraften kann, sie aber dennoch weiterleiten muß, kommt es zu einem gewaltigen Datenstau. Hunderte von Systemen, durch die dieses Paket geroutet wird, werden gebremst oder brechen unter der Last der Daten zusammen und erleiden dadurch einen elektronischen Absturz (Crash). Solche Staus werden anderen Systemen automatisch gemeldet, die dann durch komplizierte Ausweichmanöver versuchen, den Stau großräumig zu umgehen. So kann es durchaus vorkommen, daß eine Nachricht einen weltweiten Umweg nehmen muß, um letztendlich doch wieder in derselben Stadt zu landen. Hunderte von Systemen werden durch solche Racheakte in Mitleidenschaft gezogen, was dem Hacker, der den Stau verursacht hat, oft ziemlich egal ist, solange seine Angriffsaktion auch den erreicht, dem sie galt.

Nach einer erfolgreichen Mailbombing-Aktion prasseln Hunderte von Beschwerdebriefen auf das Opfer ein, obwohl dieses vielleicht völlig ahnungslos und unschuldig ist. Da der Täter nicht zu ermitteln ist, wird die Schuld kurzerhand auf das Opfer abgewälzt. Um weitere Terror-Aktionen und die dadurch entstehenden Staus zu verhindern, wird dann der Internetzugang des Opfers schnellstmöglich gesperrt. Erst wenn das Opfer daraufhin seinen Internetzugang verloren hat, hört der anonyme Hackserver damit auf, Mailbomben zu versenden. Der Hacker hat ein Ziel erreicht. Der Anwender wird mit Pauken und Trompeten aus dem Internet hinausgeworfen. Derartige Bombardierungssysteme werden von verschiedenen Hackern auch dazu genutzt, ganze Anbieter lahmzulegen. Selbst Ausfälle dieser Art (Netsplits) sind im Internet durchaus an der Tagesordnung.

Spezialisierte Provider wie beispielsweise Xenologics in Köln können sich besser schützen als die Massenanbieter. Sie beenden den Terror nicht zu Lasten des Empfängers, sondern sind meist in der Lage, auf eine Beschwerde hin alle EMails des verdächtigen Absenders herauszufiltern, bevor sie ihr Ziel erreichen. Dabei hilft es dem Übeltäter auch nicht, wenn er seine EMail-Adresse fälscht. Über die Route, die seine Datenpakete zurücklegen, ist er leicht auszumachen und muß in diesem Fall selber mit Sanktionen rechnen.

Die Mailboxkiller

Legale Mailboxen, die nicht der Szene angehören, sind ein gefundenes Fressen für Hacker. Beim Eindringen in Mailboxen ist es allerdings nur selten das Ziel, an geheime Daten zu gelangen. Was hier zählt, ist eher der Spaß an der Zerstörung. Mailboxprogramme, die noch nicht vollständig von ihren Systembetreibern beherrscht werden, weisen automatisch Lücken auf, die Hacker nutzen. Einige Szenemitglieder haben es sich daher zur Angewohnheit gemacht, Mailboxen, die nicht nach ihrem Geschmack sind, zu verwüsten. Anleitungen, die auf bestimmte Fehler aufmerksam machen, sind in der Szene oft vorzufinden.

Zwei Systembetreiber aus Köln eröffneten sogar eine eigene Mailbox, nur um die Paßwörter ihrer Mitglieder für Hackversuche in fremde Systeme zu mißbrauchen. Indem sie die Eingabe des Paßworts am Bildschirm beobachteten, konnten sie sehen, ob es eingetippt wurde, oder über die Belegung einer Funktions-Taste blitzartig erschien, was eine Mehrfach-Benutzung nahelegte. Es war also die Einfallslosigkeit der Antragsteller, die den beiden Systembetreibern die Arbeit beim Hacken erleichterte und die Zerstörung oder Verwüstung vieler Mailboxen zur Folge hatte.

Hin und wieder kommt es auch vor, daß ehemalige Hacker, die nicht mehr der Szene angehören, versuchen, in Szenemailboxen zu gelangen. Die Verwüstung eines Elite-Systems ist jedoch schwer, da hier auf Schutzvorkehrungen besonders großer Wert gelegt wird. Hacker, die sich an Szenemailboxen vergreifen, verfolgen aber ohnehin ganz andere Ziele. Sie suchen Raubkopien und versuchen, unbemerkt an szeneinterne Informationen zu gelangen, um diese dann eventuell an die Polizei weiterleiten zu können. Meistens geben sie sich als bekannte Szenemitglieder aus und können durchaus auch stimmige Referenzen angeben. Szenemailboxen auszuspionieren ist aber keine leichte Arbeit und erfordert höchste Wachsamkeit. Daher ist es für einen ehemaligen Hacker, der sich in eine Szenemailbox einschleusen will, von großer Wichtigkeit, alte Kontakte wieder aufzufrischen. Gelegentlich greifen Hacker dabei auf altbekannte Methoden zurück. Trojanische Pferde zum Beispiel erfreuen sich auch hierbei großer Beliebtheit. Diese werden wie in Netzwerksysteme auch in die Mailbox eingeschleust. Und selbst mit einem niedrigen Systemstatus kann ein Hacker seinen Virus in einer Mailbox unterbringen. Das trojanische Pferd fischt sich dann wie eine versteckte Kamera alle Systempaßwörter aus der Mailbox heraus und sendet sie an den Hacker weiter. Solche Hacker sind häufig Mitarbeiter der Polizei oder ermittelnder Rechtsanwälte und oft auch ehemalige kriminelle Szenemitglieder. Es ist keine Seltenheit, daß gegen die Szene arbeitende Hacker früher selbst einmal belangt wurden.

Berufshacker

In Deutschland machte sich vor einiger Zeit eine Gruppe von Computerhackern mit spektakulären Einbrüchen in verschiedene Firmencomputer einen Namen. Die jungen Hacker wiesen auf Systemlücken hin, obwohl sie niemand dazu beauftragt hatte. Erst daraufhin wurden Firmen, für die Datensicherheit von äußerster Wichtigkeit ist, auf das Hackerproblem aufmerksam. Die Hackervereinigung, die durch ihre Arbeit einen regelrechten Sicherheitswahn ausgelöst hatte, ist heute zu einem der bekanntesten und größten Hackervereine der Welt mutiert, dem 'Chaos Computer Club' **(CCC),** auf den wir später noch eingehender zu sprechen kommen.

Ehemalige Hacker leisten heute im Bereich Computer qualifiziertere Arbeit als manche gelernte Fachkraft. Ein fünfundzwanzigjähriger Hacker beispielsweise, der seit Jahren sein Können durch illegale Aktivitäten geschult hat, ist einer Firma, die im Bereich Computersicherheit agiert, oft viel Geld wert. Wer könnte diese Arbeit auch besser erledigen als ein ehemaliger Hacker, der sich sein Wissen in der Szene angeeignet hat? Einige Hacker, wie Kim Schmitz (Kimble), haben in diesem Bereich eine Marktlücke entdeckt. Nachdem ihre Namen durch Polizei und Medien mehr oder minder in Verruf geraten waren, gaben sich viele von ihnen als Fachleute in Sachen Computersicherheit aus und boten ihre Kenntnisse zum Schutz vor elektronischen Einbrüchen an. Ihr Werbeslogan dabei lautete: 'Wer kann eine qualifiziertere Auskunft über die Sicherheit ihres Hauses geben, ein angelernter Angestellter oder ein ehemaliger Einbrecher?'

So entsteht ein irritierendes Arbeitsverhältnis: Firmen engagieren kriminelle Hacker, um sich vor denselben zu schützen. Leider geht diese Rechnung nicht immer auf, denn nur wenige der selbsternannten Sicherheitsfachleute sind ihrer Aufgabe auch tatsächlich gewachsen. Sicherlich wird sich kaum jemand imstande fühlen, die Arbeit eines Hackers nachzuvollziehen. Und die Frage, wie ein Hacker nun überhaupt zum erfolgreichen Abschluß seiner Arbeit kommt, bleibt meistens unbeantwortet. Ein Hacker arbeitet mit vielen kleinen Tricks, um Sicherheitsbarrieren in Systemen zu überwinden. Oft nutzt er nur die Leichtfertigkeit der Mitarbeiter einer Firma, um an erforderliche Informationen zu gelangen. Abgesehen von den unzähligen möglichen Methoden entstehen die meisten Erfolge im Hacken einfach nur durch glückliche Zufälle oder gar Fehler. In der Szene gibt es daher die Redewendung: 'Ein Hacker macht einen Fehler nur einmal versehentlich, dann aber immer mit Absicht.'

Aber welcher Hacker, der außerdem noch allein arbeitet, könnte in Anbetracht der unerschöpflichen Hackvarianten eine konkrete Auskunft über die Sicherheit eines Systems geben oder gar einen Täter dingfest machen? Dies wäre wohl nur dann in zufriedenstellendem Maße möglich, wenn sich der beauftragte Hacker zu einem Computer-Rambo entwickeln würde, dem selbst Institutionen wie Polizei oder Militär mit ihren Mitteln nicht das Wasser reichen könnten.

Es ist verständlich, daß ein von einer Firma beauftragter Hacker unter dem enormen Druck steht, wenigstens einen kleinen Erfolg vorweisen zu können. Dieser kommt häufig durch den vorbildlichen Arbeitsdrang einiger Mitarbeiter zustande, die eine Methode entdeckt haben, ihre Arbeit mit nach Hause nehmen zu können: Sie schließen ein Modem an den Computer ihres Büros an, damit es ihnen möglich ist, auch von zu Hause aus Zugriff auf das gesamte Netzwerk der Firma zu haben. So arbeiten sie dann sogar in ihrer Freizeit. Für eine Firma handelt es sich bei einem solchen Mitarbeiter sicher um einen willkommenen 'Hacker'; es gehört nicht viel dazu, zu erkennen, daß er in Wirklichkeit keiner ist. Es besteht aber die Gefahr, daß auch jeder Fremde auf das betriebsinterne System zugreifen kann, wenn er das Paßwort zum Bürocomputer des Angestellten kennt. Und genau hier schlägt der heuchlerische Computerspezialist zu. Denn statt sich um die Verbesserung der Sicherheit im Netzwerksystem zu kümmern, was sehr aufwendig wäre, macht er sich auf die Suche nach Bürocomputern, an die unerlaubterweise ein Modem angeschlossen ist. Mit einem Laptop unter dem Arm, der mit einem selbstgestrickten Programm ausgerüstet ist, findet der ehemalige Hacker problemlos alle an den Firmencomputer angeschlossenen Modems. Den Mitarbeitern drohen dann Tadel oder sogar Entlassung, während der ehemalige Hacker für eine gelungene Show bezahlt wird, ohne daß das Netzwerksystem der Firma einen Deut sicherer geworden ist.

Über eines sollten sich Firmen, die solche Scharlatane einstellen, also im klaren sein: Hacker, die sich als solche einen Namen machen konnten, suchen häufig nur nach dem einfachsten Weg zum Erfolg. Ein Hacker hat gelernt, Systeme zu überlisten, nie aber, sie zu schützen. Jede Firma, die einen solchen Hacker als Sicherheitsfachmann betrachtet und ihn einstellt, könnte durchaus einem Irrtum unterliegen.

In dieser Beziehung sind die Vereinigten Staaten der europäischen Industrie um einiges voraus. Dort gibt es Institutionen, deren Hacker auch tatsächlich kompetente Arbeit leisten. Sie sind nicht auf Erfolgsbasis tätig und stehen daher auch unter keinerlei Druck von Seiten des Arbeitgebers. Der Mitarbeiter einer Sicherheitsfirma arbeitet sich meist bis in das System des Kunden vor und hinterläßt eine Nachricht. Schließlich wird dem Kunden dieser Vorgang bis ins letzte Detail erläutert und eine passende individuelle Schutzmaßnahme ausgearbeitet. Diese Sicherheitsfirmen arbeiten in der Regel mit der Polizei und Detekteien zusammen. Die äußerst kostspielige Beauftragung eines solchen Unternehmens lohnt sich verständlicherweise nur bei dringendem Verdacht und ist einer kleineren Firma ohne entsprechende Mittel meistens nicht möglich.

Etwas Sinnvolles tun, eine Bank überfallen

Der Gedanke, das eigene Hobby zu Geld zu machen, liegt auch bei Szenemitgliedem sehr nahe. Leider ist das nicht immer mit einer legalen Aktivität verbunden. Ein Hacker ist sich in der Regel seines kriminellen Handelns nicht wirklich bewußt - in Szenekreisen ist elektronischer Hausfriedensbruch nun mal ein Kavaliersdelikt. Einige Hacker jedoch haben einen Weg eingeschlagen, der sich komplett von der Szene wegbewegt.

In Verbindung mit virtuellen Bankübefällen kam in den letzten Jahren vor allem auch das sogenannte 'Homebanking' ins Gerede, das angeblich nicht sicher sein soll. Die meisten Kreditinstitute bieten ihren Kunden diesen Service mittlerweile an, unter steten Beteuerungen absoluter Sicherheit.

Anscheinend gibt es aber Hacker, die eine Lücke entdeckt haben, um Überweisungen dem eigenen Konto gutzuschreiben. Vom Telefonverteilerkasten einer Wohnung aus ist es möglich, Telefonate der Nachbarn abzuhören. Dazu benötigt man eine Leitung, die parallel an der Telekommunikationsanlage klemmt. Da auch das Modem die Telefonleitung belegt, wäre es einem Hacker möglich, die Modemverbindung anzuzapfen und den Datentransfer auf seinem Computer zu beobachten. Ein Fernsehbericht zeigte, wie so etwas funktionieren könnte: Nachdem sich der sogenannte Hacker mit Computer und Modem an die Kommunikationsanlage im Keller des Hauses gehängt hatte, entschloß sich rein zufällig kurz danach ein Hausbewohner, eine Überweisung zu tätigen. Der Hacker beobachtete den Transfer im Keller und unterbrach die Verbindung des Nachbarn unmittelbar nach Eingabe der zweiten PIN (Persönliche Identifikations Nummer). Er hatte nun mit dieser PIN die Möglichkeit, seine eigene Kontonummer einzugeben und so die Überweisung auf sein Konto umzulenken. Auf den ersten Blick eine faszinierende Methode, die wohl sämtliche Zuschauer in Angst und Schrecken versetzt hat.
Eine andere, viel unkompliziertere Methode hätte den Hacker jedoch zum selben Ziel geführt: Man nehme einen Überweisungsauftrag, trage dort als Absender eine fremde Kontonummer ein und werfe diesen dann mit einer gefälschten Unterschrift in die Überweisungsbox der Bank. Der Effekt ist dergleiche - der überwiesene Betrag trifft einige Tage später genauso sicher auf dem eigenen Konto ein, wie die Kriminalpolizei vor der Tür steht. Vergessen wird nämlich gerne, daß man bei beiden Methoden eine Kontonummer angeben muß, um das Geld in greifbare Nähe zu bringen. Die Auflösung derartiger Fälle ist meist ein leichtes für die Polizei, denn anhand der Kontonummer kann man den Täter ohne weiteres ermitteln. Diese Tatsache wird gerne von den Medien verschwiegen - schließlich könnte man sich in Anbetracht der Fakten derartige Berichte gänzlich sparen.

Vor kurzem machte ein raffinierter Hacker Schlagzeilen, der sich einer typischen Hackermethode bediente: die Vortäuschung eines Paßworteingabefeldes, das in Wirklichkeit vom Hacker programmiert wurde. In diesem Fall war die perfekte Täuschung ein Computer mit einem Kartenlesegerät, der einem Geldautomaten zum Verwechseln ähnlich sah. Dieser wurde von dem Bastler in der Nähe der Bank aufgestellt und speicherte die Information sämtlicher Bankkarten mit den dazugehörigen Geheimnummern, die von ahnungslosen Kunden in den falschen Geldautomaten eingegeben wurden. Nach erfolgreicher Aufnahme der Daten wurde die Karte mit der Meldung herausgegeben, daß der Automat außer Betrieb sei. Mit dieser Methode war es dem Hacker möglich, die gespeicherten Daten auf Blankokarten zu speichern und mit der dazugehörigen Geheimnummer Gelder von fremden Konten abzuheben. Der Hacker wurde nur dadurch gefaßt, daß ein Kunde auf das in solch einem Fall unvermeidliche Stromkabel aufmerksam wurde und die Polizei verständigte.

Im Gegensatz zu Hackern, die sich zur Szene zählen und deren Aufgabenbereiche klar definiert sind, kann man Hacker, die sich für elektronischen Bankraub interessieren, nur als Ausnahmefälle betrachten, die eventuell unberechtigten Zugang zu Quellen der Szene gehabt haben könnten. Kapitalverbrechen mit Vorsatz paßt nicht ins Schema der Szene.

Sicher ist sicher!

Viele Benutzer fühlen sich durch solche Berichte der Medien beunruhigt und fragen sich, ob ihr System sicher gegen Hacker ist. Dabei sollte eines klar sein: Ein Computer ohne Modemanschluß, der nicht mit einem anderen System verbunden, also vernetzt ist, ist gegen jeglichen unbefugten Eintritt von außen gesichert. Da die Vernetzung eher bei Firmen, Universitäten oder Schulen üblich ist, kann der private Durchschnittsanwender nur durch sein Modem einer möglichen Gefahr ausgesetzt sein. Das Modem erlaubt ihm, vor allem durch das Internet, mit Millionen von Computersystemen in Verbindung zu treten. Nutzer des World Wide Webs können jedoch beruhigt sein, denn hier droht keine direkte Gefahr durch Hacker. Da durch das World Wide Web nur Daten empfangen, aber nicht ohne eigene Bestätigung gesendet werden können, ist es einem Hacker völlig unmöglich, Zugriff auf die Daten der Festplatte eines Internetnutzers zu erhalten. Natürlich sind selbst verursachte Fehler, die das eigene System zerstören können, nicht auszuschließen. So kann das Starten eines von Viren befallenen Programms, das aus einer unzuverlässigen Quelle kommt, Hardware zerstören und Software unbrauchbar machen.

Eine wirkliche Gefahr besteht nur für diejenigen Benutzer, die ihr System an ein Modem angeschlossen haben, um anderen Anwendern die Möglichkeit zu bieten, sich in das System einzuwählen. Aus dem aktiven wird nun ein passiver Benutzer, dessen System für jedermann offen steht. Um dies jedoch überhaupt möglich zu machen, ist ein Mailboxprogramm erforderlich. Und Mailboxsysteme sind nicht immer sicher. Einige weisen Lücken und Hintertüren auf, die sich jeder erfahrene Hacker ohne großen Aufwand zunutze machen kann. Hintertüren sind dazu da, um dem Systembetreiber bei Verlust des Paßworts den Eintritt in sein eigenes System von außen doch noch zu ermöglichen. Die Programmierer solcher Mailboxprogramme haben jedoch längst erkannt, daß diese Hintertüren Hackern nur noch mehr Möglichkeiten bieten, in fremde Systeme einzudringen.

So gab es ein bekanntes Mailboxprogramm mit dem Namen 'Phobos', das im Anfangsstadium von seinem Programmierer Ulrich Simon noch mit einer Hintertür versehen war. Diese Hintertür ließ sich bei der Demoversion, die frei erhältlich war, leicht ausfindig machen. Um die Einführung neuerer Versionen von 'Phobos' auf dem Markt nicht zu gefährden, entschloß sich Simon, bei weiteren Versionen seines Mailboxprogrammes völlig auf Hintertüren zu verzichten. Heutige Mailbox-Programmierer planen Hintertüren erst gar nicht mit ein.

Hat es ein Hacker auf ein sicheres System abgesehen und mit wahllosen Paßworteingaben kein Erfolg gehabt, muß er, auf welchem Wege auch immer, in Kontakt mit dem Systembetreiber treten. Die Arbeit eines Hackers ist in diesem Fall eher mit der eines Spions zu vergleichen. Wenn ein einbruchsicheres System trotzdem erhackt wurde, kann man mit hoher Wahrscheinlichkeit davon ausgehen, daß sich Opfer und Hacker persönlich kannten. In vielen Fällen sind die Besitzer solcher Systeme nur zu nachlässig gewesen und haben zu vielen unbekannten Besuchern den Zugriff erlaubt. Der Hacker ist in einem solchen Fall kaum noch zu ermitteln.

Kryptographie

Die beste Art, sich gegen unbefugten Zugriff auf die eigenen Daten zu schützen, ist die Methode der Verschlüsselung. Mit einem komplizierten mathematischen Algorithmus ist es möglich, beliebige Daten, Texte oder Bilder mit einem Paßwort zu versehen, um sie für Fremde unlesbar zu machen. Dies ist für Nachrichtendienste und andere geheime staatliche Einrichtungen geradezu unverzichtbar. Aber auch private Anwender sind darauf gekommen, ihre Daten zu verschlüsseln, um sie effektiver vor Fremdeingriffen zu schützen.

Eine verschlüsselte Datei, deren Paßwort unbekannt ist, sollte in der Regel nicht zu knacken sein. Dennoch gibt es Hacker, die sich durch ihre enormen mathematischen Fähigkeiten auf das Entschlüsseln derartig codierten Nachrichten spezialisiert haben. Bislang gab es noch keine Zeichenkombination, die nicht gelöst worden wäre. Es war stets nur eine Frage der Zeit.

Ein wahres Genie auf seinem Gebiet ist Philip R. Zimmermann, ein Ingenieur mit über zwanzig Jahren Programmiererfahrung. Er hat sich auf Echtzeitsysteme, Kryptographie, Authentisierung und Datenaustausch spezialisiert. Seine Arbeit umfaßt Design und Implementierung der Authentisierungssysteme für Informationsnetze, Netzdatensicherheit, Schlüsselmanagementprotokolle, Simultanbetrieb mit Echtzeitzugriffsleitprogrammen, Betriebssysteme und lokale Netzwerke. Für internationalen Gesprächsstoff sorgte Zimmermann mit der Entwicklung eines einzigartigen Verschlüsselungsprogramms, das mit heutigen technischen Möglichkeiten noch nicht entschlüsselt werden kann: PGP (Pretty Good Privacy).

PGP wurde ursprünglich für den privaten Benutzer entwickelt, der seine Daten vor fremdem Zugriff schützen wollte. Im EMail-Bereich sollte PGP Anwendern ermöglichen, Nachrichten verschlüsselt zu senden. Wie alle neuen Verschlüsselungsarten wurde auch diese von den amerikanischen Geheimdiensten auf ihre Wirksamkeit untersucht und geprüft. PGP ließ schon relativ bald sämtliche Alarmglocken schrillen, denn es stellte sich heraus, daß Daten, die in PGP codiert werden, praktisch nicht zu knacken sind. Selbst ein Supercomputer der heutigen Zeit würde zwanzigtausend Jahre benötigen, um eine Datei, die mit PGP codiert worden ist, zu decodieren.

Die US-Regierung hat schon in vielen Fällen die Benutzung guter kryptographischer Technologie verboten, dazu gehört auch Philip Zimmermanns PGP 2.6.3. Software dieser Art wird in Amerika wie Kriegsmaterial gehandhabt und fällt unter das Waffenexportgesetz. Aus diesem Grunde wurde es strengstens verboten, diese Version von PGP aus den USA, auf welchem Wege auch immer, in ein anderes Land zu exportieren und zu benutzen. Jemand, der seine EMails mit PGP 2.6.3 codiert und dessen Nachrichten von Geheimdiensten in den USA abgefangen werden, kann unter Umständen Schwierigkeiten bekommen.

Um den Fortbestand seines Unternehmens nicht zu gefährden entwickelte Philip Zimmermann auf Betreiben der US-Regierung die Version PGP 5 mit 'Key Recovery', das heißt, es gibt eine Hintertür, die einen Zugang, zum Beispiel für nachrichtendienstliche Entschlüsselung offenhält. Mit dem Verkauf von PGP an eine Firma, die zum Teil von Regierungsaufträgen lebt, wird sich diese Entwicklung wohl fortsetzen.

PGP 2.6.3 ist freeware, und jeder kann die Vollversion des Programms aus dem Internet beziehen und zumindest noch in Europa völlig legal benutzen. Auf folgenden Internetseiten kann jeder PGP 2.6.3 für Systeme wie Windows, Macintosh oder Amiga downloaden:

http://www.pgpi.com

http://www.cryptography.org/getpgp.htm

Beginnend mit der PGP-Version 2.o erfolgte die Verbreitung der Software auch außerhalb der USA auf allgemein zugänglichen Computern, noch bevor die USA ein generelles Verbot durchgesetzt hatten. Kundenspezifische Versionen der Kryptographie- und Authentisierungsprodukte und der allgemeinen Schlüsselimplementierungen von Zimmermann, sowie kundenspezifische Produktentwicklungsdienstleistungen kann man auch direkt von folgender Homepage bekommen: **http://www.pgp.com**

Vor allem die Szene nutzt heutzutage PGP 2.6.3, wenn es um die Abwicklung illegaler Geschäfte via EMail geht.

Wie werde ich zum Hacker?

Hacker zu sein bedeutet nicht immer, böse zu sein. Ein Hacker kann auch viel Gutes tun. Diese Ansicht zumindest vertritt der Chaos Computer Club, der dies auch deutlich unter Beweis stellen konnte. Die Besucher auf ihrer Homepage im Internet werden mit 'Willkommen, Hacker' begrüßt: **http://www.ccc.de**

Und so stellt sich der Chaos Computer Club e.V auf seiner Homepage selbst vor: 'Der Chaos Computer Club versteht sich als Kommunikationsplattform für Hacker, sowie solche, die es werden möchten. Angesprochen sind alle technisch interessierten Menschen, wobei aber nicht nur die Chancen der Technik, sondern auch die Risiken und Auswirkungen auf die Gesellschaft vom Chaos Computer Club untersucht werden. Der Chaos Computer Club veröffentlicht seine Ergebnisse in Zusammenarbeit mit allen Medien sowie auf allgemeinen Veranstaltungen, Fachkongressen und politischen Anhörungen, zum Beispiel vor dem Ausschuß für Post und Telekommunikation des Deutschen Bundestages. Der Chaos Computer Club steht ebenso in der Lobbyliste des Deutschen Bundestages und vertritt damit die Interessen von Hackern, Netzwerkern und Online-Bürgern im besonderen.'

Wer Mitglied im Chaos Computer Club werden möchte, der kann das mit einem gewöhnlichen Antragsformular und einem Jahrebeitrag von 120 Mark problemlos tun. Damit erhält man auch die Möglichkeit, in Kontakt mit Leuten zu treten, die in diesem Bereich viel Erfahrung sammeln konnten. Außerdem kann man als Mitglied die Clubzeitschrift 'Die Datenschleuder' kostenlos abonnieren, die auch so manche Insider-tricks verrät. Der Chaos Computer Club ist aber nicht als eine Art Einstieg in die illegale Szene mißzuverstehen. Vielmehr sind dort Hacker zu finden, die ihre kreative Energie am Computer dazu nutzen, einige technische und politische Machenschaften mit kritischem Blick zu betrachten.

Den schnelleren Einstieg in die Welt der Hacker bietet aber trotzdem die illegale Szene. Dort sind die hartgesottenen Hacker zu finden, die schon so manchen großen Schaden angerichtet haben. Hacker treiben sich auch häufig im Internet herum, wo sie Informationen austauschen. Unter dem Service World Wide Web des Internets findet man mit Hilfe der Suchmaschine **http://www.yahoo.com** Internetseiten von Hackern. Es empfiehlt sich, einfach den Begriff 'Hacker' als Suchbegriff einzugeben. Unter dem Service Internet Relay Chat (IRC) kann man ebenfalls Hacker antreffen, die jedoch unter sich bleiben wollen. Dazu ist es nötig, in das EfNet des Internet Relay Chat (IRC) zu gelangen. Diesen völlig legalen Zugriff bieten IRC Server wie:

irc.funet.fi

irc.fu-berlin.de

irc.stealth.net

Dort muß man versuchen, die speziellen Chatkanäle ausfindig zu machen, die nicht in Listen eingetragen sind, da sie geheim genutzt werden. Von Insidern empfohlene Chatkanäle sind:

#amielite
#thescene
#hack
#phreak

Hacker im Visier der Justiz

In den 80er Jahren entwickelte sich Hacken in der Szene zu einer Art Volkssport, und nur den besten Hackern war es möglich, über all die Jahre unentdeckt zu bleiben. Fast jeder langjährige Hacker hatte irgendwann in seinem Leben schon einmal Probleme mit der Polizei. Und es gibt nicht wenige Hacker, die nach einer solchen Begegnung, bei der sie noch einmal mit dem Schrecken davon gekommen sind, ihr illegales treiben eingeschränkt haben. Wer einmal eine Hausdurchsuchung miterlebt hat, denkt lieber ein zweites Mal über einen Neueinstieg in die illegale Szene nach.

Das Hackerproblem ist wohl noch zu jung, als daß die Justiz wirklich begriffen hätte, wie sie mit diesem Personenkreis am besten verfährt. Denn rein rechtlich gesehen sind viele Hacker Kriminelle, doch die Betrachtung aus einem anderen Blickwinkel zeigt, daß die Realität meist ganz anders aussieht. Häufig brechen Hacker in fremde Systeme ein und hinterlassen bloß eine kleine Nachricht, ähnlich der Fahne eines Bergsteigers, der einen Berg zuerst erklommen hat. Es ist wohl nicht nötig zu erklären, daß solche Hacker keinen reellen Schaden anrichten. tyotzdem fühlen sich viele Institutionen durch diese unerlaubten Besuche geschädigt und fordern Schadensersatz und strengere Strafen. Es mag für viele nur schwer nachvollziehbar sein, aber der Großteil der Hacker arbeitet rein zum Spaß. Nur ein ganz kleiner Prozentsatz derer, die das computerspezifische KnowHow haben, nutzen diese Fähigkeiten zur eigenen Bereicherung.

Ganze Arbeit in Sachen Hacken leisten auch polizeiliche Institutionen. Diese haben natürlich eigene Hacker angestellt, die mit ihrer Erfahrung andere Ziele verfolgen als die Verwüstung anderer Systeme. Sie ermitteln gegen illegale Hacker. Feuer bekämpft man nun mal am besten mit Feuer. Wird die Polizei auf der Suche nach Hackern fündig, stehen für die Betroffenen hohe Strafen an.

Eine bekannte und traurige Geschichte handelt von einem jungen Computerhacker namens Karl Koch. Seine kurze Lebensgeschichte war die Grundlage für den Film '23'. Im Jahre 1986 schaffte Koch es, sich in den Zentralcomputer des Pentagons einzuhacken und verkaufte die gestohlenen Informationen angeblich an den KGB. Das blieb nicht lange unentdeckt. Polizei und Geheimdienste waren ihm auf den Fersen, und der junge Karl Koch, der durch seine Aktionen einen der größten Spionagefälle der deutschen Geschichte angezettelt hatte, nahm sich, überfordert durch den Druck, dem er ausgesetzt war, nur drei Jahre nach seinen ersten großen Hacks das Leben, indem er sich mit Benzin übergoß und anzündete - so lautet jedenfalls die offizielle Version.

Die Geschichte von Karl Koch ist nicht nur aufgrund ihres tragischen Ausgangs eine Ausnahme. Es kommt einfach nicht alle Tage vor, daß sich ein Hacker in einen Computer der Größenordnung des Hauptcomputers des Pentagon einschleichen kann. Dafür sind die Sicherheitsvorkehrungen zu groß und die Strafen für einen aufgeflogenen Versuch zu hart. Viele Hacker sind - oftmals ohne genau zu wissen, was sie wirklich angestellt hatten - für mehrere Jahre hinter Gitter gewandert. Die Bestrafung dieser zum Teil sehr jungen Leute ist eine reine Prestigeangelegenheit des Rechtsstaates. Verschwiegen wird nämlich, welchen Nutzen die Gesellschaft hatte. Denn Hacker wie Karl Koch lieferten mit ihren Aktionen wohl die größten Beiträge zur Sicherheit öffentlicher Computersysteme überhaupt. Sie machten auf Probleme aufmerksam, die vorher noch gar nicht erkannt worden waren. Der Zentralrechner des Pentagon zählt heute zu den sichersten der Welt. Ohne die Erprobung durch Hacker wäre der heutige Sicherheitsstand niemals erreicht worden.

So ist es heutzutage eher eine Seltenheit, daß ein Hacker größeres Aufsehen erregt. Die Schäden, die in den letzten Jahren angerichtet wurden, mögen schwerwiegend gewesen sein, doch diese Zeiten sind vorbei. Das Problem wird eher durch dumme Propaganda aufgebauscht. Hacker, die es über Jahre geschafft haben, in fremde Systeme einzudringen, stehen inzwischen vor immer größeren Barrieren und schwierigeren Aufgaben. Die Hackerszene hat sich dadurch beruhigt, ihre Protagonisten sind vernünftiger geworden. In der Szene selbst sind daher die Hacker, die zerstörerisch in fremde Systeme eindringen können, ebenfalls fast nur noch Legende.

Wenn auf einer Szeneveranstaltung solch ein Hacker auftaucht, wird seine Anwesenheit betuschelt. 'Der Hacker' ist mittlerweile auch in Insiderkreisen ein Mythos, und es gibt Hunderte von mehr oder weniger wahren Geschich-

ten, die man sich über ihn erzählt.

Die Demoszene ist eine Organisation,
die den Blick gen Zukunft gerichtet hat,
ihr größtes Potential ist die Kreativität.
Freundschaft, Toleranz und positives
Denken sind die Leitfäden der Mitglieder,
die sich in ihr bewegen. Diese Motive
sollten Respekt verdienen.

Marcus Farle, Veranstalter

Hauptsache Spaß

Vom Cracker zum Coder

Nach all den Hackern, Phreakern und Crackern mag es wohl schwer sein, sich eine ganz andere Seite der Szene vorzustellen. Eine Seite, die sich vom illegalen und kriminellen Handeln anderer Szenemitglieder distanziert und trotzdem nicht ohne sie existieren kann: die Demoszene, auch 'legale Szene' genannt.

Einen Einblick in diesen Teil der Szene zu bekommen, ist um ein Vielfaches einfacher, denn Versammlungen und Parties sind in der Regel für jedermann zugänglich. Das ist wohl einer der Gründe dafür, daß die Demoszene in den letzten Jahren von der Presse als eher uninteressante Begleiterscheinung der Szene rezipiert wurde - sie war einfach nicht geheimnisvoll genug. Irgendwie ist es auch verständlich, daß einem siebzehnjährigen Jungen, der sich in einen CIA-Computer einhackt, mehr Aufmerksamkeit geschenkt wird als einem scheinbar durchgeknallten Programmierer, der seine Zeit und sein Talent damit 'verschwendet', titschende Bälle und rotierende Würfel auf einem Bildschirm zu erzeugen.

Im Vordergrund der Demoszene steht, wie sollte es auch anders sein, die **Demo.** Um zu verdeutlichen, was eine Demo ist und wer sie macht, muß man die Geschichte kennen, die die Demo durchlaufen hat. Und diese beginnt, wie in diesem Buch geschildert, in der illegalen Szene.
Die ursprüngliche Motivation eines Softwarecrackers, einen Kopierschutz zu entfernen und das entsicherte Programm in Umlauf zu bringen, war nicht immer nur Geld. Der wirkliche Anreiz für die Mühen manch durchgemachter Nacht war der Ruhm in der Szene. Schneller und besser zu sein, vor allen Dingen aber bekannter zu werden, waren die treibenden Kräfte, die Cracker zu Höchstleistungen anspornten. Um jedem mitzuteilen, wer nun das Programm gecrackt hatte, versuchte der Cracker, seinen Namen an irgendeiner Stelle des Programms unterzubringen. Der beste Platz dafür war der vor dem Programm, denn nur so war gewährleistet, daß jeder, der das gecrackte Programm startete, zuerst den Namen des Crackers zu Gesicht bekam. Die Cracker entwarfen also kleine Vorspanne, in denen der Name des Crackers und das Datum des Cracks vermerkt wurden. Diese Vorspanne, in der Szene 'Intros' genannt, waren zunächst recht lieblos und unspektakulär gestaltet. Oft waren es nur starre Bilder mit kleinen Texten darunter, die sich bei edleren Vorspannen vielleicht einmal in Zeitlupentempo von rechts nach links bewegten.

Mit der Zeit begannen die Softwarecracker, immer größeren Wert auf das Erscheinungsbild ihrer Vorspanne zu legen. Die Intro war schließlich die eigene Leistung, Verpackung und Präsentation zugleich. Bald verbrachten Cracker mehr Zeit damit, den Vorspann zu gestalten, als den Kopierschutz zu entfernen. Die Bilder fingen schließlich an, sich auf und ab zu bewegen, Texte wanderten hin und her **(Scrolltext)** und schließlich kam auch Musik hinzu. Die Cracker damals konnten natürlich nicht wissen, daß sie damit den Grundstein zu einer produktiven und ausschließlich legalen Szene legten.

Man kam auf immer neuere und verblüffendere Ideen. Aber je mehr man in einen solchen Vorspann hineinpacken wollte, desto mehr Platz schluckte er. Das wurde zu einem Problem, denn die Hersteller programmierten ihre Software so, daß nicht mehr viel Platz auf einer Diskette übrig blieb - schon gar nicht für einen zusätzlichen Vorspann. Es entstand ein neuer Wettbewerb. Man versuchte, bessere und größere Effekte auf möglichst wenig Platz unterzubringen. Optimierung des eigenen Vorspanns war dabei nicht immer die beste Lösung. Oft optimierte der Cracker sogar die Software selbst, um mehr Platz auf dem Datenträger zu bekommen. Dadurch konnte es durchaus vorkommen, daß eine Raubkopie besser lief als das Original.
Die Programmierer solcher Vorspanne machten sich in den frühen Achtzigern einen großen Namen in der Szene und sind bis heute bekannt. Ihre Effekte waren zu der damaligen Zeit bahnbrechend und bildeten die Grundstufe der Computerspiele der heutigen Zeit. Würfel bewegten sich auf dem Bildschirm, geometrisch angeordnete Punkte bildeten Schlangen, Kreise und Spiralen. Wie ein Effekt entstanden war, war völlig egal. Ob Können oder Zufall, das einzige, was zählte, war die Innovation.

Die Popularität der Intros wuchs. Viele Leute, sowohl Szenemitglieder als auch Außenstehende, bewunderten die Künste dieser Programmierer, und der Bedarf an größeren, schnelleren und besseren Effekten nahm zu. Der

Vorspann bekam einen Eigenwert und war nicht mehr Mittel zum Zweck. Viele Cracker erwarben sich mit ihren Vorspannen mehr Ruhm als durch das Cracken von Programmen. Einige entschlossen sich deshalb, ihre Arbeit einzig und allein auf das Programmieren von Intros zu konzentrieren. Sie gründeten neue Gruppen in der Szene, die sich von nun an auf völlig legalen Bahnen bewegten.

Es entstand eine Art Arbeitsteilung. Der Programmierer einer Demo, in der Szene 'Coder' genannt, hatte Spezialisten, die sich ausschließlich um die Musik und die Grafik kümmerten. Damit hatte er mehr Zeit zur Verfügung, um sich auf den eigentlichen Teil seiner Arbeit zu konzentrieren. Die Intros wurden größer und eigenständig. Damit war das Wort 'Intro' oder 'Vorspann' nicht mehr treffend und die mittlerweile zu Demonstrationen ausgearteten Produktionen bekamen ihren heutigen Namen 'Demo'.

Demos: Die elektronische Kunst

Mittlerweile gehört kein programmiertechnisches Verständnis mehr dazu, diese Demos zu bewundern. Sie ähneln Videoclips und erzählen oft auch kleine Geschichten. Der rotierende Würfel ist in der Intro inzwischen eine Rarität geworden, und seinen Platz nehmen nun atemberaubende Tunnelfahrten und komplex umhertanzende Figuren ein. Die Coder, Grafiker und Musiker haben sich selbst auf ein so hohes kreatives Niveau katapultiert, daß die Medienindustrie langsam aber sicher auf sie aufmerksam wurde. Computerspezialisten behaupten, daß eine Demo die multimedialen Fähigkeiten eines Computers am besten hervorheben kann.

Was ist aber nun der grundlegende Unterschied zwischen einer Multimedia-Präsentation und einer Demo? Eine Demo besteht aus einem programmierten Code und nicht aus einer Animation. Animationen sind gezeichnete Bilder, die nacheinander abgespielt werden, wie in einem Zeichentrickfilm. Diese können mit Hilfe eines speziellen Programms angefertigt werden. Daher benötigt man für ihre Herstellung keine Programmiererfahrung, sondern es genügen allgemeine Computerkenntnisse. Die Anfertigung einer Demo dagegen verlangt ungewöhnlich große Programmierkenntnisse. Diese setzt nämlich die Anwendung der Maschinensprache **Assembler** voraus.

Aber nicht nur die Kenntnis der Programmiersprache, sondern auch eine überdurchschnittliche Kreativität ist erforderlich. Und eine Demo, die mit vorberechneten Daten arbeitet, wird in der Szene nicht als Leistung anerkannt. Hier ein stark vereinfachtes Beispiel für die Aufgabe eines Coders: Eine Kugel in einer Demo dreht sich, während der Computer die Drehbewegung zeitgleich mit der Ausgabe auf dem Bildschirm berechnet, also in Echtzeit. Sobald andere Faktoren, wie zum Beispiel komplexe Lichtquellen, hinzukommen, wird die Ausgabe auf dem Bildschirm langsamer und der Coder muß sich Tricks einfallen lassen, um den Computer zu entlasten.

Es ist immer der Coder, der bei der Herstellung einer Demo die Hauptarbeit leistet. Hat irgendein Szenemitglied auf der Welt einen neuen Effekt entdeckt, muß der Coder versuchen, herauszubekommen, wie dieser funktioniert; erklären wird es ihm kaum einer. In aller Regel ist er es, der die Qualität der Demo durch sein Können bestimmt. Denn eine schlecht programmierte Demo kann noch so schöne Musik oder Bilder haben, niemand wird ihr sonderlich große Beachtung schenken. Schlechte Qualität kann neben einem schwachen Design bedeuten, daß ein komplizierter Weg gewählt wurde, wo auch eine simplere Möglichkeit der Programmierung zum gleichen Ziel geführt hätte. Man kann den Programmieraufwand in einer Demo zum Beispiel daran erkennen, wie sich die Figuren bewegen.

Wie man mit der Arbeit an einer Demo beginnt, ist unterschiedlich. Es gibt Coder, die es bevorzugen, die Demo direkt auf die Musik abzustimmen. Andere machen ihre Arbeit zuerst und lassen dann den Musiker etwas komponieren. In vielen Fällen scheitert die Demo auch schon bei der Planung. Alle Leute, die an einer Demo mitwirken, müssen ständig auf dem Laufenden gehalten und vor allem motiviert werden. Das ist oft keine leichte Aufgabe. Dieser Job wird von dem Hauptorganisator einer Gruppe erledigt. Ständig muß er sich darum kümmern, daß alle Arbeiten rechtzeitig erledigt werden. Die Idealsituation wäre, wenn alle Beteiligten einer Demo nicht nur in demselben Land, sondern auch in derselben Stadt leben würden. Leider ist das nur sehr selten der Fall. Da der direkte Austausch unter den Beteiligten unverzichtbar ist, bietet das Internet die beste Lösung für dieses Problem. Hier können sich auch weit voneinander entfernt lebende Szenemitglieder treffen und Vorabversionen ihres Projektes austauschen. Für alle Arbeiten gibt es einen festen Zeitplan, denn der Erscheinungstermin einer Demo ist oft vorher festgelegt. Meist fällt er direkt mit einer Party zusammen. Eine Party ist ein äußerst wirkungsvoller Erscheinungstermin für eine Demo, denn hier kann eine Gruppe ihr Produkt und sich im Rahmen von Wettbewerben publik machen.

Wenn die Szene feiert

Einmal im Jahr wird wechselweise einer der drei kleinen Orte Aars, Fredericia oder Heuring in Dänemark für je-

des Szenemitglied, legal oder illegal, zum Mittelpunkt der Computer-Welt. Zwischen Weihnachten und Silvester findet dort das größte Szenetreffen der Welt statt. Tausende von Hackern, Phreakern, Tradern, Codern, Grafikern und Musikern reisen oft um den halben Globus, um an diesem Ereignis teilzunehmen. Dieses gigantische Treffen, in der Szene als 'The Party' bekannt, ist ein organisatorischer Geniestreich. Dabei sind die meisten Organisatoren der Party kaum älter als 23. Presse und Fernsehen sind häufig anwesend, um das Ereignis zu dokumentieren. Auch die führenden Leute der Softwarefirmen kommen auf diese Party und nutzen die Gelegenheit, neue Talente anzuwerben. Mehr Informationen über 'The Party' sind jährlich zwischen November und Januar zu finden unter der Homepage:

http://www.theparty.dk

Derartige Parties finden meist in riesigen Hallen statt. Für 'The Party' in Dänemark werden schon seit Jahren Messehallen angemietet, um die enormen Menschenmassen fassen zu können.

Szenemitglieder erscheinen ständig auf irgendwelchen kleineren oder mittelgroßen Parties rund um Europa, um ihren Bekanntheitsgrad zu sichern. Doch das wäre wohl kaum Grund genug für ein Szenemitglied, eine stundenlange Reise auf sich zu nehmen. Im Mittelpunkt steht der Spaß an der Sache: Szenemitglieder treffen, alte Gesichter wiedersehen, neue Freundschaften schließen und vor allen Dingen die Arbeit der anderen bewundern und begutachten. Da die meisten Szenemitglieder Autodidakten sind, nutzen viele diese Gelegenheit, um sich neues Wissen anzueignen. Häufig steht man vor

Problemen, die man selbst nicht lösen kann. Hier steht der Austausch mit anderen Szenemitgliedern an erster Stelle. Natürlich wird keiner dem anderen die eigenen Spezialtricks verraten, doch der eine oder andere T1p wird hier und da gegeben.

Für einen Außenstehenden mag die Vorstellung, bei einer Party anwesend zu sein, auf der nur Computerfreaks herumgammeln und sich in hermetischer, fast wissenschaftlich erscheinender Sprache über abstruse Themen der Computerwelt unterhalten, dem Effekt einer Valiumtablette gleichkommen. Ganz so ist dem aber nicht. Die verbreitete Vorstellung, daß auf einer solchen Veranstaltung nur Menschen mit Hornbrille und Pickeln umhergeistern, ist absoluter Nonsens. Ebenso falsch wäre es allerdings, das Gegenteil zu behaupten. Den Durchschnitts-Szenetypen kann man nun mal nicht ermitteln, und das aus einem ganz einfachen Grund: es gibt ihn nicht. Man trifft Menschen, von denen man nicht einmal denken würde, daß sie der Programmierung eines Videorekorders mächtig seien, und nicht selten sind es genau diese, die die absolute Computerelite darstellen. Die Bandbreite reicht von Punker bis Papa, von scheinbar normal bis total übergeschnappt, von jung bis alt. Es ist einfach alles vertreten, was das bunte Leben zu bieten hat. Toleranz wird in der legalen Szene nicht nur mit großen, sondern auch mit fetten Lettern geschrieben.

Auf vielen Parties im deutschen Raum kann man sogar den bekannten und berüchtigten Rechtsanwalt Günter von Gravenreuth antreffen, von dem böse Zungen sagen, er sei der Szenefeind Nummer Eins. Doch was auch immer seine Motivation ist, eine Szeneparty zu besuchen, sei sie beruflicher Natur oder rein privat: auf eine gewisse Weise ist er immer willkommen, wie ein alter Freund der Familie. So kommt es nicht selten vor, daß Jäger und Wild zusammen an einem Tisch sitzen und sich gegenseitig zuprosten. Auf einer Szeneparty hat jeder freies Geleit. Irgendwie macht er es selbst den illegalen Szenemitgliedem, die das Glück hatten, ihm noch nicht auf beruflicher Ebene zu begegnen, schwer, ihn nicht zu mögen. Denn wer von Gravenreuth schon einmal auf einer Party erlebt hat, kann bezeugen, daß er für jeden Spaß zu haben ist. Auf der 'Rainbow Party' in Aachen ließ er sich zu einer Runde Fußball überreden und dribbelte seine Kontrahenten gekonnt aus. Es ist wohl seine unermüdliche Art, die ihm in einer Ausgabe des 'Amiga Joker Computermagazin' den Titel 'Partylöwe' einbrachte. Seine Aufkleber mit der Aufschrift 'Don't spread illegal copies, Gravenreuth is watching you!' (zu deutsch: Bring keine Raubkopien in Umlauf, Gravenreuth sieht Dich!) werden mittlerweile hoch gehandelt. Von Gravenreuth, von der legalen Szene **Günni** genannt, gehört zumindest in der deutschen Szene fast schon zum Inventar. Auf der 'Coma Party' in Köln liefen ihm einige wildgewordene Szenemitglieder hinterher, um sich ein Autogramm auf ihr Mousepad geben zu lassen. Von Gravenreuth würden wohl die letzten grauen Haare ausfallen, wenn er wüßte, wieviele illegale Aktionen schon auf diesen Mousepads, die er signiert hat, gelaufen sind.

Wie vielfältig das Spektrum an Besuchern auch ist, man muß wohl ein wenig verrückt sein, um sich diesem Haufen anzuschließen. Was geht im Kopf eines Coders vor, der zwei Tage und Nächte auf seinen Computer eingetippt hat, um dann zu sehen, daß nichts so läuft, wie er es sich vorgestellt hat? Oft sieht man Leute, die den Abdruck ihrer Tastatur im Gesicht haben, weil sie vor lauter Schlafentzug erschöpft auf ihrem Rechner zusammengebrochen sind.

Neben der Riesenmenge an Computern, die von den Besuchern zu einem Partyplatz mitgeschleppt werden, finden sich noch allerhand andere Gerätschaften, die man zum täglichen Überleben braucht. Auf größeren Parties mit über zweitausend Besuchern sind Kühlschränke, Elektroherde und Fernseher keine Seltenheit. Hin und wieder kommt es dann auch zu Streitigkeiten, weil zum Beispiel Mikrowellen als Störsender die Funktion von Monitoren beeinträchtigen. Platzprobleme lassen andere zu wahrhaftigen Zirkusakrobaten werden. Eine Mikrowelle, der halsbrecherisch über einem Monitor schwankt und eine Pizza nach der anderen ausspuckt, interessiert den am Computer sitzenden Coder nur wenig. Er ist nur darauf bedacht, daß, falls die Mikrowelle herunterfallen sollte, seine Tastatur keinen Schaden nimmt. Deshalb bastelte er sich ein Mikrowellenfall-FrühwarnSystem, das aus einer Schnur und einer Kuhglocke besteht, die an der Mikrowelle und am Fernseher des Nachbartisches befestigt ist. Wenn die Mikrowelle nun langsam nach vorne wegrutschen sollte, bimmelt die Glocke, und der Coder hat

noch genügend Zeit, die bevorstehende Katastrophe abzuwenden. Es bleibt ein Rätsel, wer auf die sinnlose Idee kam, eine Kuhglocke mit auf die Party zu nehmen.

Jeder will auf einer Party gegen alle erdenklichen Fälle gewappnet sein, und so nimmt man einfach alles mit, was irgendwie brauchbar ist. Und wenn man etwas nicht braucht, nimmt man es trotzdem mit, um die anderen Besucher zum Lachen und Staunen zu bringen. Jeder inszeniert sich selbst, je verrückter, desto besser. Denn verrückt ist lustig, und Spaß wollen alle haben.

Wer einmal in seinem Leben eine Party miterlebt hat, wird dieses Erlebnis in Erinnerung behalten und den Sinn dieser Veranstaltungen besser verstehen. Wie bei vielen Dingen im Leben ist es schwer zu erläutern, worin der Reiz einer Szeneparty besteht. Parties finden in der Regel über einen Zeitraum von mehreren Tagen statt, was auch nötig ist. Denn die Vielfalt des Programms auf einer solchen Party ist so groß, daß man sich kaum traut zu schlafen, um bloß nichts zu verpassen. Das Angebot geht von Tanzeinlagen auf der Bühne bis hin zu Sportturnieren wie Modem-Weitwurf oder Computer-Fußball auf dem Vorplatz des Partygeländes. Die Organisatoren der Parties lassen sich immer wieder etwas Neues einfallen, um ihre Party zu einem unvergeßlichen Event zu machen. So gibt es immer wieder verrückte Wettbewerbe, wie zum Beispiel den 'Computer-Zerstör-Wettbewerb', der auf der 'Saturne Party' in Paris viele Szenemitglieder wie gewalttätige Monster aussehen ließ. Es gab einen völlig verrückten Typen, der mit einem Schwert, das er von zu Hause mitgebracht hatte, solange auf einen Computer einschlug, bis es in zwei Teile brach. Eß- und Trink-Wettbewerbe erfreuen sich auch immer wieder neuer Beliebtheit. Es ist ein verrückter Anblick, jemandem dabei zuzusehen, wie er eine 1,5-Literflasche Cola in nur zwanzig Sekunden leertrinkt.

Doch der wichtigste Wettbewerb einer Party ist und bleibt mit dem Computer verbunden und ist in drei Grundwettbewerbe gesplittet: Demo, Grafik und Musik. Hier kann jeder sein Können beweisen. Demos und Grafiken werden auf eine riesige Leinwand projiziert. Musik wird abgespielt und später von einem Jurorenteam oder von den Besuchern bewertet.

Den Gewinnern winken Geld- oder Hardwarepreise, die sich durchaus sehen lassen können. Sie schwanken zwischen umgerechnet einhundert und fünftausend Mark. Die Höchstsumme, die bei der Prämierung der besten Demo auf einer Veranstaltung je ausgesetzt war, belief sich auf sage und schreibe fünfzigtausend Mark. Doch dies ist nicht der größte Ansporn, an einem Wettbewerb teilzunehmen. Wie bei den olympischen Spielen gilt hier eher: 'Dabeisein ist alles.' Hinzu kommt noch, daß es schon ein angenehmes Gefühl ist, wenn die eigene Produktion von über tausend Leuten mit tosendem Applaus bejubelt wird. Die Mitarbeiter von Demos werden wie Stars umringt und regelrecht gefeiert. Eine bessere Motivation, um ein neues Projekt in Angriff zu nehmen, gibt es nicht.

Neben diesen drei Grundwettbewerben tauchen immer neue Wettbewerbe auf, die sich zu festen Bestandteilen einer Party entwickeln. Einer, der mittlerweile zum festen Programm jeder Party geworden ist, ist die 'Wild Competition', in der jeder das machen kann, was er will. Wenn jemandem danach ist, auf die Bühne zu steigen und laut zu singen, dann darf er das im Rahmen der Wild Competition tun. Es ist einfach alles erlaubt, was lustig, verrückt oder einfach nur 'wild' ist. Natürlich gibt es auch kreative Beiträge. Beliebt sind Kurzfilme und alles rund um das Medium Video.

Parties sind nicht nur ein wesentlicher Teil der legalen Demoszene, sie sind auch für viele illegale Softwarepiraten, die die Szene mittlerweile als Goldesel entdeckt haben, ein Ort, an dem sie neue Beziehungen knüpfen, um ihre Waren zu verkaufen. Dieser bittere Beigeschmack bleibt, doch er wird toleriert.

I am Chaos. I am the substance from which your artists and scientists build rythms. I am the spirit with which your children and Clowns laugh in happy anarchy. I am Chaos. I am alive, and tell you that you are free.

Eris, God-dess Of Chaos, Dis-cord & Con-fusion

In Kontakt mit der Szene

'Eine Bande von Chaoten'

Abgesehen von den größeren Parties gibt es in der Szene auch andere Orte, an denen man sich in kleinerem Rahmen begegnen kann. Früher wurden diese kleineren Versammlungen **Copyparties** genannt, da sich Szenemitglieder dort hauptsächlich trafen, um Raubkopien zu tauschen. Wie auch auf den heutigen Parties durfte auf Copyparties der eigene Computer nicht fehlen und viele brachten ihren Rechner und kistenweise elektronische Bauteile in vollbeladenen PKWs mit. Kopierparties, auf denen nur die Elite eingeladen war, fanden an geheimen Orten ohne Öffentlichkeit oder Außenstehende statt. Die Szene war damals noch völlig im Untergrund.

Heute ist sie nicht mehr dieselbe geschlossene Gesellschaft wie vormals. In den letzten zehn Jahren sind viele weitere Treffpunkte dazugekommen, die mittlerweile auch der Öffentlichkeit zugänglich sind. Die alljährliche Computermesse in Köln ist ein solcher Ort. Am Anfang war diese Messe, die jedes Jahr an einem Novemberwochenende stattfindet, noch ausschließlich als Messe für Amiga-Benutzer gedacht. Im Laufe der Jahre hat sie sich zu einer Besucher- und Fachmesse entwickelt, auf der alle möglichen Systeme und die Computerperipherie vertreten sind. Seit den Anfängen ist es Szenetradition, sich am zweiten Tag, dem Samstag, zu versammeln. Früher geschah das noch durch interne Bekanntgaben, mittlerweile hat sich dieses Treffen etabliert. Zur Computermesse Köln, die parallel zur Kunstmesse 'Art Cologne' läuft, reisen Hunderte von Szenemitgliedem aus ganz Europa an. Die Mitglieder legen für diesen besonderen Tag oft sehr weite Strecken zurück, nur um sich hier mit den Mitgliedern ihrer und anderer Gruppen zu treffen.

Die Messeveranstalter haben schon seit längerer Zeit mit der Szene zu kämpfen. Vor allem in den Anfangszeiten der Computermesse machte sie stets deutlich auf sich aufmerksam. Mit Sprühdosen und Eddings beschmierten Szenemitglieder die Wände der Messe und verewigten sich und ihre Gruppen in großen Graffitis. Bei der großen Zahl von Szenemitgliedern war es für die Sicherheitsleute der Messe unmöglich, ein Messeverbot zu erteilen, das von erkennbarer Wirkung gewesen wäre.

Die Messeveranstalter lernten aus ihren Fehlern und sahen ein, daß ein Ausschluß der Szene von der Veranstaltung keine Lösung sein konnte. Man mußte sich also etwas ausdenken, um diese 'Bande von Chaoten' in die Messe zu integrieren und dabei den Schaden so niedrig wie möglich zu halten. Daher wird mittlerweile von der Messeveranstaltung samstags eine Szenewand eingerichtet. Diese Wand wird mit weißem Papier bespannt, damit die Szene ihre Graffitis nicht direkt auf die Wände schmiert. Seltsamerweise ließ sich die Szene auf den Kompromiß ein, und seit diesem geglückten Versuch kann man nun so manchen abgedrehten Spruch an der Szenewand lesen. Oft findet man dort auch wertvolle Informationen. Adressen von Internetseiten und Systempaßwörter von Szenemailboxen, durch die man in direkten Kontakt mit der Szene treten kann, sind zum Beispiel keine Seltenheit.

Die Messeveranstalter geben den Sicherheitsbeauftragten jedes Jahr die ausdrückliche Order, den Szenemitgliedern freien Lauf zu lassen. Zudem werden neben den Sicherheitsleuten des Hauses noch weitere Kräfte angestellt, die, mit Lederjacken und Jeans bekleidet, möglichst unauffällig die Szene observieren sollen. Dieses Wachpersonal, das jährlich nur für diesen Zweck engagiert wird, hatte zunächst sicher keine leichte Aufgabe. Meist hatte die Sicherheitstruppe mit Randalierern und Computer-Anarchisten zu tun, die manchmal in Gruppen brüllend durch die Messehallen zogen und einen Computer nach dem anderen durch Viren unbrauchbar machten. Auch konnte man nicht selten beobachten, daß Szenemitglieder einfach wild in der Gegend herumpöbelten und Aussteller von renommierten Computerfirmen durch ihre ungehobelte Art bei der Arbeit störten. Mittlerweile hat sich die Security mit der Szene auf freundlicher Basis einigen können. Auf der Computermesse 1997 konnte man beobachten, wie die Security entlarvt, von der Szene umzingelt und mit Aufklebern von Szenegruppen beklebt wurde.

Bei der Computermesse Köln kann man tatsächlich von einem öffentlichen Szenetreffen sprechen, bei dem jeder einen Einblick bekommen kann. Die verächtlichen Blicke der meisten Messebesucher, die leicht irritiert an der Szenewand vorbeilaufen, kann man jedes Jahr aufs Neue sehen. Dennoch ist sie für einige Computerfirmen

nicht wegzudenken. Viele Softwarehersteller sind auf die Szene angewiesen. Hier findet man die besten Programmierer, Grafiker und Musiker im Computerbereich. Die besten Programmierer der Welt, insbesondere was Systemprogrammierung angeht, sind Szenemitglieder. Auf der 'Computer '97' konnte man beobachten, wie sich ein Aussteller der Firma Software 2000 - eine der renommiertesten Softwarefirmen Deutschlands - mitten unter die Szeneleute mischte und nach Programmierern fragte.

Auch die Firma Data Becken die ebenfalls auf der Computermesse ausstellt, profitierte einst von der Szene. So brachte Data Becker 1991 mit der weltweit agierenden Szenegruppe 'Red Sector' im Rahmen der 'Goldenen Serie' das Programm 'Demomaker' auf den Markt, das es Anwendern ermöglichte, Demos per Mausklick und ohne Programmiererfahrung zu erstellen. Diese und weitere Produktionen von Red Sector wurden bei Data Becker zu Verkaufsschlagern. Eine andere Szenegruppe faßte auf dem kommerziellen Markt sogar soweit Fuß, daß sie mit einigen Leuten eine eigene Softwarefirma gründete und heute unter dem Namen 'Factor 5' mit Spielen wie 'Turrican' weltweit bekannt ist.
Wer die Szene auf der Computermesse Köln einmal in Augenschein nehmen möchte, der kann dies an einem Samstag als gewöhnlicher Messebesucher tun.

Internet als Treffpunkt

Obwohl die Szene die persönliche Begegnung auf Parties jeder anderen Form der Kommunikation vorzieht, sind diese Meetings für viele Mitglieder mit großem Aufwand verbunden. Da sie oft über den ganzen Globus verteilt leben, bietet das Internet meist die beste Möglichkeit, sich wenigstens virtuell zu begegnen. Abgesehen von den Homepages hat die Szene ihre eigenen Online-Chatkanäle, in denen hunderte von Szenemitgliedern kommunizieren und Daten austauschen können. Ursprünglich waren diese IRC-Chatkanäle dazu gedacht, eine internationale Kommunikationsebene für Internetnutzer herzustellen. Es gibt die verschiedensten Chatkanäle, in denen sich Leute aus aller Welt über alle möglichen Themen unterhalten können. Die Szene nutzt diesen Service des Internets allerdings auch für ihre eigenen Zwecke.

Die Chatkanäle der Szene sind völlig unterschiedlich. Es gibt Chatkanäle sowohl für die legale als auch für die illegale Szene. Die Auswahl geht von Kanälen, in denen hauptsächlich die neuesten Raubkopien und Internet-Adressen mit Raubkopien ausgetauscht werden, bis hin zu Kanälen, in denen sich legale Demogruppen einfach nur unterhalten. In all diesen Chatkanälen werden Szenemitglieder respektiert und zuvorkommend behandelt.

Das Betreten eines Chatkanals erfolgt mit einem Pseudonym, das im Internet als 'Nick' bezeichnet wird. Sobald man in einen Chatkanal eingetreten ist, wird man automatisch auf das Thema des Chatkanals aufmerksam gemacht. In einen Chatkanal können sich mehrere Leute einklinken. Sobald jemand etwas schreibt, kann es jeder, der sich in dem Chatkanal befindet, in einem großen Fenster lesen. Das ganze ist vergleichbar mit einem Telefontreff. In einem Chatkanal jedoch kommuniziert man ausnahmslos schriftlich. Darüber hinaus gibt es zusätzliche Funktionen, die zum Beispiel den privaten Schriftverkehr zwischen zwei Personen sowie den gegenseitigen Austausch von binären Daten ermöglichen.

Die Pseudonyme der einzelnen Szenemitglieder ändern sich in der Regel nicht. Dadurch ist gewährleistet, daß man sich auch nach vielen Wochen noch wiedertreffen und erkennen kann. Daher sind die meisten Leute, die sich regelmäßig in diesen Chatkanälen aufhalten, bekannte 'Gesichter'. Heutzutage haben nur wenige Szenemitglieder keinen Internet-Zugang. So ist es eigentlich immer möglich, ein bestimmtes unter vielen Tausenden von Szenemitgliedern im Internet ausfindig zu machen.

Bei Nicht-Szenemitgliedem ist es nicht unüblich, daß ihnen in Chatkanälen der Szene arrogant begegnet wird. Betritt jemand diese Chatkanäle mit einem unbekannten Pseudonym, so wird er zunächst nicht beachtet. Stellt es sich mit der Zeit heraus, daß es sich um einen ahnungslosen Computeranwender handelt, wird er mit einem Rauswurf aus dem Chatkanal rechnen müssen. Ein Rauswurf hat zur Folge, daß der Anwender durch Sperre seiner Internet-Erkennung diesen bestimmten Chatkanal nicht mehr betreten kann - selbst dann nicht, wenn er sein Pseudonym wechselt. Diese Sperre wird solange aufrechterhalten, bis der Leiter des Chatkanals sie aufhebt. Solche Maßnahmen wird man in der illegalen Szene oft bei der sogenannten Elite antreffen, die sich auf Diskussionen erst gar nicht einläßt.

Durch diese meist wahllosen Rauswurf- und Verbannungsaktionen entstehen zwischen den Betreibern der unterschiedlichen Chatkanäle immer wieder Konflikte. Gerade aus den Kanälen der normalen User kommen dann heftige Anfeindungen gegen die Szene. Diese enden oft in kriegsähnlichen Auseinandersetzungen, die 'Channel-Wars' genannt werden.

Einige wenige Leute sind im Besitz eines bevorzugten Internetzugangs und haben Zugriff auf Befehle, die einen Chatkanal zerstören können. Auch die Szene hat solche Mitglieder, die meist in Rechenzentren arbeiten und ihre Arbeit unterstützen. Durch diese Leute kann eine Gegenattacke oft ganze Provider für einige Tage komplett vom Internet abschotten. Deshalb ist bei Channel-Wars gegen Szenekanäle immer mit dem Schlimmsten zu rechnen. Viele haben inzwischen dazugelernt und mischen sich nicht in die Chatkanäle der Szene ein. Man sollte nicht vergessen, daß in der Szene mit die besten Hacker zu finden sind, und diese möchten in ihren privaten Chatkanälen in Ruhe gelassen werden. Gesetzlich ist selten etwas zu machen, denn meist fehlen eindeutige Beweise,

um Anschuldigungen belegen zu können.

Das Internet hat sich nicht zuletzt deswegen für die Szene zu einem der beliebtesten Treffpunkte entwickelt und wird es auch sicher noch lange Zeit bleiben.

Interviews

Interview mit einem Phreaker: Lawnmower Man

von der Gruppe Birdhouse Projects

Lawnmower Man von der Gruppe 'Birdhouse Projects' gehört zu den Leuten in der Szene, die sich durch Tricks die Möglichkeit verschaffen, kostenfrei zu telefonieren. Er ist bereits seit langem Mitglied der Szene, dort auch als Phreaker bekannt und noch aktiv. Wir kennen Lawnmower Man noch aus der Zeit, in der Calling-Card-Nummern in der Szene zu Hunderten verkauft wurden. Wir trafen ihn auf einer Szeneveranstaltung und konnten ihn zu einem Interview überreden.

Autoren: Du bezeichnest dich selbst als Phreaker. Kannst du uns sagen,
worin die Aufgaben eines Phreakers bestehen?

Lawnmower Man: Möglichst viel Schaden am Telefon anzurichten und Wege zu finden, kostenfrei zu telefonieren.

Wem gibst du die Möglichkeit, kostenfrei zu telefonieren?

Natürlich der Szene, dem Freundeskreis oder der eigenen Gruppe. Das bedeutet aber weit mehr als nur telefonieren. Da steckt eine Menge dahinter, zum Beispiel Voicemailsysteme **(VMB).** Oder was gibt es noch? Konferenzen und ähnliches.

Im Grunde machst du das also nur für die Szene. Birdhouse Project ist doch eine legale Demogruppe. Du dagegen bist jedoch ein Phreaker, also illegal. Wie kommt es zu einer Verbindung zwischen einem Phreakerund der legalen Demoszene?

Ich gehe ganz in der Gruppe auf, aber eigentlich stelle ich nur meine Phreaker-Fähigkeiten zur Verfügung. Weil ich die Leute kenne und weil ich dabeisein wollte. Das ist einfach ein positiver Nebeneffekt, daß die Gruppe davon profitiert. Denn auch bei einer Demogruppe fallen überall Telefongebühren an.

Was war überhaupt deine Motivation, der Szene beizutreten?
Durch welche Beziehungen bist du reingekommen?

Reingekommen bin ich damals über die C64-Zeit mit **Mailswapping,** also Versendung von Disketten per Post. Und dann habe ich angefangen, auf andere Systeme zu wechseln. Von C64. auf Amiga und dann auf PC. Und wenn man mit einem Modem in einem Board drin ist, kann man weitere Kontakte knüpfen. Ist man einmal drin, geht's weiter. Eine Nummer nach der anderen. Irgendwie wurde das immer mehr.

Wir hörten von einem Fall, bei dem ein Szenemitglied an Calling-CardNummern von MCI gekommen ist, weil er ein Angestellter der Firma war.
Gab es noch weitere ähnliche Vorfälle?

Gab und gibt es durchaus. Allerdings, wo du jetzt MCI erwähnst, da gab es doch vor drei Jahren den sogenannten 'MCI-Bug'. Aus irgendeinem Grund waren dort tausende von Karten vorhanden. Die waren nicht dazu da, benutzt zu werden, sie waren fiktiv da. Wie man an die rangekommen ist, war reiner Zufall. Es gab in den Staaten eine Art Partyline. Aus Gag bin ich einfach zum elektronischen Operator gegangen und habe dort die Telefonnummer der Partyline plus Pin Eleven Nintynine angegeben. Und das hat funktioniert. Auf einmal warst du im MCI-Zentralcompy drin. Dann hat man mit dem Block im Mund ein bißchen rumgescannt, und da kam halt immer mehr bei rum. Mit diesen Nummern hat die halbe Szene rumgecallt, bis MCI dahintergekommen ist.

Das war also nur Zufall?

Genau, reiner Zufall, da waren keine bösen Absichten dahinter. Man kann natürlich auch gezielt suchen. Zum Beispiel, indem du dir ein kleines Scanprogramm schreibst, um Calling-Cards zu scannen. Aber das ist eigentlich nur Schnickschnack. Die meistens Geschichten laufen auf sogenanntem 'Social Engineering', das heißt, man ruft Leute an und erzählt denen irgendwas, um an deren Calling-Card-Nummer oder Social-Security-Nummer (Amerikanische Sozialversicherungsnummer) zu kommen. Mit der Social-Security-Nummer kann man beispielsweise gerade im Internet sehr viele Sachen bestellen und buchen.

Gab's einen Höhepunkt in der Geschichte der

Phreaker?

Als im Jahre 1995 die Bluebox in den Sack gegangen ist. Da hatte man die Möglichkeit, sich die Frequenzen in den Boards zu ziehen, um damit zu callen. Da haben dann 90% der Scener zum Schluß an irgendwelchen Boards rumgehangen, um an die Frequenzen zu kommen. Und in den USA sind Mailboxen mit zehn bis zwanzig **Nodez** wie Pilze aus den Boden geschossen. Das Ziel des Blueboxings war ja, kostenfreie Leitungen in die USA zu bekommen. Danach war's eigentlich ruhig. Die Boards in den USA sind in den Keller gegangen. Die haben ziemlich gelitten, und deswegen sind in den USA auch nur wenige gute Boards übriggeblieben, die Umsatz machen.

Interview mit Timelord von der Gruppe TRSI

Timelord ist ein Szenemitglied, das der Szene bereits in der Anfangszeit beigetreten ist. Er war jahrelang in der illegalen Sektion der legendären Gruppe TRSI tätig. Hin und wieder trifft man ihn auf Szeneveranstaltungen, wo er sich der alten Zeiten wegen blicken läßt. Wir hatten das Glück, ihn zufällig auf der Computermesse '97 in Köln zu treffen und nutzten dieses freudige Wiedersehen für ein Interview.

Autoren: Würdest du uns von den An-fängen der Szene erzählen?

Timelord: Das fing in den 80er Jahre an, als die Szene in dieser Form noch gar nicht existierte. Man traf sich in der Kölner Innenstadt, meistens in Geschäften, hat sich mit ein paar Leuten unterhalten, auch mit denjenigen, die dort arbeiteten. Dann hat man angefangen Software zu tauschen, weil die damals noch so wahnsinnig teuer war. Um die 100 Mark. Und so ist man da eben reingeklettert.

Wie lief der Tausch mit der Software ab? Ist es damals einfacher gewesen als heutzutage?

Am Anfang schon. Da konnte man in den Zeitschriften noch annoncieren: 'Suche Software' und ähnliches. Da gab es noch keinen Gravenreuth. Zum Teil hat man die Leute auch persönlich kennengelernt. Zu einigen habe ich auch jetzt, nach zwanzig Jahren, noch Kontakt.

Wie hat sich die Szene überhaupt entwickelt? Wie kam es dazu,
daß sich die Leute organisiert haben?

Die Softwarefirmen haben damals für Software viel zu hohe Preise verlangt. Und es gab nur ein paar Ausnahmen, wie Brotherbund, die dafür auch Qualität lieferten. Die meisten Firmen haben im Grunde Crap für sehr teures Geld verkauft. Und deshalb etablierte es sich, daß die Szene die Sachen crackte und weiterverteilte.

In welcher Beziehung hast du damals zur Szene gestanden? Hast du auch Software gecrackt?

Damals haben wir im kleinen gecrackt, es ging ja noch alles viel viel einfacher. Da hat man Speedos gehabt, hat dann ganz dezent auf den Tasten rumgehauen und die Einsprungadressen in 64er-Games gesucht. Nachher nutzten die Lamer Freezeframe und wie der ganze Kram hieß, damit konnte jedes Würstchen cracken. Aber die alte Garde hat da immer noch mit Esmon gearbeitet, den im Höchstfall vielleicht auf ein Modul gebrannt, Reset gedrückt und im Speicher rumgewühlt. Dann lief der Kram, und der wurde natürlich auch getauscht.

Wie war die Szene damals organisiert, wie hat man sich ab-gesprochen?

Absprache - das war zu der Zeit, wo die Modems noch Akustikkoppler hießen und 300 Baud hatten. Da ging's ganz normal über Telefon. Oder man hat eben feste Zeiten vereinbart. Also ich habe mich zum Beispiel mit ein paar Leuten immer samstags in der City getroffen. Dort haben wir die Sachen kopiert und getauscht.

Hattet ihr Leute, die in eurer Gruppe waren und gleichzeitig bei einer Softwarefirma arbeiteten?

Ja, selbstverständlich. Selbst heute in der Szene gibt es noch genügend Szenemitglieder, die in Softwarefirmen und in Softwarevertrieben arbeiten oder selbst Geschäfte haben und Programme cracken, um sie zu vertreiben.

Verschiedene Mitar-

beiter von Software-firmen cracken also selbst?

Ja, sicher.

In der Szene geht ein glaubhaftes Gerücht um, nachdem eine Softwarefirma mit der Szene zusammengearbeitet haben soll.

Es hat ein paar szeneinterne Sachen gegeben damals, auch Absprachen, daß Gelder gezahlt worden sind, damit eine bestimmte Gruppe ein Spiel nicht crackt.

Kannst du uns da einige konkrete Beispiele nennen?

Es gibt eine ehemalige Szenegruppe, die sich jetzt 'Factor 5' nennt. Ein paar von den Leute hießen damals in der Szene 'The Light Circle' und stammten aus Köln. Es gab Absprachen, Sachen erst nach einem bestimmten Termin zu cracken. Die haben es dann auch ungecrackt der Szene zur Verfügung gestellt, und so ist es dann trotzdem verbreitet worden.

Die Crackergruppe hat sich doch dadurch auch einen schlechten Namen gemacht, oder? Schließlich bemüht sich jede Crackergruppe um einen guten Namen. Versuchen dann nicht die anderen Gruppen in der Szene, diese Gruppe zu ruinieren?

Das hat es zu der Zeit, in der ich aktiv war, mehrfach gegeben, siehe TRSI und Alpha Flight - der ewige Krieg. Das ist klar. Aber die besten Cracker sind zu Gruppen gegangen, die auch dafür zahlten oder sonstwie Vergünstigungen anboten. Und die haben sich zum Teil dann eben übel bekriegt.

Wie laufen solche Kriege ab? Ist das nur Propaganda innerhalb der Szene oder geht das auch manchmal körperlich zur Sache?

Also, das ging damals los mit Hetzbriefen, bevor es die **File-Id-diz** gab, da wurde dann Textfiles geadded - mit Bekanntgabe von Namen und Adressen und sonstigem -, aber das waren Kinkerlitzchen. Was darüber hinaus noch alles passiert ist, dazu will ich lieber nichts genaueres sagen.

Kannst du von Konflikten mit der Polizei in der damaligen Zeit erzählen? Unangenehmes oder vielleicht sogar Lustiges?

Es gab da einen guten Freund von mir, Das ist eigentlich eine witzige Geschichte. Ich war bei ihm zu Besuch. Er war noch nicht zu Hause, weil er noch arbeiten war und Überstunden machte. Ich hab auf ihn gewartet, ich kannte auch seine Familie. Auf einmal kam sein Vater zu mir rein und zeigte mir ein Din-A4-Blatt und meinte: 'Sag mal was dazu.' Es handelte sich um einen Hausdurchsuchungsbefehl. Ein paar grüne Männlein rannten mit zwei Typen in Zivil ums Haus. Ein ganz normales Einfamilienhaus. Mein Freund, der gebustet wurde, war Phantom vom BAT und hatte sein eigenes abschließbares Zimmer im Keller. Die haben ein Brimborium gemacht, daß der Schlüssel besorgt werden sollte, um die Tür aufzumachen. In der Zwischenzeit bin ich kurz zum Nachbarn rübergegangen, da die Polizei sich nicht für mich interessierte. Von da aus habe ich Phantom angerufen, er war Co-Sysop. Der ging dann von außen ins Board rein. Er hat das Board formatiert soweit es ging. Bis die Polizei die Türe geöffnet hatte, war das Board unbrauchbar geworden. Das wußte die Polizei aber nicht. Die sind dann unten wie wild rumgelaufen bis einer der Polizisten eine 5 1/4-Zoll-Diskette auspackte und sie seinem Kollegen unter die Nase hielt und todernst meinte: 'Danach suchen wir.' Das war superwitzig, man bemerke, das war Anfang der 90er und da suchten die nach 5 1/4-Zoll-Disketten! Da aber zu dem Zeitpunkt 5 1/4-Zoll-Disketten noch billiger als 3 1/2er-Scheiben waren, hatte mein Kumpel trotzdem sehr viele davon. Die haben sie dann alle eingesammelt, das Board aber haben sie stehengelassen. Darüber hinaus lagen da noch sechshundert bis achthundert 3 1/2-Zoll- Disketten mit Warez im Schrank. Die haben sie auch nicht angerührt. Und oben im Zimmer, wo ich schon mal übernachtete, stand mein Super-Nintendo und ein paar hundert raubkopierte Spiele, die sie auch übersehen haben. Endeffekt war, Günni hat ihm eine Unterlassungsklage reingedrückt, und er mußte 4000 Mark bezahlen, damit war die Sache gegessen.

4000 Mark? Gerüchten zufolge müßte es sich doch um viel mehr handeln. Warum einigt man sich dann auf eine so geringe Summe?

In Deutschland muß bewiesen werden, was im Endeffekt raubkopiert worden ist. Und da in diesem Falle die Beweismittel eher mager waren, kamen halt 4000 Mark raus und eine Unterlassungsklage.

Wir haben von Deals zwischen Anwälten und Computerbenutzern gehört, kannst du uns auch davon erzählen?

Es gibt einige Sachen, die da gelaufen sind. Zum Beispiel Gravenreuth, der hat auch ein paar Deals gemacht, über die ich Bescheid weiß. Da haben Leute andere verpfiffen, damit sie nicht selbst vor Gericht kommen. Das ist mehrfach vorgekommen.

Interview mit Ekkehard Brüggemann (sTEELER)

Ekkehard Brüggemann stieg schon im Kindesalter in die Computerszene ein und agiert heute im legalen Bereich. Als Hauptorganisator der 'Mekka & Symposium Party' ist er in der Szene unter dem Namen 'sTEELER' bekannt. Die Mekka & Symposium Party findet jedes Jahr zu Ostern in einer großen Halle im niedersächsischen Fallingbostel statt. Im Laufe der Jahre gewann sie an Bedeutung und gehört heute mit über tausend Besuchern zu den beliebtesten Szeneveranstaltungen Europas.

Autoren: In welchen Gruppen bist du jetzt?

sTEELER: Phantasm und Hellfire.

Du scheinst immer gut drauf zu sein, woran liegt das?

(lacht) Naja, alle Scener sind irgendwie bescheuert!

Erzähle uns doch mal etwas über die alten Zeiten, wann hast du angefangen zu cracken?

Das hab ich zur selben Zeit mit Tapes auf dem C64 gemacht. Einen Tape-Header konnte ich schon auf dem C 64 erkennen. Ich hab für den C 64 damals ca. hundertfünfzig Spiele gecrackt.

Wie alt warst du damals?

Ich glaube fünfzehn. Das muß dann so um 1987 gewesen sein. Ich hatte noch richtig Zeit damals. Aber ich bin zum Glück nicht in soziale Armut geraten wie einige unserer Kollegen. Viele sind wohl ziemlich vereinsamt vor ihrem Rechner.

Wie bist du damals an den Commodore-64 gekommen?

Ich hab für meinen C64 damals noch 1500 Mark ausgegeben. Mein Konfirmations-Geld war futsch! Und nach einem Jahr habe ich schon angefangen zu cracken. Hatte aber schon in der Schule erste Kontakte mit Rechnern gehabt. Einen PET2001 von CBM. Das sind uralte Rechner aus den Anfängen. Dann habe ich damals bei Vobis meinen ersten richtigen Computer gesehen. Den wollte ich unbedingt haben. Damals kosteten Disketten noch 30 Mark die Packung.

Hast du mit Raubkopien Geld verdient?

Man verdiente sich sein Geld mit seiner eigenen Raubkopierer-PLK. Meine war damals PLK 933655C, 2100 Hamburg 90. Ich schrieb den Leuten, die kaufen wollten: 'Write to sTEELER for swapping!'

Ist die PLK heute noch gültig?

Ist schon lange off. Hab ich gecancelt, als die ersten abgefangen wurden. Heikle Geschichten damals! Bei meinen Kumpel Rascal von der Gruppe HF haben sie zu der Zeit die gesamte Wohnung auf den Kopf gestellt.

Wurden die anonymen PLKs von der

Post nicht ab-geschafft?

Genau, irgendwann ging das nicht mehr. Aber einmal ausgestellte wurden noch eingelöst. Später ging aber nur noch Postfach. Ohje, die alten Zeiten, es kommt alles wieder hoch! (lacht)

Wie kamst du zum Cracken?

Mein Kumpel Heino Snyder von der Red-Label-Mailbox hat mir Coden beigebracht. Er war der erste Scener, den ich kennenlernte. Dann war da noch Freddy von Secret-Castle, und die wurden richtig fett gehustet. Eines Tages klingelt es, die Mutter macht die Tür auf, und da steht ein Mann und sagt: 'Guten Tag, wir haben hier einen Hausdurchsuchungsbefehl für das Zimmer ihres Sohnes.' Die Frau ist zusammengebrochen. Was für ein Spaß, und Freddy war in der Schule! (lacht)

Wie alt war Freddy damals?

Freddy? So an die siebzehn denke ich.

Wie bist du in die Szene reingekom-men?

Ich wußte noch gar nicht, daß es die Szene gab, und da war ich irgendwie schon drin. Mein erstes Modem hatte ich 1988 am C64: 300 Baud. Damit bin ich immer in die TECS gegangen: eine reine Multiport-Chat-Mailbox. Das war geil! Richtig reingerutscht würde ich aber sagen, bin ich durch Freddy und Heino. Das waren die ersten Kontakte mit Szenemailboxen. Parallel dazu gab's noch eine Mailbox bei mir im Dorf: Maschen bei Hamburg. Der Betreiber war Gandalf, ein guter Kumpel von mir. Nun, ich stieg als Co-Sysop bei Gandalf ein. Die Mailbox lief damals noch auf einem alten Amiga 2000 mit 8o Megabyte Festplatte, was mehr als genug war. Gandalf kaufte sich eine 020er Turbokarte, und die ersten 9600-Baud-Courier-Modems gingen ans Netz. Wir stellten beide gleichzeitig fest, daß es in Hamburg ein paar Mailboxen gab, die nicht nur PD-Software anboten, sondern auch in einem harten Geben-Und-Nehmen-Schema ihre Software für uns lösten. Also war unsere Idee, das ein wenig in den Süden Hamburgs auszudehnen und unseren Bereich mit der Software abzudecken. Wir teilten unsere Mailbox in einen schwarzen und einen weißen Bereich auf. Der weiße Bereich war für jeden zugänglich, der schwarze nur für schwarze Schafe, die wir selber bestimmen konnten. Ein idealer Einstieg. Ein Besucher der Mailbox, der keine Ahnung hatte, bekam nichts zu sehen.

Wußtet ihr damals überhaupt, was die Szene war?

Schwer zu sagen. Ich wußte, daß es Gruppen gab, die Software crackten. Ich wußte aus C64-Tagen auch, daß diese Gruppen sich untereinander kennen. Aber aus meinem Bereich kannte ich eigentlich nur Leute, die mit der DFÜ-Szene (Datenfernübertragung) in Kontakt standen. Demos hatte ich auf dem C64 aber auch selber programmiert. Erst in Basic, dann in Assembler. Aber direkt 'Scene' dazu zu sagen, war mir fremd. Es gab keinen direkten Kontakt zu den Mitgliedern.

Wie kam es dazu, daß du Organisator von einer der größten privaten und legalen Szeneveranstaltungen, der 'Mekka & Symposium Party' geworden bist?

Es fing damit an, daß wir, nachdem die Mailbox mehr als hundert Mitglieder hatte, einige jährliche Treffen abhielten. Zu Anfang eigentlich nur für die lokalen Mitglieder der Mailbox. Dort lernte ich auch immer mehr Mitglieder aus der Szene kennen. Das Meeting nannten wir 'Black-Box-Symposium'. Black Box war Gandalfs Mailbox. Und je mehr Leute zu diesen Treffen kamen, desto mehr lernten wir kennen. Anfang 1993 nur an die zwanzig bis dreißig Leute; später, um 1994, kamen achtzig Leute aus der Szene, 1995 um die hundert Szenemitglieder. Heute sind es bereits über tausend Szenemitglieder.

Interview mit Uwe Fürstenberg, Pressesprecher der Firma Software 2000

Die Produktionsfirma Software 2000 gehört zu den größten Softwareherstellern in Deutschland. Sie ist bekannt für ihre Strategie- und Sportsimulationspiele. Jedes Jahr präsentiert sich Software 2000 auf der Computermesse in Köln in eindrucksvoller Weise. Wir hatten das Glück, den Pressesprecher Herrn Uwe Fürstenberg bei dieser Gelegenheit zu einem Interview überreden zu können.

Autoren: Wann wurde Software 2000 gegründet?

Fürstenberg: Software 2000 hatte 1997 sein zehnjähriges Jubiläum. Die Firma wurde im Jahre 1987 ursprünglich als Amiga-Unternehmen ins Leben gerufen und ist heute bekannt für Spiele für PC und Sony Playstation. Da gab es zunächst einige Highlight-Produkte, die sich noch heute als aktuell erweisen. Natürlich in modifizierter Form der 'Bundesliga Manager', dessen Erfolg jetzt schon in der 5. Auflage besteht. Aktuellster Titel ist der 'Bundesliga Manager 1998'. Insgesamt hat sich dieser Titel in den letzten Jahren als Vollversion in Stückzahlen von mehreren Hunderttausend verkauft.

Erzählen Sie uns doch bitte von den Erfahrungen, die Sie bislang mit Raubkopierern gemacht haben. Sind Raubkopierer eine Bedrohung für Softwarefirmen?

Raubkopierer sind keine wirkliche Bedrohung, ich würde sie eher als lästig bezeichnen. Diejenigen, die Raubkopien machen, haben Spaß daran, das Spiel zu cracken und zu verbreiten. Raubkopierer gehören von vorneherein nicht zu unseren Kunden, da sie mit einem anderen Interesse an das Produkt herantreten. Diese Leute wollen nicht mit der Software spielen, sondern sie cracken und verbreiten. Das ist deren persönlicher Spaß. Heute besitzt jedes unserer Spiele einen individuellen Kopierschutz, wodurch Gelegenheitskopien ausgeschaltet werden. Das Problem sind die Raubkopierer, die nach der Veröffentlichung eines Produktes die CD in größeren Stückzahlen duplizieren oder gleich im Duplikationswerk professionell herstellen lassen.

Dann sind Raubkopierer also keine Gefahr?

Die größte Gefahr entsteht, wenn ein Produkt, noch bevor es auf dem Markt erscheint, kostenlos im Internet oder für Billigstpreise zu haben ist. Dadurch geht Kaufkraft verloren, und diejenigen, die tatsächlich bereit wären, für ein Spiel den regulären Preis zu zahlen, fühlen sich übervorteilt. Letztlich sind wir aber der Meinung, daß der

Computerspieler sich bewußt ist, wie teuer Computerspiele in der Entwicklung sind. Daher sind viele ehrlich und investieren in ein Original-Produkt den regulären Preis, weil sie wissen, daß sie damit auch hochwertige Software bekommen.

Wie ist es möglich, daß Software als Raubkopie zu haben ist, bevor sie auf dem Markt erscheint?

Man muß natürlich ein Produkt, bevor man es auf dem Markt einführt, in Form von Beta-Versionen an unterschiedliche Stellen ausgeben, damit es getestet wird. So etwas ist wichtig, damit das Programm nach Fertigstellung fehlerfrei läuft. Dadurch kommen einige Versionen vorab in Umlauf. Wenn man nicht sorgfältig kontrolliert, wie viele genau verteilt worden sind, können Lücken entstehen.

Homepages

Internet-Adressenverzeichnis

Um auch Außenstehenden Einblick in die Welt der Szene bieten zu können, haben wir eine umfangreiche Liste mit Internet-Adressen zusammengestellt, die direkt in Verbindung zu der Szene stehen. Leser mit einem Internet-Zugang haben so die Möglichkeit, sich einen kleinen Eindruck von der Szene zu verschaffen. Da sie nicht nur auf IBM-Kompatiblen Rechnern aktiv ist, sondern auch auf anderen Plattformen agiert, trifft man unter anderem auch auf Programme und Links, die in Verbindung zu Computern wie Amiga, Acorn, Atari, Apple Macintosh, Silicon-Graphics und sogar dem legendären Commodore 64 stehen.

Wir bitten um Verständnis dafür, daß wir Adressen von Internetseiten, die unter anderem auch Raubkopien beinhalten, aus rechtlichen Gründen nicht veröffentlichen können. Dennoch glauben wir, daß Anwender, die auf der Suche nach Raubkopien sind, ohnehin nicht an den entsprechenden Links und Hinweisen vorbeikommen.

Homepages von Szenegruppen

Die größten und bekanntesten Szenegruppen der Welt nutzen Homepages zur Präsentation ihrer eigenen Produktionen innerhalb und außerhalb der Szene. Unter anderem sind hier auch Szenegruppen zu finden, die professionell und legal Musik, Grafik oder gar Softwareprodukte herstellen und vertreiben. Durch die Homepages kann man so ziemlich alles über eine bestimmte Gruppe in Erfahrung bringen. Man kann beispielsweise Mitgliederlisten einsehen, oder einfach nur die Entstehungsgeschichte einer Gruppe nachlesen.
Wir haben jeder Homepage einen Vermerk über das Herkunftsland beigefügt. Da die meisten Gruppen jedoch international vertreten sind, sagt dieser Vermerk nichts über das eigentliche Hauptquartier der Gruppe aus.

Abyss (Deutschland): http://home.ml.org/abyss
Accession (Finnland): http://www.megabaud.fi/~lennu

Agony (Schweden): http://www.rby.hk-r.se/~pt96bto/agony.html

Anadune (Polen): http://www.optimus.wroc.pl/anadune

Anthrox: http://www.anthrox.com

Balance (Schweden): http://hem.passagen.se/excelblc

Birdhouse Projects (Deutschland): http://birdhouseprojects.hypermart.net

Blackout (Kroatien): http://fly.cc.fer.hr/~ld/blt.html

Bonzai (Dänemark): http://chrom.imbg.ku.dk/bonzai.html

Broken (Österreich): http://www.iinet.net.au/~hweigt/index.html

C64 Demo Page (Dänemark): http://www.diku.dk/students/delirium/c64

C-Lous (Schweden): http://www.algonet.se/~egoben
Candle (Schweden): http://enterprise.shv.hb.se/~aeroba/candle.html
Centolos Fun House (Spanien): http://www.redestb.es/personal/marcos
Charlie Brown Records (Italien): http://www.cbr.avnet.it
Complex (Finnland): http://www.jyu.fi/complex/index.html
Corrosion (Italien): http://www.crsn.com

Cubic & Seen: http://www.cubic.org

Crux & Bad Karma (Schweiz): http://www.space.ch/scene/crux

Da Jormas (Finnland): http://www.jormas.com

Darkness (Argentinien): http://www.giga.com.ar/randy/darkness.htm

Demolution (Singapur): http://www.cyberway.com.sg/~nickybay/demo.htm

Damones (Finnland): http://www.damones.net

Depth (Norwegen): http://www.colargol.idb.hist.no/~madsjm/depth

Donut Fetish (Norwegen): http://home.sn.no/~iulsund

Doomsday (Finnland): http://www.lut.fi/~piiraine/doomsday

DPS-Crew (Schweden): http://www.ida.his.se/ida/~a94matpe/dps.html

Duel *Crew* Shining (Finnland): http://www.hut.fi/~mkolsi/dcs.html

Ethos 9 (USA): http://www.kaoz.org/ethos9

Factor (Schweden): http://hem2.passagen.se/boog/factor

Fairlight (USA/Schweden): http://www.fairlight.org oder http://www.ludd.luth.se/~watchman/fairlight

Flood (Dänemark): http://home3.inet.tele.dk/svg/flood/index.htm

Fudge (Dänemark): http://inet.uni-c.dk/~solon

Genetic (Holland): http://home.worldonline.nl/~onegnt

Gollum (Norwegen): http://www.nano.no/~espeng/gollum

Hall of Fames (Ungarn): http://www.agt.bme.hu/hof

Impact (Dänemark): http://home3.inet.tele.dk/nigel/impact

Impulse (Ungarn): http://members.tripod.com/~impulsed

Insane (Belgien): http://www.ping.be/~pin10450/index.html

Iris (Dänemark): http://home3.inet.tele.dk/barkholt/index.html

Kinetic PC (Finnland): http://www.hut.fi/~ksaarila/kinetic.html

Legend Design (Deutschland): http://www.homepages.de/t_molitor@dialup.nacamar.de

Lightforce (USA): http://www.geocities.com/tokyo/flats/2042

Lightstorm Inc. (Deutschland): http://www.snafu.de/~ray

Melon (Frankreich): http://imac.u-paris2.fr/~debelen

Mode 19 (Singapur): http://www.singnet.com.sg/~kaboon/mode19.html

Mono (GB): http://www.scene.org/mono

Nah-Kolor (Polen): http://www.nah.dom.pl

Nature (Schweden): http://move.to/nature

Nevermind (Jugoslawien): http://members.xoom.com/nvm

N.o.i.s.e (USA): http://www.noisemusic.org

Nuance (Deutschland): http://nuance.home.pages.de

Oops! (Holland): http://oops.in.nl

Paranoids (Finnland): http://www.modeemi.cs.tut.fi/~esap/paranoids/paranoids.html

Phantasm (Deutschland): http://www.iuk.tu-harburg.de/~frank/PHN/phn.html

Quartex (Argentinien): http://www.giga.com.ar/randy/qtxmain.htm

Rebels (Norwegen): http://www.uib.no/people/oodkr/Rebels

Ram Jam (Italien): http://www.algheronet.it/ramjam

Rage (Schweden): http://www.rage.nu/html/start.htm

Sapphire (Norwegen): http://home.sn.no/~escarlse/sapphire.html

Scoopex (Dänemark): http://amigascne.org/scoopex

Shining-8 (Deutschland): http://user.baden-online.de/~vrockenb

Silents DK (Dänemark): http://www.silents.dk

Spreadpoint (Deutschland): http://www.spreadpoint.com/museum.html

Supplex (Deutschland): http://www.supplex.com

Swiss Cracking Assocation (Schweiz): http://www.sca.ch

Talent (Norwegen): http://www.pvv.unit.no/~pallo/talent

Teklords (Deutschland): http://www.geocities.com/~teklords

The Experience Group (Australien): http://www.smug.adelaide.edu.au/~davew/TheExperience

The Sharks (Finnland): http://stekt.oulu.fi/~mysti/the_sharks

The Spooky Fellows (Italien): http://www.sgol.it/amiga/tsf.html

Tulou (Schweden): http://www.canit.se/~todi/tulou.html

TRSI (Deutschland): http://www.trsi.de

TRSI Recordz (Deutschland): http://recordz.trsi.de

Underground Empire (Deutschland): http://ue.home.pages.de

Ward (Schweden): http://home2.swipnet.se/~w-20762/index.html

Xography (Deutschland): http://rzstud1.rz.uni-karlsruhe.de/~uke4

Zero Defects (USA): http://zerodefects.babylonet.com

Homepages von Szenemagazinen (Diskmags)

Die meisten Diskmags, die Informationen über die Szene enthalten, sind auch über das Internet erreichbar. So bieten viele Szenegruppen, die sich speziell auf die redaktionelle Arbeit innerhalb der Szene konzentriert haben, ihre Magazine für Szenemitglieder online an. Hier findet man Berichte über Szenegruppen, Hacker, Cracker, Phreaker und andere szeneinterne Informationen. Aber auch für Nicht-Szenemitglieder sind derartige Homepages ein Insider-Tips Sie enthalten darüber hinaus auch kritische Berichte über Computermessen, Veranstaltungen, Wettbewerbe, sowie kompetente Anleitungen zu Programmierung, 3D-Grafik, Internet und allem, was kreative Arbeit mit dem Computer sonst noch ausmacht.

GFX Zone's Scene Stuff: http://www.hornet.org/info/gfxzone/scene.html

Generation: http://www.ssmedion.de/generation

Hardcore online: http://www.crsn.com/hc

House of Insanity: http://ww.ping.be/insanity

Imphobia Diskmag: http://www.infomaniak.ch/~imphobia

Jurassic Pack: http://home.sn.no/~terjjoha

Network: http://ww.scene-central.com

No Sense: http://www.one.se/nosense

Oepir Risti: http://www.one.se/oepir

Orange Juice: http://ojuice.citeweb.net

Pressure: http://dspace.dial.pipex.com/zone

Relax Online: http://home.sol.no/~zapotek

Restless Diskmag: http://opiate.home.ml.org/restless

R.A.W online: http://www.thies.net

R.O.M online: http://rom.home.ml.org

Scene News: http://www.neutralzone.org/scene-news

Scenet: http://www.scenet.home.pages.de

Showtime: http://www.algheronet.it/ramjam

The Demo Guide: http://generation.www.de/DemoHtml/main.htm

The Jungle: http://pcwww.uibk.ac.at/s06user/csaa1298/welcome.htm oder

http://pc23-c801.uibk.ac.at/~blitter/welcome.htm

Homepages von Szeneveranstaltungen

Die meisten Party-Homepages werden kurz vor Beginn einer Veranstaltung eröffnet. Daher kann es durchaus vorkommen, daß viele dieser Adressen zunächst nicht erreichbar sind. Auch wenn die Internet-Adressen für jedermann zugänglich sind, raten wir vor allem der Presse ab, ohne Genehmigung der Hauptorganisatoren auf einer solchen Party zu erscheinen. Parties wie die 'Mekka & Symposium' sehen sich als private Veranstaltung und möchten nur Szenemitglieder als Gäste. Eine vorherige und vor allem rechtzeitige Absprache mit den Organisatoren öffnet jedoch auch hier so manche Tür. Dagegen gewähren Parties wie 'The Party' in Dänemark (mit über viertausend Besuchern aus aller Welt eine der größten Europas) Außenstehenden gern einen eindrucksvollen Einblick in die Szene.

Abduction (Finnland): http://www.hut.fi/-maurala/abduction.html
Assembly (Finnland): http://www.assembly.org
Belgian Scene Event, BSE (Belgien): http://ucz.unicall.be/crisp
Bizarre (Holland): http://bizarre.concepts.nl
Bush Party (Norwegen): http://www.neutralzone.org/bp
Campus Party (Spanien): http://www.campus-partyorg
Cologne Conference (Deutschland): http://www.academicus.de/cc98
Compusphere (Schweden): http://compusphere.lindesign.se
Demobit (Slowakei): http://intemet.sk/demobit
Distance (Norwegen): http://www.neutralzone.org/distance
DreamHack (Schweden): http://www.dreamhack.org
Drome (Holland): http://www.drome.demon.nl
Euskal Party (Spanien): http://euskal.jet.es
Gravity (Polen): http://polbox.com/g/gravity
Icing (Schweden): http://www.icing.net
Jumper Party (Ungarn): http://d-eyes.jpte.hu/-jumper
LowRes (Holland): http://www.cryogen.com/lowres
Mekka E Symposium Party (Deutschland): http://ms.demo.org
Remedy (Schweden): http://www.remedy.dcs-graphics.se
Saturne Party (Frankreich): http://www.saturne.org oder http://abyss.moving-people.net/parties.html
Scene Strike 2 (Jugoslawien): http://www.crsn.com/ssz
Siliconvention (Deutschland): http://www.siliconvention.com
Takeover Party (Holland): http://www.takeover.nl
The Party (Dänemark): http://www.theparty.dk
The Gathering (Norwegen): http://www.gathering.org/tgg8 oder http://www.crusaders.no/tg
Wired (Belgien): http://nl.scene.org/wired98

Homepages von Hackern

Mittlerweile haben sich Tausende von Homepages von Hackern, Phreakern und Crackern im Internet etabliert. Auf diesen Internetseiten findet man Anleitungen zum Erhacken oder Zerstören verschiedenster Systeme, sowie die Möglichkeit, anonyme EMails zu versenden. Nicht selten demonstrieren solche Homepages aber auch dem Anwender, wie leicht sein Ausgangspunkt rekonstruierbar ist, indem sie ihm die komplette Route seiner Verbindung auf dem Bildschirm sichtbar machen. Die neuesten Erkenntnisse sowie kritische Berichte rund um das Thema Hacken, Phreaken und Cracken sind in folgenden Homepages zu finden:

2600 Hackers: http://www.26oo.com

8o's Hacker Textfiles: http://dsl.org/m/doc/arc/index.html

Anarchist Hacker Klan: http://www.angelfire.com/ar/ahk5

Anonymizer: http://www.anonymizer.com

Chaos Computer Club: http://www.ccc.de

Computer Hacking Forum: http://www.sotmesc.org/gcms/hackbb/wwwboard.html

Cosmos' Underground: http://www.eden.com/~cosmos/ug/underground.html

Crackstore: http://www.crackstore.com

Cyberheads Hack Page: http://ns.mtinter.net/~marcust/hack.html

Dark Secrets: http://www.dark-secrets.com

Elite Hacken (eH): http://www.elitehackers.com

Elite Social Club: http:J/www.sotmesc.org/gcms

German Software Revenge (GSR): http://come.to/GSR

Gnome Project: http://www.gnome.org/hacker.shtml

Hackers 101: http://www.hackers.com

Hackers Heaven: http://www.voicenet.com/~jackal

Hackers Suppy: http://www.hackers-supplycom

Hackerz Hideout: http://www.hackersclub.com

Hackerz Island: http://www.xs4all.nl/-lord

Hacker´s World: http://home.t-online.de/home/guys-underground-files

Happy Hacker: http://www.happyhacker.org

Happy Hopeless Hacker House: http://www.hhhh.org

Itaiamir: http://www.angelfire.com/il/itaiamir/index.html

Little Cyberia: http://start.at/lc

Mega Phreakers Homepage: http:llpages.prodigy.com/Hell/hackerz

New Hack City: http://www.newhackcity.net

Philadelphia Hackers: http://www.hackerz.org/-professr

Phreak 33: http://home.sprynet.com/sprynet/dukenuke/phreak33.htm

Phreaker: http://www.ameritech.net/users/jmartino/index.html

Secret Hacker Page: http://www.vmed.com.br/crack.htm

Swiss Cracking Assocation (SCA): http://www.sca.ch

The Darklord: http://people.a2ooo.nl/hliss/index.html

wAre'Zz sLuT'z1: http://www.warezslutz.com

Alle Szene-Begriffe sind bei der ersten Verwendung im Text markiert

acc: Abkürzung für 'Account' (zu deutsch: 'Zugang'). Damit ist meistens ein Zugriffscode gemeint, der mehrere Komponenten beinhaltet, wie zum Beispiel Usemame und Paßwort.
Addy: unter Systembetreibern von Szenemailboxen (» Board) verbreitete Abkürzung für 'Address' (zu deutsch: 'Adresse').
Akustikkoppler: Vorgänger des » Modems. Funktioniert auf die gleiche Weise, mit dem einen Unterschied, daß ein Telefonhörer auf das Gerät 'gekoppelt' werden muß.
Ami-Express: » /X
Ascii-Artist auch **Ascii-Master:** Bezeichnung für ein Szenemitglied, das grafische Bilder und Logos in Form von gewöhnlichen Buchstaben zusammenstellt. Diese Bilder sind stilistisch sehr eigen und haben einen graffitiähnlichen Charakter. Mittlerweile hat sich diese Kunst zu einem festen Bestandteil der Szene etabliert. Szenetexte und Signaturen, sowie die gesamte Oberfläche einer Szenemailbox (» Board)
tragen diese grafischen Verzierungen.
asm: Abkürzung für » Assembler.
Assembler: Computersprache.
axs: Abkürzung für 'Access' (zu deutsch: 'Zugriff). Ein häufig genutzter Begriff in Szenemailboxen. H Board
BB: Abkürzung für » Blue Boxing.
BBS: Abkürzung für 'Bulletin Board System'. » Mailbox
BBS-Advents: Abkürzung für 'Bulletin Board System Advertisements'. Mailbox-Werbung, die häufig an Infodateien der Szene angehängt wird.
Blue Boxing: Manipulation eines Telefonvermittlungscomputers durch Tonsignale, die es möglich macht kostenfrei zu telefonieren.
Board: Szenemailbox, die meist unter der Mailboxsoftware AmiExpress (» /X) oder » Fame betrieben wird.
Bug: (zu deutsch: 'Käfer'). Eine nicht nur in der Szene genutzte Bezeichnung für einen Fehler in einem Programm. » buggy
Bugfix: Programm, das helfen soll, Softwarefehler zu beheben. » Bug
buggy: Software, die fehlerhaft arbeitet. » Bug
Buster: Person, die für die polizeiliche Überführung einer Szenemailbox (» Board) verantwortlich ist oder daran mitgewirkt hat.
C64: Abkürzung für den legendären Computer 'Commodore 64', der bis heute noch eine treue Schar von Fans um sich versammelt. Elektronische Musikstücke, wie sie auf dem C64 komponiert wurden, werden noch heute auf anderen Plattformen komponiert und gehört.
CC: Abkürzung für 'Calling Card'. Um kostenfrei telefonieren zu können, wird in der Szene auch heute noch mit gestohlenen CallingCard-Nummern der Firmen AT&T, MCI und Sprint gehandelt. Vergleichbar mit der T-Card der deutschen Telekom.
CCC: Abkürzung für Chaos Computer Club.
cheat: zu deutsch 'mogeln'. Meist eine Tastenkombination, die Computerspielern erlaubt, im Programm versteckte Optionen zu aktivieren.
closed system: Szenemailboxen (» Board), die keine weiteren Mitglieder mehr akzeptieren.

Code: Quelltext eines Computerprogrammes.

Coder: Demoprogrammierer in der legalen Szene.
coding: Programmierung.
Colly: Abkürzung für Collection (zu deutsch 'Sammlung').

Conf oder **Confenence:** Konferenzräume in einer Szenemailbox (» Board), die in Themenbereiche unterteilt sind. Gewöhnliche Conferences sind: Amiga (Raubkopien rund um den Computer Amiga), PeeCee (Raubkopien rund um den IBM-kompatiblen Rechner), MAC (Raubkopien rund um den Apple Macintosh), PSX oder Console (Playstation Raubkopien oder Raubkopien anderer Spielekonsolen).
Console: Spielekonsolen wie Nintendo 64 oder Playstation. » PSX
Copyparty: Szenetreffen, bei dem es in erster Linie um den Austausch neuer Software geht.
Copystation: Zusatzhardware, die das Abspielen von raubkopierten Spielekonsole-CDs trotz Kopierschutz ermöglicht.
Cosy oder **CoOp:** Abkürzung für Co-Sysop oder Co-Operator. Helfer eines Systembetreibers.
Crack: Software, deren Kopierschutz entfernt wurde.
Cracker: Szenemitglied, das sich auf das Entfernen von Kopierschutzvorkehrungen in Softwareprogrammen spezialisiert hat.
Cracktro: vor einer Raubkopie eingebauter Vorspann (» Intro) einer Crackergruppe.
Cracktune: Musikstück für einen Crackervorspann. » Intro
Credit: Daten-Kontostand eines Mitglieds einer Szenemailbox. » Board
Credits: Namensliste der Beteiligten an einer Produktion in der legalen Szene.
crunch: besondere Art der Komprimierung (Packen) von Daten. Ein gecrunchtes Programm dekomprimiert sich beim Start von selbst (decrunch).
Demo: legale Produktion einer Szenegruppe, die unter anderem zur Präsentation des eigenen Könnens in Form von Animation, Bild und Musik dient.
Demotune: Musikstück für eine Demo.
Dentro: Verknüpfung der beiden Begriffe 'Demo' und 'Intro'. Eine Intro, die einer Demo ähnelt.
Dialer: Blue-Boxing-Jargon: Software, die Frequenzen erzeugt, die das Telefonnetz austricksen sollen. » line breaking
Diskmag: Abkürzung für 'Disk Magazine.' Elektronisches Nachrichtenmagazin der Szene, das früher hauptsächlich in Form von Disketten, heute als gewöhnliche Dateien im Internet und Szenemailboxen (» Board) zu finden sind. Diskmags sind legale Produktionen der Szene. Ihre Mitarbeiter nennen sich Editors und leisten nicht selten höchst kompetente Arbeit. Sie sind oft Mitglieder von offiziellen Presseverbänden, sind im Besitz entsprechender Presseausweise und genießen europaweit freien Eintritt zu Computermessen. Diskmags enthalten Informationen über Szenegruppen und Mitglieder weltweit. Themeninhalte sind auch Messeberichte und Veranstaltungen, die außerhalb der Szene stattfinden.
Division: » Section
dizzy: steht für 'disabled', ein Status, der einem Mitglied einer Szenemailbox (» Board) erlaubt, Software herunterzuladen, ohne eine Gegenleistung erbringen zu müssen (free download).
Doublemember: ein Szenemitglied, das in zwei Gruppen Mitglied ist.
Download: der Empfang von Daten (zu deutsch: 'Herunterladen'). In der Szene 'leech' (zu deutsch: 'saugen') genannt.
Dupe: ein bereits gecracktes Spiel, das von einer weiteren Crackergruppe ein zweites Mal gecrackt wird.
Editor: » Diskmag
EHQ: » HQ
Elite: Bezeichnung für Szenemitglieder, die extrem illegal tätig sind. In der legalen Szene meistens spöttisch verwendet.
Endlosschleife: » Start
Ende: » Start
Fake: (zu deutsch: 'Fälschung'), Bezeichnung für gecracktes Softwareprodukt, das nicht funktioniert.
Farne: » /X

fast: (zu deutsch: 'schnell'), 1. Bezeichnung für Szenemailboxen, die gecrackte Software anbieten, bevor sie auf dem Markt erschienen ist. 2. Bezeichnung für einen besonders aktiven Trader.
FIlE_ID.DIZ: Kurzbeschreibung zu einem Softwareprodukt in einem » Board.
Founder: Gründer einer Szenegruppe.
Function: Bezeichnung für den Aufgabenbereich eines Szenemitglieds.
Gold-Disk: 1. andere Bezeichnung für CD-Rohling. 2. Bezeichnung für eine gebrannte CD mit Raubkopien.
GvG: Abkürzung für den Münchener Rechtsanwalt Günter Freiherr von Gravenreuth.
Günni: » GvG
Hacker: Einwohner von Hackerland.
Handle: Bezeichnung für ein Pseudonym bzw. einen Usernamen.
Headquarter: » HQ
HQ: Abkürzung für 'Headquarter' (zu deutsch: 'Hauptquartier'). Bezeichnung für eine Szenemailbox (Board), die eine Sammelstelle für eine Szenegruppe darstellt. Je nach Größe der Szenemailbox (Board) kann es zusätzlich noch zum 'World Headquarter' (WHQ), 'European Headquarter' (EHQ) oder einfach nur zum Hauptquartier der eigenen Gruppe ernannt werden.
Infofile: Textfile der Szene, das szeneinterne Informationen enthält.
Intro: Abkürzung für Introduction, eine kurze Demo.
Introtune: Musikstück für eine Intro.
join: einer Szenegruppe beitreten.
Joshua: durch den Film 'War Games' in den 80er Jahren populär gewordenes Paßwort, das noch heute von Hackern verwendet wird.
kick: Bezeichung für den Rausschmiß einer Person aus einer Szenegruppe oder Szenemailbox (» Board).
l: p: Login-Name und Paßwort.
Lamer: 1. Bezeichnung für Nicht-Szenemitglieder. 2. Abfällige Bezeichnung für ein unbekanntes, ahnungsloses oder schlecht arbeitendes Szenemitglied.
lame: wird häufig als Äquivalent zu 'Schrott' oder 'Mist' benutzt.
Leader: Leiter und Chef einer meist illegalen Szenegruppe. In der legalen Szene mittlerweile von der nicht so hierarchisch wirkenden Bezeichnung 'Organizer' abgelöst.
leech: » Download
live breaking: (zu deutsch 'Brechen der Telefonleitung') Beim Blue Boxing: Erfolgreicher Signalaufbau durch einen Phreaker im Telefonnetz.
LMB: Abkürzung für 'left mouse button' (zu deutsch: 'linke Maustaste').
Mailbombing: absichtliche Übersendung riesiger Datenmengen, die zu Staus im Internet führen können. Oft enden Mailbombingaktionen mit der Sperrung des Internetaccounts der betroffenen Person.
Mailbox: System, das an das Telefonnetz angeschlossen und für jeden Anwender, der ein Modem besitzt, zugänglich ist. Mailboxen, die der Szene angehören, werden 'Boards' genannt.
Mailswapping: » Swapper
Major: ein gecracktes Spiel, das durch die illegale Szene veröffentlicht wird.
Messy oder **Msg:** Abkürzung für 'Message'.
Modem: Abkürzung für 'Modulation/Demulation'. Gerät, das Töne in Daten umwandelt, um sie durch eine gewöhnliche Telefonleitung senden und empfangen zu können.
Mod-File: elektronisches Musikformat, das nur vier Tonspuren belegt und aufgrund des niedrigen Speichervolumens meistens in Demos Verwendung findet.
Module: » Mod-File
Musicdisk: Softwareprodukt einer legalen Demogruppe, die Musikstücke von Szenekomponisten (Composer)

vorspielt.

Node: Bezeichnung für einen Telefonanschluß in einer Szenemailbox (» Board)

NON oder **NONPD:** Bezeichnung für raubkopierte Software (non public domain).

np: Abkürzung für 'no problem' (zu deutsch: 'kein Problem').

nuke: 1. Hintertür in einigen Internet-Programmen, die unter dem Betriebssystem 'Windows' laufen. Durch den Mißbrauch dieser Hintertür ist es möglich, den Internetnutzer aus dem System zu werfen. Dabei bemerkt er nicht, daß er 'genuked' wurde. 2. Board-Jargon: Das Downloadkonto (» Credit) eines Mitglieds in einem Board minimieren, weil alte Software upgeloadet wurde (» Upload).

NUP: Abkürzung für 'New User Password'. Das NUP ist ein festes Paßwort, das in Szenemailboxen (» Board), die man noch nie besucht hat, automatisch gefragt wird.

Organizer: » Leader

OP: » Sysop

PC-Express: eine Szenemailbox (Board), aufgebaut wie Ami-Express, jedoch speziell für Nicht-Multitasking-Betriebssysteme.

PeeCee: abfällige Bezeichnung für den handelsüblichen IBM-kompatiblen PC.

Phreaker: Verknüpfung der beiden Worte 'Phone' und 'Freak'. Illegales Szenemitglied, das sich auf kostenfreie Telekommunikation spezialisiert hat.

PM: Abkürzung für 'private message' (zu deutsch: 'private Nachricht').

Prog oder **Proggy:** Abkürzung für 'Programm'.

PSX: Abkürzung für 'Playstation'.

pw: Abkürzung für'Paßwort'.

Refs: Abkürzung für 'Referenzen'.

Release: Veröffentlichung eines » Cracks oder eines » Demo durch die Szene. Auch: 'Major'.

Rename: Softwareprodukt, dessen Datenname ('Filename') geändert wurde und damit durch die » tyader unbewußt erneut verbreitet wird.

Section: Aufgabenbereiche in der Szene sind in verschiedene Sections und Divisions aufgeteilt. Eine große Gruppe hat oft eine illegale und eine legale Section. Zusätzlich gibt es in einzelnen illegalen Sections weitere Aufgabenbereiche, die in verschiedene Divisions aufgeteilt sind (Amiga-Division, Console-Division, PC-Division, tyader-Division etc.). Diesen Divisions zugeteilt werden meist auch verschiedene Leader, die zusätzlich zum Gruppenkürzel noch entsprechende Titel tragen, wie beispielsweise Amiga-Division-Leader, Console-Leader etc.

Scener: Bezeichnung für ein Szenemitglied. Auch: ' Scene-Membei . **Scrolltext:** Text, der ähnlich wie ein Filmabspann von unten nach oben oder von links nach rechts wandert.

SCX: Kürzel der legendären Szenegruppe 'Scoopex'.

Slideshow: Softwareprodukt einer legalen Demogruppe, die Grafiken von Szenegrafikem zeigt.

Social Engineering: Phreakersprache. Methode, um an Calling-CardNummern zu kommen. Ein Phreaker ruft bei einem Calling-CardBesitzer an, gibt sich zum Beispiel als Mitarbeiter einer Telefongesellschaft aus und läßt sich durch trickreiche Argumentation die Calling-Card-Nummer durchgeben.

spread: verbreiten

Start: »Ende

Stampfaking: Präparieren von Briefmarken: Briefmarken werden mit einer bestimmten Substanz behandelt (meistens Haarspray), so daß der Empfänger den Stempel wieder abkratzen kann. »Swapper benutzten früher diese Methode, um beim weltweiten Tausch von Raubkopien über den Postweg Portokosten zu sparen.

Stuff: (zu deutsch: 'Stoff) Bezeichnung für raubkopierte Software. Ursprünglich aus der Drogenszene, wurde der Begriff Ende der 8oer Jahre in die Szenesprache übernommen. »WaReZ

Supplier: eine Kontaktperson, die neueste Software an eine Crackergruppe weitergibt.

Swapper: (zu deutsch: 'Tauscher') Auch 'Mailswapper genannt. Szenemitglied, das Software ausschließlich über den Postweg tauscht.

Sysop: Abk. für 'System Operator'. In der Szene mit 'OP' abgekürzt.

SYSPW oder **SPW:** Abkürzung für 'system password'.

Szenemailbox: »Board

THX: Abkürzung für 'Thanks' (zu deutsch: 'Danke').

trace: Zurückverfolgung eines Telefonpiraten durch die Polizei mit Hilfe der Telefonzentrale.

trade: tauschen

Trader: illegales Szenemitglied, das sich auf das Tauschen und Verkaufen von Raubkopien spezialisiert hat.

Trainer: von Crackern in Computerspiele eingebautes Unterprogramm, das verhindern soll, daß der Spieler verliert. Üblich sind Einstellungen wie unendliche Lebensanzahl, Energie und Munition oder die freie Wahl des Levels.

trojanisches Pferd: Softwareprogramm, das sich im System versteckt hält und Daten, wie zum Beispiel Paßwörter speichert und an den Hacker weitergibt.

TRSI: legendäre und mächtigste Gruppe der Szene. 1985 von kanadischen Szeneanhängern gegründet, trug sie ursprünglich den Namen 'Red Sector'. Später kam sie in Kontakt mit einer deutschen Gruppe und dehnte sich auch nach Europa aus. Den absoluten Durchbruch in der Szene hatte die Gruppe mit der Entwicklung einer einzigartigen »Demo namens 'Red Sector's Megademo'. Später kamen Programme wie 'Demomaker' und 'Multimedia Maker' auf den Markt, die von der Firma Data Becker vertrieben wurden. Red Sector fusionierte dann mit einer illegalen Szenegruppe namens 'Tristar' und ist seitdem unter dem Namen "Tristar and Red Sector Incorporated' (TRSI) in der Szene bekannt. Diese Vereinigung ist die bis heute am längsten währende Fusion in der Geschichte der Szene. TRSI hat mittlerweile Führungskäfte, Mitglieder, Quartiere, Computerläden, sowie Firmen und Musikfirmen wie 'TRSI Recordz', in allen Bereichen in Sachen Computer, in Europa, USA und Japan. Der Hauptsitz von TRSI ist Wien. Zu erreichen ist TRSI in Deutschland unter der InternetAdresse: **http://www.TRSI.de**

Tune: Musikstück.

Upload: Senden elektronischer Daten.

VMB: Abkürzung für 'Voicemailbox'. Akustische Mailbox, die mit den Tasten eines Telefons bedient werden kann.

WaReZ: Bezeichnung für Raubkopien.

WHQ: » HQ

ZyX: Abkürzung für 'ZyXEL'. Das in der Szene, aus Gründen der Stabilität am weitesten verbreiteste Modem des Fabrikats ZyXEL.

/X: die beiden Zeichen '/' und 'X' stehen für das Wort 'Ami-Express'. Zusammen bilden Sie ein Zeichen, das ein 'A' und ein 'X' darstellen soll. Ami-Express ist wie auch das Programm 'Fame' ein gängiges Mailboxprogramm, das aufgrund seiner schwierigen und komplexen Benutzeroberfläche nur von der Szene genutzt wird. Ami-ExpressSysteme werden von der Szene » Boards genannt.

0-Day-Warez: gecrackte Software, die 'noch keinen Tag alt ist', d.h. sie wird noch am selben Tag, an dem sie gecrackt wurde, verbreitet. » WaReZ

40K-Intro: eine kleine Demonstration (» Demo), die 4o Kilobyte an Datengröße nicht überschreiten darf. In der legalen Szene eine Herausforderung für den Programmierer (» Coder).

4CH-Musician: ein Szenemusiker, der Musik auf einem Programm erzeugt, das nur vier Soundkanäle (Channels) zuläßt.

Was immer auch geschehen wird, eines kann ich sicher
prophezeien: Die Szene ist nicht mehr aufzuhalten.
Oguzhan Özcelik – Micronik Computer

Nachwort

Seit vielen Jahren sind wir jetzt in die Szene verwickelt. Wir haben ihre Höhen und Tiefen erlebt, folgten blind jeder Einladung auf Parties rund um den Globus und mußten uns häufig dieselbe Frage stellen: Was machen wir hier eigentlich?

Wahrscheinlich hingen wir mehr vor unseren Computern, als uns heute klar ist. Während andere normalen Hobbies nachgingen, verbrachten wir unsere gesamte Freizeit in der Szene. Das Resultat ist nicht etwa elektronisch, sondern ein Buch, das die Szene an die Öffentlichkeit bringt. Noch können wir nicht abschätzen, wie diese Veröffentlichung aufgenommen wird. Sicherlich sind wir auf die Meinung der Leser und Kritiker gespannt. Am meisten erwarten wir jedoch die Reaktion der Szene, an der wir dieses Buch nicht vorbeischmuggeln können.

Es gibt Mitglieder der Szene, denen dieses Buch schon im Vorfeld ein Dorn im Auge war. Wahrscheinlich sehen viele darin eine Verletzung des Szenegeistes und einen weiteren Schritt zu deren Kommerzialisierung. Es ist nicht abzusehen, ob der mittlerweile unaufhaltsam gewordene Prozeß der Öffnung ihr schaden oder aber nutzen wird.

Vielleicht haben Dinge wie Freundschaft und Solidarität unter dem ständig größer werdenden Einfluß des Geldes mittlerweile einen geringeren Stellenwert als damals. Dennoch ist eine positive Tendenz nicht zu leugnen: Für immer mehr Mitglieder bietet die Szene ein Sprungbrett in die multimediale Berufswelt und dadurch eine realistische Zukunftsperspektive.

Wie die Zukunft der Szene aussehen wird, ist ungewiß. Sie wird sich aber auch weiterhin an den Fortschritt der Computertechnologie anpassen, um immer auf dem neusten Stand zu sein. Es ist wahrscheinlich, daß die Szene ein wenig lauter werden wird, zumindest so laut, daß man von ihr hören wird.

Ihr illegaler Teil ist auf dem Höhepunkt einer Entwicklung angelangt, an dem mehr Geld als je zuvor in die Taschen der Mitglieder fließt. Durch die CD-ROM als Datenträger floriert das Geschäft mit raubkopierter Software erneut, und die stetig wachsende Zahl der Computerbenutzer kann der illegalen Szene nur neuen Antrieb geben. Die Aufhebung des Monopols der Deutschen Telekom wird einigen Phreakern neue Wege des kostenfreien Telefonierens eröffnen. Ideen dazu findet man schon auf den entsprechenden Seiten im Internet.
Leader und Szenegrößen illegaler Gruppen, die schon in der zweiten Dekade dabei sind, leben wie die Maden im Speck. Eine Gruppe, die sich über einen solch großen Zeitraum halten konnte, hat einen gewissen Ruf in der Szene und nutzt ihn zum Anwerben junger Mitglieder. Zwar sind nur selten neue Mitglieder erforderlich, doch junge Leute werden in eine illegale Elite-Gruppe gern aufgenommen. Sie bilden die zukünftige Generation.

Einige Szenemitglieder illegaler Vereinigungen arbeiten immer noch zum Spaß. Diese Leute scheinen aber einer aussterbenden Spezies anzugehören. Neben das Geld tritt Macht als Hauptmotivation. Die illegale Szene kontrolliert Firmen unterschiedlichster Art, hat ihre Finger in gewinnbringenden Geschäften der Softwareindustrie und expandiert von Tag zu Tag. Es ist nur eine Frage der Zeit, bis die illegale Szene entdeckt, daß auch außerhalb der Computerwelt noch Geld zu holen ist.

THX

Bevor wir die Idee hatten, ein Buch über die Szene zu schreiben, hatten wir nicht mit dem Aufwand gerechnet, der auf uns zukommen würde. Erst mit der Zeit wurde uns klar, wie schwierig es ist, eine Recherche im Datenjungle durchzuführen. Ohne die Hilfe von Freunden und freien Mitarbeitern wäre eine ausführliche Dokumentation über eine Organisation wie die Szene sicherlich nicht möglich gewesen.
Kurz vor der Fertigstellung des Manuskripts besuchten wir die 'Mekka & Symposium Party '98' in Fallingbostel. Zu dieser Zeit hatte es sich in der Szene schon herumgesprochen, daß wir an einem Buch über diese Organisation arbeiteten. Viele Partygäste kamen völlig offen auf uns zu und stellten Fragen über das Buch und unsere Arbeit. Während wir uns bemühten, auf alle Fragen einzugehen, behielten wir ständig den mit dem WDR vereinbarten Termin vor Augen. Ein Kamerateam wollte einen Bericht über uns machen, in dem unsere Arbeit an dem Buch dokumentiert werden sollte. Dieser Bericht machte uns zunächst große Sorgen, weil wir nicht wußten, wie die Partygäste darauf reagieren würden. Für die kompetente Berichterstattung des WDR möchten wir uns bei Mehmet Coban und seinen Mitarbeitern bedanken. Auch sind wir Ekkehard Brüggemann (sTEELER), dem Hauptveranstalter der Mekka & Symposium Party, zu großem Dank verpflichtet. Ohne sein Einverständnis hätte der WDR-Bericht in dieser Form nicht realisiert werden können.
Für den großartigen Zusammenhalt auf der Party bedanken wir uns außerdem noch bei unserer eigenen Szenegruppe 'Nuance' und unserem Hauptorganisator Harald Wittmaack (Raven), der uns eine große Hilfe war.
Ebenfalls möchten wir uns bei den Rechtsanwälten Knops & Barthelmeß in Köln (http://www.knuba.de) bedanken, die uns
in allen rechtlichen Fragen zur Seite standen.

Von besonderer Bedeutung für dieses Buch war auch die Arbeit der Kölner Journalistin Lydia Keck, die die vorläufige Fassung des Manuskripts korrigierte und unserer Arbeit zahlreiche Denkanstöße gab. Dank gebührt auch Elke Ludwig, die uns mit vielen kompetenten Antworten zur Seite stand und uns vor allem mit ihrer positiven Einstellung motivierte.

Für die kostenlose Bereitstellung eines einzigartigen Internet-Providers bedanken wir uns ganz herzlich bei Hans Thomas Teuschow (Postmaster~teucom.xnc.com), dem System-Operator des 'Teucom's Terminal' in Köln. Ohne ihn wäre eine weltweite Recherche sowie der internationale Datenaustausch mit anderen Szenemitgliedern kaum möglich gewesen.

Außerdem bedanken wir uns noch bei allen, die beim Zustandekommen der Interviews geholfen haben: Lawnmower Man von der Szenegruppe Birdhouse Projects, Timelord von der Szenegruppe TRSI, Ekkehard Brüggemann von der Gruppe Phantasm und bei Herrn Uwe Fürstenberg, dem Pressesprecher der Firma Software 2000.

Es ist jahrelange Szenetradition, daß nach jeder Produktion stets Gruppen gegrüßt werden, mit denen man in freundschaftlichem Kontakt steht. Wir grüßen daher folgende Gruppen: Abyss, Balance, Birdhouse Projects, Clique, CNCD, Crux Design, Cryptoburners, Da Jormas, Damones, Depth, Darkage, Duel-Crew-Shining, Elke, Elven-z r, Eremation, Essence, Fairlight, Faith, Giants, Gods, Haujobb, Illusion, Iris, Kefrens, Lego, Looker-House, Matrix, Mono, Nah-Kolor, NerveAxis, Network, Nuance, Ozone, Omen, Phantasm, Phuture 303, Polka Brothers, Rebell, Riot, Shining-8, Smash Designs, Scoopex, Spaceballs, Silents, Talent, Teklords, The Black Lotus, TRSI, TRSI Recordz und Virtual Dreams.