Angriff auf Netze und Systeme

Hackerkultur zwischen gesellschaftlicher
Anerkennung und Kriminalisierung

Dissertation
zur Erlangung der Würde
eines Doktors der Rechtswissenschaft
der Fakultät für Rechtswissenschaft
der Universität Hamburg

vorgelegt von
DARIUS KEMPA
Hamburg 2006

Erstgutachter: Prof. Dr. Sebastian Scheerer
Zweitgutachter: Prof. Dr. Rainer Keller
Tag der mündlichen Prüfung: 28 Juni 2006

Meinen Eltern

und

meinem Bruder

Vorwort

Die folgende Abhandlung ist meine im Juni 2006 abgeschlossene Dissertation, die von der Juristischen Fakultät der Universität Hamburg angenommen wurde.

Für die unkomplizierte und freundliche Betreuung, sein Vertrauen sowie die vielen fruchtbaren Hinweise möchte ich meinem Doktorvater, Herrn Prof. Dr. Sebastian Scheerer, ganz herzlich danken. Mein Dank gilt auch Herrn Prof. Dr. Rainer Keller für die Erstellung des Zweitgutachtens. Bedanken möchte ich mich ferner bei allen, insbesondere bei Hergen Hillen, Marina Schmidt, Ulrike Klugmann, Matthias Domsch, Peter Baumstark, Dr. med. dent. Thomas Jüde sowie allen anderen, die mir während der Erstellung dieser Dissertation stets mit Rat und Tat zur Seite standen.

Besonderen Dank schulde ich nicht zuletzt meinen lieben Eltern, die nicht nur weit über das übliche Maß hinaus durch ihre Unterstützung meine lange Ausbildung gefördert haben, sondern mir mit ihrer Zuwendung und ihrer Liebe das für diese Arbeit erforderliche ideelle Rüstzeug mitgegeben haben.

Hamburg, August 2006

Darius Kempa

Inhaltsverzeichnis

1. Einleitung 1

1.1 Einführung 1
1.2 Fragestellung 5
1.3 Aufbau und Vorgehensweise 6
1.4 Empirische Erhebungen zu Computerdelikten 9
1.4.1 Die Polizeiliche Kriminalstatistik 9
1.4.2 Computer Emergency Response Team (CERT) 13
1.4.3 CSI/FBI-Untersuchungen 15
1.5 Aktueller Bezug 18
1.5.1 Der Sasser-Wurm 18
1.5.2 Der Pentagon-Hack 20

2. Computerkriminalität 22

2.1 Der Begriff Computerkriminalität 23
2.1.1 OECD-Definition 24
2.1.2 Werkzeug oder Ziel der Tat 24
2.1.3 Vermögensverletzungen 25
2.1.4 Netzkriminalität 25
2.1.5 Multimedia-Kriminalität 26
2.1.6 Eigene Definition und Typologie 27
2.2 Entstehungsgeschichte des Computers und des Internets 28
2.3 Computerkriminalität im weiteren Sinn 45
2.3.1 Spam 45
2.3.1.1 Definition und Formen 45
2.3.1.2 Verbreitungsarten 46
2.3.1.2.1 Adresshandel 47
2.3.1.2.2 Scannen 47
2.3.1.2.3 Brute Force 47
2.3.1.2.4 SMTP-Harvesting 48
2.3.1.3 Schäden 48

2.3.1.4 Verbote ... 49
2.3.2 Betrugsformen ... 50
2.3.2.1 Allgemein ... 50
2.3.2.2 Spezielle Formen ... 51
2.3.2.2.1 Kreditkartenmissbrauch ... 51
2.3.2.2.2 Onlineauktionen ... 52
2.3.2.2.3 Onlinebanking ... 53
2.3.2.2.4 Dialer ... 54
2.3.2.2.5 Sonstige Delikte ... 55
2.3.3 Piraterie oder Urheberrechtsverletzungen ... 56
2.3.3.1 Überblick ... 57
2.3.3.2 Tauschbörsen-Modelle ... 59
2.3.3.2.1 Zentrale Datenbank-Modelle ... 60
2.3.3.2.2 Servants-Modelle ... 61
2.3.3.2.3 Fasttrack-Modelle ... 61
2.3.3.3 Urheberrecht und Software ... 62
2.3.3.3.1 Software-Arten ... 63
2.3.3.3.1.1 Kommerzielle Software ... 63
2.3.3.3.1.2 Open-Source Software ... 63
2.3.3.3.1.3 Freeware ... 64
2.3.3.3.1.4 Public Domain Software ... 64
2.3.3.3.1.5 Shareware ... 65
2.3.3.3.2 Arten der Software-Piraterie ... 65
2.3.3.3.2.1 Lizenzmissbrauch ... 65
2.3.3.3.2.2 Produktmanipulation ... 66
2.3.3.3.2.3 Compilation-CD ... 67
2.3.3.3.2.4 Hard Disk Loading ... 67
2.3.3.3.2.5 Internet-Piraterie ... 67
2.3.3.3.3 Urheberrecht und WWW ... 68
2.3.3.3.3.1 Texte, Bilder und Layouts ... 68
2.3.3.3.3.2 Programmcodes und HTML ... 69
2.3.3.3.3.3 Deep-Linking ... 70
2.3.4 Zeitdiebstahl ... 70
2.3.5 Harte Pornografie ... 71

2.3.5.1 Newsgroups 72
2.3.5.2 Chat-Rooms und IRC 72
2.3.5.3 E-Mail 74
2.3.6 Extremistische Propaganda 74
2.3.7 Cyberterror 75
2.3.8 Sonstige Delikte 75
2.4 Computerkriminalität im engeren Sinn 76
2.4.1 Manipulations- und Sabotagehandlungen 76
2.4.1.1 Viren und Würmer 76
2.4.1.1.1 Historische Entwicklung 78
2.4.1.1.2 Strategie und Aufbau eines Virus 86
2.4.1.1.3 Virenarten 88
2.4.1.1.3.1 Boot-, Datei- und Makroviren 89
2.4.1.1.3.2 Mischformen und Untergruppen 91
2.4.1.1.4 Strategie und Aufbau eines Wurms 96
2.4.1.1.5 Schäden durch Computerviren/-würmer und ihre Entstehungsgründe 98
2.4.1.1.5.1 Schäden durch Computerviren/-würmer 98
2.4.1.1.5.2 Computerviren/-würmerentstehung 99
2.4.1.2 DoS- oder DDoS-Attacken 100
2.4.1.2.1 Definition 100
2.4.1.2.2 DoS-/DDoS-Arten 103
2.4.1.2.2.1 Mail Bombing 103
2.4.1.2.2.2 Broadcast Storms 104
2.4.1.2.2.3 Smurf/Fraggle 105
2.4.1.2.2.4 TCP Syn Flooding (Land Attacks) 106
2.4.1.2.2.5 Ping Flooding 107
2.4.1.2.2.6 Ping-AT-Attacks 107
2.4.1.2.2.7 Large Packet-Attacken (Ping of Death)/ IP-Fragment-Angriff (Teardrop) 108
2.4.1.2.3 DDoS-Tools 108
2.4.1.3 Weitere Sabotageakte 109
2.4.1.3.1 Guestbookbombing 109
2.4.1.3.2 Crackz 109

2.4.2 Spionagehandlungen 110
2.4.2.1 Trojaner 110
2.4.2.1.1 Logische Bomben 112
2.4.2.1.2 ANSI- und Makrobomben 113
2.4.2.1.3 Dropper 114
2.4.2.1.4 Keylogger und Sniffer 114
2.4.2.1.5 RAT-Trojaner oder Backdoors 116
2.4.2.1.6 Netzwerktrojaner 116
2.4.2.2 Kleine Trojaner 117
2.4.2.2.1 Cookies 117
2.4.2.2.2 Spyware 118
2.4.2.2.3 Clear-Gifs 118
2.4.2.2.4 Banner-Ads 119
2.4.2.3 Eingriffe in die Datenübertragung 120
2.4.2.3.1 Falsche Adressangaben und gefälschte E-Mail ... 120
2.4.2.3.2 DNS- oder Server-Spoofing 121
2.4.2.3.3 IP-Spoofing 122
2.4.2.3.4 ARP-Spoofing 122
2.4.2.3.5 (Browser-) Highjacking 123

2.5 Zwischenfazit 123

3. Computerszenen 126

3.1 Einleitung 126
3.2 Die Verwendung des Begriffs Szene 127
3.3 Cyberpunk-Szene 128
3.4 LAN-Szene 129
3.5 MUD-Szene 130
3.6 Programmierer-Szene 131
3.7 Hacker-Szene: Selbst- und Fremdbilder 132
3.7.1 Ursprünglicher Sinn und Jargon File 132
3.7.2 Netzwerkhacker 134
3.7.3 Die Cracker 136

3.8 Forschungsergebnisse zu Motivationslagen 139
3.8.1 Politisch motivierte Hacker 139
3.8.2 Aufklärerische und kritisch-kreative Computernutzung 145
3.8.3 Macht und Kontrolle 152
3.8.4 Spieltrieb und Probehandeln 158
3.8.5 Anerkennung der Gruppe 163
3.8.6 Wirtschaftliche Gründe 169
3.8.7 Schadensabsicht und Rache 172
3.8.8 Sucht 175
3.9 Aktuelle empirische Studien 178
3.9.1 „Where have all the Hackers gone?“ von Tom Mulhall 178
3.9.2 „Hacker Survey“ der Boston Consulting Group 181
3.9.3 „Account Missbrauch im Internet“ des Bundeskriminalamts 187
3.9.4 RSA-Studie: „Understanding a hacker’s mind“ 195
3.9.5 „Virtual Criminology Report“ von McAfee 202

3.10 Zwischenfazit 206

4. Die Entstehung der Hackerkriminalität nach der Self-Control Theorie von Gottfredson und Hirschi 209

4.1 Die Self-Control Theory in ihren wesentlichen Elementen 209
4.1.1 Social Bond Theory von Travis Hirschi 210
4.1.2 Self-Control Theory 211
4.1.3 Gemeinsamkeiten und Unterschiede der Self-Control Theory und der Social Bond Theory 222
4.2 Ein Erklärungsversuch anhand der Self-Control Theory 224

5. Zusammenfassung und Ausblick 252

Literaturverzeichnis 258

1. Einleitung

1.1 Einführung

Die fortschreitende Entwicklung der Computertechnologie stellt Polizei, Justiz und Gesetzgeber vor erhebliche Schwierigkeiten. Der damit zusammenhängende Bereich der Computerkriminalität stellt einen komplexen und sich schnell wandelnden Bereich der Kriminalität dar. Dabei sind nicht allein der Computer und seine Entwicklung von Bedeutung. Die zusammenhängende globale Vernetzung unterschiedlicher Computersysteme führt ebenfalls zu einer Erschwerung der Verfolgung. Das Internet ist für Wirtschaftsunternehmen sowie staatliche Institutionen ein wichtiges Medium für die Übertragung von Informationen geworden. Die wettbewerbsorientierten Wirtschaftssysteme erfordern immer schnellere Kommunikationsformen. Das neue Medium bietet hier im Vergleich zu anderen Technologien eine überlegene Plattform. Der weltweite Zusammenschluss von Computern führt zudem zu bedeutenden sozialen und gesellschaftlichen Veränderungen. Der gesellschaftliche, kulturelle und bildungspolitische Einfluss des neuen Mediums ist erheblich. Der Computer und das Internet werden zunehmend auch von Personen für kriminelle Zwecke genutzt. Straftäter haben den Computer und das Internet als leistungsfähiges Medium erkannt. Mit dem neuen Medium haben sich auch neue Deliktsfelder eröffnet. Dazu zählen unter anderem die Verbreitung von Viren und das Ausspähen von digitalen Daten. Daneben bietet das Internet viele Möglichkeiten, die „klassischen“ Straftaten zu begehen. Es erleichtert Straftätern zum Beispiel im Bereich der Pornographie oder in dem des politischen Extremismus die Kommunikation und die Verbreitung von Inhalten und Daten. Die Palette der möglichen Computerdelikte reicht von leichten Beleidigungsdelikten über Glücksspiele und Betrug bis hin zu Gefährdungen des Rechtsstaats.

Durch die gesellschaftlichen Veränderungen im Bereich des Alltags, der Freizeitgestaltung oder des Berufslebens entstehen mit dem Computer und dem Internet auch neue Gruppierungen. Dabei haben sich in den letzten Jahren im Bereich der Programmierung und der interaktiven Kommunikation verschiedene hoch spezialisierte Subkulturen gebildet. Im Bereich der Computerkriminalität wird meist von der so genannten Hackerszene gesprochen. Gemeint sind damit im Allgemeinen jugendliche Computerfans, die in fremde Computersysteme eindringen. Die Tätigkeiten der Hacker werden zum Teil mit politischen und gesellschaftlichen Zusammenhängen verknüpft. Dabei kristallisiert sich als typisch angesehener Krimineller mehr und mehr ein klischeehafter genialischer Einzeltäter heraus. Wer Hacker sind, wie die

Hackerszene aussieht, wie Hacker vorgehen, ob sie als Einzeltäter oder in Gruppen agieren und ob alle Handlungen von Hackern krimineller Art sind, bleibt dabei meist unberücksichtigt.

Computerkriminalität wird grundsätzlich als ein Teil der Wirtschaftskriminalität betrachtet.[1] Im Bereich der Wirtschaftskriminalität befassen sich Kriminologen bislang schwerpunktmäßig mit den traditionellen Vermögensdelikten wie Betrug und der White Collar-Kriminalität[2], Verbandskriminalität und dem Missbrauch öffentlicher Stellungen. Quantitativ dominieren wirtschaftlich orientierte Delikte. Die Computermanipulation stellte bis Ende der 1970er-Jahre die häufigste Erscheinungsform der Computerkriminalität dar. Heute steht bei den polizeilich erfassten Fällen die Softwarepiraterie im Vordergrund.[3] Auf Schulhöfen und in Internetbörsen werden Filme, Musikstücke und Softwareprogramme untereinander ausgetauscht. Bei der Frage, warum Kriminologen sich so ungern mit dem Bereich der Hackerszene und deren Kriminalitätsform der Computerkriminalität beschäftigen, fällt vor allem ins Auge, dass neben kriminologischen Aspekten ein umfangreiches computertechnisches Verständnis erforderlich ist, um die Vielseitigkeit dieser neuen Deliktform zu verstehen. Trotz dieser zusätzlichen Erfordernisse müssen Kriminologen sich in Zukunft mit der Computerkriminalität und deren Tätern beschäftigen, da die Digitalisierung im Beruf und Alltag zunehmend an Bedeutung gewinnt.[4]

Informations- und Kommunikationstechnologien durchdringen mittlerweile alle Lebensbereiche. Wirtschaft und Gesellschaft sind einem tief greifenden Strukturwandel ausgesetzt.[5] Der Computer und das Internet als weltweites Datennetz haben in den letzten Jahren eine rasante Weiterentwicklung erfahren. Digitale Medien sind inzwischen ein bedeutender Wirtschaftsfaktor geworden, aber auch ein überaus wichtiger Träger von Information und Kommunikation in nahezu sämtlichen Lebensbereichen. Sowohl öffentliche Einrichtungen als auch Wirtschaft und Privatpersonen nutzen die durch das Internet eröffneten Informations- und Kommunikationsmöglichkeiten, und zwar mit ansteigender Tendenz. Das Internet basiert auf dem Grundkonzept von Offenheit und Freiheit der Informationen. Jedermann kann an dem freien

[1] Göppinger 1997, S. 545 ff.; Eisenberg 2005, S. 964 ff.
[2] Scheerer 1993, S. 246 ff.
[3] Göppinger 1997, S. 547.
[4] Ulrich Sieber vom Max-Planck-Institut für ausländisches und internationales Strafrecht in Freiburg sieht Internetkriminalität als den sich am schnellsten entwickelnden Deliktbereich in Europa an.
[5] Geiger 2000, S.129.

Austausch von Informationen teilnehmen. Zugleich wird das Internet jedoch auch für kriminelle Handlungen missbraucht.

Die zunehmende Computerisierung und Vernetzung der Haushalte und Unternehmen ermöglicht es Hackern, von zu Hause aus kriminelle Handlungen zu begehen. Dabei werden der Computer und das Internet mit den damit zusammenhängenden neuen Gelegenheiten genutzt. Fähigkeiten und Kenntnisse, die Erwachsene im Bereich informationstechnischer Neuerungen erst verinnerlichen müssen, werden von Jugendlichen bereits früh erkannt und sich angeeignet.[6] Dabei stellt sich auch die Frage, ob die Täter sich des Ausmaßes ihrer kriminellen Handlungen überhaupt bewusst sind.

Neben dem eigenen Zimmer als neuer Tatmodalität treten mit dem Computer neue Anreize hinzu, welche sich aus Softwareprogrammen und Betriebssystemen ergeben und die Möglichkeiten der kriminellen Nutzung vervielfältigen. Durch die Anonymität des Internets wird der Reiz verstärkt, Neues zu entdecken.[7] Täter können erstmals unzählige Webseiten mit unterschiedlichen Inhalten unbemerkt ansehen, sie können anonym chatten und E-Mails verschicken. Webseiten zeigen und erklären, wie man sich in fremde Netzwerke einschleust, Daten manipuliert, Viren, Trojaner oder Würmer problemlos selbst gestalten kann, Firewalls umgeht, Passwörter und technische Lücken der Betriebssysteme identifiziert. Hinzu kommen weitere Gelegenheiten, die das Internet bietet: In interaktiven Tauschbörsen können Musik, Filme, Spiele, Klingeltöne und viele andere digitalisierte Daten ohne Qualitätsverlust heruntergeladen, kopiert und an Dritte weitergegeben werden. Dabei bleibt zwar zu bedenken, dass das Internet nicht anonym ist. Jeder Datentransfer und jede Handlung im Netz kann durch Registrierungsdateien[8] nachgewiesen werden. Dies würde jedoch einen immensen Auswertungsaufwand hinsichtlich der Registrierungsdateien bedeuten. Diese Daten werden daher meist nur bei größeren Schadenssummen von den staatlichen Verfolgungsbehörden ausgewertet, so dass aufgrund der geringen Verfolgung von einer zumindest empfundenen Anonymität ausgegangen werden kann.

Für die Urheber und Vermarkter der digitalen Produkte bedeuten die Angriffe auf Computersysteme finanzielle Verluste und Imageschäden. In diesem Zusammenhang ist das bisherige

[6] Hebecker 2001, S. 109 ff.
[7] Das Internet ist nur bedingt anonym, man kann aber zumindest von einer empfundenen Anonymität ausgehen.
[8] Man spricht hier meist von so genannten Log-Dateien, auf denen Zugriffe auf Rechner festgehalten werden. Gleichzeitig besitzen Server, auf denen sich User anmelden, derartige Log-Dateien, mit denen herausgefunden werden kann, welcher Rechner sich wann und wo angemeldet hat.

Ausmaß von Schadenshöhe und Schadensart übertroffen worden. Hacker können im Bereich der Wirtschaftskriminalität tätig werden, indem sie sich in Intranets einhacken, dort Daten manipulieren oder kopieren, mit Viren und Würmern ganze Netzwerke lahm legen oder auf Tauschbörsen oder auf dem Schulhof Musik, Filme und Software tauschen und damit die Verkaufszahlen ganzer Industriezweigs erheblich mindern. Das Ausmaß der Schäden beläuft sich nach Schätzungen der betroffenen Branchen teilweise auf Beträge in dreistelliger Millionenhöhe.[9] Dabei soll nicht unbeachtet bleiben, dass einige Softwarehersteller erst durch die Verbreitung von Raubkopien überhaupt bekannt geworden sind und sich infolgedessen auf dem Markt etablieren konnten. Angriffe, die auf die Spionage und Nutzung von Börsendaten abzielen, welche in zunehmendem Maße online transferiert werden, könnten sich ebenfalls global auf das Wirtschaftsgeschehen auswirken.

Neben der Wirtschaft sind auch politische, universitäre und private Einrichtungen betroffen. Die Auswirkungen der Computerkriminalität sind mittlerweile beträchtlich und eine Bedrohung für staatliche Organe geworden. Durch die Nutzung von Netzwerken durch staatliche Instanzen wie z.B. das Militär ergibt sich etwa die Gefahr zwischenstaatlicher Konflikte infolge von Attacken mittels staatlicher Computerressourcen. Außerdem sind Attacken auf die Infrastruktur eines Staates wie Stromversorgung, Flugsicherheit oder Telefonsystem über den Missbrauch von Computer- und Kommunikationsnetzwerken nicht auszuschließen.[10] Es ist Hackern möglich, weltweit alle über das Internet vernetzten Systeme zu manipulieren. Je stärker der Einfluss von Computernetzwerken auf globaler wie auf lokaler Ebene ist, desto mehr sind die oben genannten Bestandteile der Gesellschaft diesen und weiteren Gefahren durch Computerkriminalität ausgesetzt.

Die Gefahren des Computermissbrauchs durch Hacker liegen neben quantitativen besonders in qualitativen Gesichtspunkten begründet. Sie beruhen im Speziellen auf der Verletzlichkeit

[9] Kaiser 1996, S. 879; www.ftd.de/tm/it/1073815421239.html?nv=rs (zuletzt abgerufen am 10.03.04); www.spp.at/Sicherheit/Viren/Sicherheit.jsp (zuletzt abgerufen am 10.11.04); www.chip.de/news/c_news_11103940.html (zuletzt abgerufen am 10.11.04); www.heise.de/tp/deutsch/inhalt/te/16051/1.html (zuletzt abgerufen am 10.11.04); www.nzz.ch/netzstoff/2002/2002.09.24-wi-article8DKDJ.html (zuletzt abgerufen am 10.11.04).

[10] Die CIA warnt seit Mitte der neunziger Jahre davor, dass die nationale Sicherheit durch Cyber-Attacken auf Kraftwerke, Banken, Flugsicherung oder Streitkräfte zunehmend bedroht sei. Diese Gefahren gingen, so die Sicherheitsbehörden, nicht nur von feindlichen Staaten aus, sondern auch von Insidern und Teenagern. Zu finden unter http://userpage.fu-berlin.de/~bendrath/SuF_2000.rtf. Auch die Kommission der Europäischen Gemeinschaft weist auf eine besorgniserregende Zunahme von Übergriffen auf private, wirtschaftliche und staatliche Computersysteme und dabei im Speziellen auf jugendlichen Täter hin. Diese als Hacker beschriebenen Täter sind laut EU-Kommission zunehmend besser organisiert. Zu finden unter http://www.computerundrecht.de/cybercrime27.doc (zuletzt abgerufen am 07.07.2004).

der modernen Informationsgesellschaft, da Wirtschaft, Verwaltung und in zunehmendem Maße auch der private Sektor von der Sicherheit der modernen Informationstechnologien abhängig sind. Elektronische Bank- und Wertpapiergeschäfte (E-Banking, E-Brokerage) setzen beispielsweise die Möglichkeit voraus, Informations- und Liquiditätsquellen jederzeit und von jedem Ort aus abzurufen. Es wird eine Vielzahl der Geldtransaktionen in der Wirtschaft über Computersysteme abgewickelt. In Büros nehmen Intranet, Internet und E-Mail einen wichtigen Bereich der Informationsbeschaffung ein. Der elektronische Handel in Computernetzen ist in großem Umfang von sicheren Transaktionssystemen abhängig, und in vielen Fabriken ist über die Fertigungssteuerung der gesamte Produktionsprozess auf die Funktionsfähigkeit der EDV angewiesen. Die fortschreitende Konvergenz der verschiedenen Anwendungen integriert die Funktionen von Handy und Personal Digital Assistant. Mit einem einzigen Gerät kann man also mobil telefonieren und im Internet surfen. In zahlreichen Unternehmen wie auch im privaten Bereich werden die wichtigsten Betriebsgeheimnisse und in vielen anderen Bereichen sicherheitsrelevante Informationen in digitalen Speichern abgelegt. Schifffahrts- und Luftüberwachungssysteme beruhen ebenfalls auf Computersystemen. In zunehmendem Maße werden die Börsen weltweit digitalisiert und betreiben das Marktgeschehen ausschließlich online. Kernkraftwerke werden mittels elektronischer Systeme betrieben und kontrolliert und Krankenhäuser verlassen sich bei der medizinischen Überwachung zunehmend auf digitale Endgeräte.

Internationale Datenverarbeitungs- und Datenkommunikationssysteme sind damit zu den Nervenzentren der Wirtschaft, des öffentlichen Bereichs sowie des privaten Sektors geworden. Aufgrund der hieraus resultierenden Abhängigkeit der modernen Informationsgesellschaft haben sich Computerdelikte zu einer zentralen Bedrohung der modernen Informationsgesellschaft entwickelt. Der Einsatz des Computers in fast allen Lebensbereichen sowie der Zusammenschluss über weltweite Computernetze führt zu unberechenbaren und international ausgerichteten Deliktsformen und deren Folgen.

1.2 Fragestellung

Die Computerdelikte sind ein Kriminalitätsbereich, der sich parallel zu der Computertechnik entwickelt hat und durch eine ständige Anpassung an die veränderten Bedingungen auf diesem Gebiet geprägt ist.[11] Aufgrund der Erleichterung von Straftatbegehungen, des hohen Ge-

[11] Kaiser 1996, § 74 Rn. 61.

fährdungspotenzials, das von Computerdelikten ausgeht, sowie des bisher fehlenden Problembewusstseins soll in dieser Arbeit die Frage untersucht werden, welche Computerdelikte möglich sind, wie sie gestaltet und ausgeübt werden können.

Mit der Computertechnologie sind auf diesem Gebiet auch neue Szenen entstanden. Um den Problembereich der Hackerszene und des unberechtigten Zugangs zu Computerdaten aus kriminologischer Sicht untersuchen zu können, muss Klarheit über die in diesem Zusammenhang auftretenden Tathandlungen (Vorgehensweisen), Strukturen und Beweggründe der Szene geschaffen werden. Diese Darstellung dient als Anknüpfungspunkt für die anschließende kriminologische Betrachtung. Somit soll die Arbeit die neu entstandene Hackerszene, deren Kultur, Vorgehensweise und Beweggründe erläutern und kriminologisch erfassen. Dabei soll ebenfalls die Frage untersucht werden, ob die Hacker die einzigen Computerkriminellen sind oder ob neben ihnen noch andere Gruppierungen existieren, die gleichermaßen kriminell handeln, und ob die Kriminalisierung der Hackerszene sich zum Teil als ein Zuschreibungsprozess darstellt.

Es stellen sich folgende Fragen: Welche Probleme ergeben sich für eine Definition von Computerkriminalität? Welche Delikte gibt es im Bereich der Computerkriminalität und mit welchen Besonderheiten sind sie ausgestattet? Welche neuen Kriminalitätsformen sind durch den Computer entstanden? Lassen sich die Delikte im Bereich der Computerkriminalität strukturieren? Welche neuen Tätergruppen entstehen durch die Computerisierung und wie lassen sich diese neuen Formen kriminologisch erfassen und verstehen? Als Haupttätergruppe werden zumeist Hacker und deren Szene als die eigentliche Tätergruppe bezeichnet. Es soll die Frage geklärt werden, wie die Hackerszene strukturiert ist. In diesem Zusammenhang wird dann untersucht, welche Motive Hacker zu kriminellem Verhalten verleiten.

1.3 Aufbau und Vorgehensweise

Ziel der Arbeit ist es zu zeigen, wie Täter im Bereich der Hackerszene kriminell werden und welche Beweggründe sie zu diesem Handeln verleiten. Es geht darum, den (Regelungs-) Bereich, auf den sich strafrechtliche Normen beziehen, in seinem Eigensinn kennen zu lernen, und zwar bevor der Staat mit seinem massiven Interventionsinstrumentarium in ihn hineinre-

giert.[12] Bevor der Staat beginnt, alle möglichen Handlungsweisen zu sanktionieren, die von Hackern begangen werden, sollten ihre Handlungsweisen und Beweggründe zumindest verstanden werden.

Der erste Teil stellt empirische Erhebungen zu Computerdelikten vor, dem dann zwei aktuelle Bezüge folgen. Mit dem zweiten Teil soll ein Überblick über die vorhandenen Computerdelikte geschaffen werden. Diese sollen sodann typologisiert werden, wobei der Schwerpunkt auf den Delikten liegt, die von Hackern begangen werden können. Es werden alle bislang bekannten kriminellen Handlungen, die mit dem Computer und dem Internet zusammenhängen, aufgezeigt und erläutert. Nicht alle Deliktgruppen werden gleichermaßen ausführlich dargestellt. Ein Schwerpunkt der Arbeit soll darin liegen, die Begehungsweisen und Deliktarten genauer darzustellen und zu erläutern, die mit der Digitalisierung hinzugetreten sind oder einen Wandel erfahren haben. Delikte, die durch den Computer nur eine geringe Veränderung erfahren haben oder diesen sogar nur als neues Medium nutzen, sollen nur kurz dargestellt werden.[13] Höhe und Ausmaß der Schäden werden exemplarisch anhand von Einzelfällen aufgezeigt.

Im dritten Teil liegt der Schwerpunkt auf der Hackerszene und deren Motiven für kriminelle Handlungen. Nach einer Darstellung der Entstehungsgeschichte der Hacker wird anhand von ausgewählter Forschungsliteratur die Hackerszene und ihre Strukturen untersucht. Dabei soll die Frage behandelt werden werden, ob es sich bei der Hackerszene um eine homogene Tätergruppe handelt oder ob die Szene aus verschiedenen Gruppierungen besteht, die sich jeweils im Alter und Aufbau unterscheiden. Dabei ist entscheidender Schwerpunkt dieses Teils die Herausarbeitung der Motive, die Hacker zu kriminellem Verhalten verleiten.

Im vierten Teil der Arbeit wird anhand der Self-Control Theory erklärt, aus welchen Gründen die Hacker Computerdelikte begehen. Dabei wird zunächst die Self-Control Theory in ihren

[12] Ein Beispiel hierfür dürfte die Urheberrechtsreform (BGBl. I 1774) darstellen, die unter massivem Druck der Wirtschaft zu einer Änderung des Urhebergesetzes führte und vor allem darauf abzielte, das Tauschen von Musik- und Filmdateien über Internettauschbörsen zu unterbinden. Das Tauschen von Dateien über Tauschbörsen kann unter Jugendlichen wohl als ubiquitär bezeichnet werden. Die Beweggründe Jugendlicher sind hierbei nicht allein wirtschaftlicher Art. Auch der Reiz des neuen Mediums, die Einfachheit, von zu Hause aus an Musikstücke und Filme zu gelangen, ohne dabei Öffnungszeiten und lange Schlangen vor Kassen beachten zu müssen, sind von Bedeutung. Ein zukünftiger von der Musik- und Filmindustrie bislang verschlafener Internetauftritt mit der Möglichkeit legal, schnell und unkompliziert Dateien herunter zu laden, könnte das illegale Raubkopieren stoppen. Ein Anfang wurde im Juni 2004 mit der Eröffnung des I-POD-Portals von Apple gemacht.

[13] In diesem Zusammenhang kann die Kinderpornografie erwähnt werden, die durch das Internet ein neues Medium zur Verbreitung und zur Kommunikation erfahren hat, die Struktur der Taten und ihre Schäden bleiben jedoch unverändert.

Kernaussagen dargestellt. Danach werden die gewonnenen Erkenntnisse genutzt, um die kriminellen Antriebe von Hackern zu erklären, und die gewonnenen Erkenntnisse wiederum auf die Self-Control Theory angewandt. Michael R. Gottfredson und Travis Hirschi bezeichnen ihre Self-Control Theory als „General Theory of Crime“. Ob diese Bezeichnung auch auf den Bereich der Computerkriminalität anwendbar und dazu geeignet ist, diese neue Kriminalitätsform zu erklären, wird ebenfalls im vierten Teil der Arbeit analysiert.

Gottfredson und Hirschi sehen die Ursachen für abweichendes Verhalten in fehlender Selbstkontrolle und vorhandenen Gelegenheiten verortet.[14] Erst die Kombination beider Faktoren veranlasse Täter dazu, Verbrechen zu begehen. Gottfredson und Hirschi definieren Low Self-Control als die Neigung von Personen, kurzfristigen Bedürfnissen eher nachzugehen, auch wenn sie mit langfristigen negativen Konsequenzen verbunden seien. Personen mit High Self-Control dagegen beziehen die künftigen Folgen in ihre Kosten-Nutzen-Kalkulation adäquat mit ein und sind weniger dazu bereit, den unmittelbaren Bedürfnissen zu erliegen.[15] Die Autoren sehen die Hauptursachen für die Herausbildung von Self-Control in der primären Sozialisation verortet, wobei der Schwerpunkt in einer effektiven Erziehung in den ersten acht Jahren gesehen wird.[16] Effektiv i.S.v. High Self-Control sei das erzieherische Verhalten nur, wenn folgende Verhaltensweisen bei den Eltern gegeben seien:[17]

1. Das Verhalten des Kindes muss überwacht werden.
2. Eltern müssen deviantes Verhalten wahrnehmen können.
3. Eltern müssen auftretendes deviantes Verhalten in angemessener Weise ahnden.

Die Beaufsichtigung des Kindes, das Erkennen und das effektive Bestrafen abweichenden Verhaltens führe zur Herausbildung von High Self-Control.[18]

High Self-Control reduziere aus der Sicht von Gottfredson und Hirschi zwar effektiv die Wahrscheinlichkeit von Verbrechensbegehungen, jedoch reiche das Fehlen von Self-Control allein nicht aus, um Kriminalität zu erklären. Neben Low Self-Control als zentralem Erklärungsprinzip müssten Gelegenheiten hinzukommen. Gottfredson und Hirschi sehen Gelegenheiten als wichtige Komponente für die Erklärung von Kriminalität an und integrieren sie in ihre General Theory of Crime. Fehlen Gelegenheiten, so komme es trotz mangelnder Self-

[14] Gottfredson/Hirschi 1990.
[15] Gottfredson/Hirschi 1994.
[16] Gottfredson/Hirschi 1990, S. 94 ff.
[17] Gottfredson/Hirschi 1990, S. 99 ff.
[18] Gottfredson/Hirschi 1990, S. 99.

Control nur mit geringer Wahrscheinlichkeit zu kriminellen Handlungen.[19] Gelegenheiten würden dabei von den Autoren in Anlehnung an die Routine-Activity-Theorie von L. E. Cohen und M. Felson definiert.[20] Danach hingen Gelegenheiten von dem Vorhandensein eines attraktiven Ziels und der Abwesenheit von Instanzen sozialer Kontrolle ab.

1.4 Empirische Erhebungen zu Computerdelikten

Unabhängig von definitorischen Problemen sollen zunächst einige empirische Erhebungen zur Computerkriminalität dargestellt werden. Nach Angaben der EU-Kommission liegen über das volle Ausmaß der Computerkriminalität kaum verlässliche Daten vor.[21] Die Zahl der bisher aufgedeckten Fälle und gemeldeten Übergriffe dürfte das tatsächliche Ausmaß eher verschleiern. Dieses Problem ist auf vielfältige Faktoren zurückzuführen: mangelnde Erfahrung und ungenügende Vorsicht bei den Systemadministratoren, geringes Anzeigeverhalten der geschädigten Unternehmen zur Vermeidung von Imageschäden und schlechte Ausbildung bezüglich der Computerkriminalität bei den staatlichen Verfolgungsbehörden.[22]

Im Folgenden sollen Statistiken Auskunft über das quantitative Ausmaß der Computerkriminalität geben. Dabei wird auf folgende Quellen zurück gegriffen: Die Polizeiliche Kriminalstatistik, Statistiken des CERT (Computer Emergency Response Team)[23] und Untersuchungen des CSI/FBI.[24]

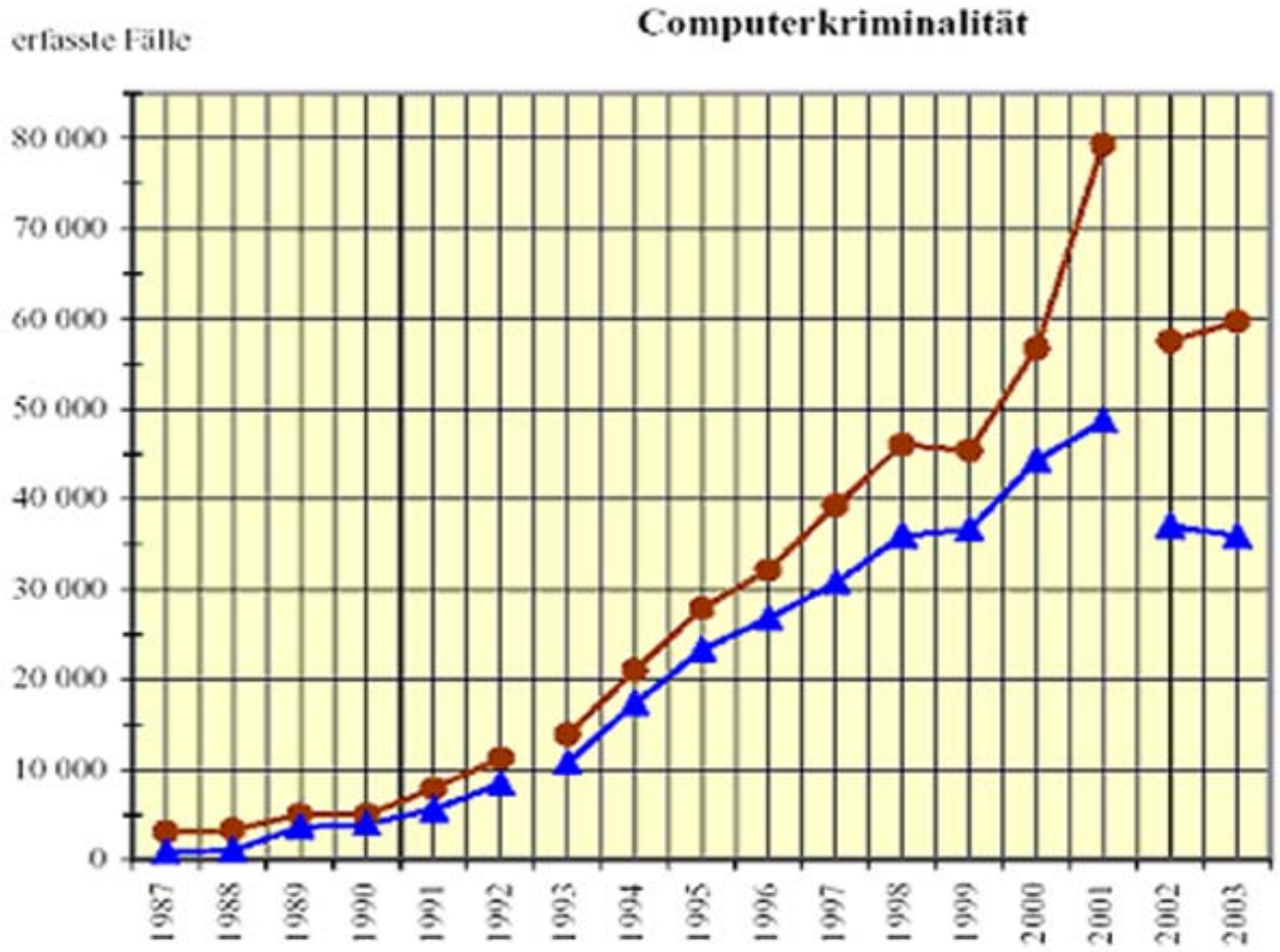
1.4.1 Die Polizeiliche Kriminalstatistik

Die Reichweite und Neuartigkeit des Deliktfelds der „Computerkriminalität“ führten auch zu neuen allgemeinen statistischen Aussagen in der Polizeilichen Kriminalstatistik (PKS). Um sinnvolle Aussagen treffen zu können, werden Computerdelikte in der PKS nach ihrer delikt-

---

[19] Gottfredson/Hirschi 1990, S. 89.
[20] Cohen/ Felson 1979; La Grange/ Silverman 1999, S. 47.
[21] http://www.computerundrecht.de/cybercrime27.doc (zuletzt eingesehen am 25 10.04)
[22] In einem Vorschlag der EU-Kommission vom 19.04.2002 wird der Bereich der Computerkriminalität und deren Tätergruppen als ein sehr ernst zu nehmendes und besorgniserregendes Problem diskutiert und darauf hingewiesen, dass das Problem auf Seiten staatlicher Einrichtungen darauf zurückzuführen sei, dass es zu wenige Erkenntnisse über das wahre Ausmaß gebe und zu wenige Erkenntnisse über die Technologie und die eigentlichen Tätergruppen herrsche. Es bestehe danach ein großer Bedarf an genaueren Informationen bezüglich der Computerkriminalität. Vgl. http://www.computerundrecht.de/cybercrime27.doc (zuletzt abgerufen am 07.07.2004).
[23] Hierbei handelt es sich um Organisationen, die sich mit Computersicherheit befassen, Warnungen bei Sicherheitslücken herausgeben und Lösungsansätze bieten.
[24] Das CSI (Computer Security Institute) ist ein Computersicherheitsinstitut in den USA, welches Computerangriffe analysiert, die sich gegen amerikanische Einrichtungen richten.

spezifischen Form gegliedert. Dabei trifft die PKS hauptsächlich Aussagen über das Hellfeld der Computerdelikte im Hinblick auf die Straftaten des Computerbetrugs, des Betrugs mittels Karten für Geldausgabe- und Kassenautomaten, Betrug mit Zugangsberechtigung zu Kommunikationsdiensten, der Fälschung von Computerdaten, der Datenveränderung und der Computersabotage, des unbefugten Verschaffens von Daten, Softwarepiraterie sowie im Hinblick auf Datenschutzverletzungen.



Straftaten(gruppen)	erfasste Fälle		Veränderung		Aufklärungsquote	
	2003	2002	absolut	in %	2003	2002
Computerkriminalität	59691	57488	2203	3,8	46,7	50.0
davon:						
Betrug mittels rechtswidrig erlangter Debitkarten mit PIN	35954	36969	-1015	-2,7	40	40,5
Computerbetrug -§263a StGB-	11388	9531	1857	19,5	43,2	57
Betrug mit Zugangsberechtigung zu Kommunikationsdiensten	7003	5902	1101	18,7	67	77,1
Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung -§§ 269, 270 StGB	237	228	9	3,9	86,5	80,7
Datenveränderung, Computersabotage -§§ 303a, 303b StGB-	1705	1327	378	28,5	39,3	38,1
Ausspähen von Daten	781	806	-25	-3,1	57,6	64,4
Softwarepiraterie (private Anwendung z.B. Computerspiele)	2053	1947	106	5,4	97,6	96,1
Softwarepiraterie in Form gewerbsmäßigen Handelns	570	780	-210	-26,9	97	95,1

Die rote Verlaufslinie zeigt die Entwicklung der gesamten Computerkriminalität von 1987 bis 2003 an. Mit der blauen Verlaufslinie wird die Zunahme von rechtwidrig erlangten Kreditkarten dargestellt. Deutlich ist ein stetiger Anstieg der Computerkriminalität zu erkennen. Von unter 5.000 erfassten Fällen im Jahr 1987 steigt die Zahl bis zum Jahr 2003 auf ca. 80.000 erfasste Fälle. Zwischen dem Jahr 1992 und 1993 ist ein Bruch in der Verlaufslinie zu erkennen. Dieser Bruch verdeutlicht, dass bis zum Jahr 1992 nur die alten Bundesländer einschließlich Berlin von der PKS erfasst wurden und ab dem Jahr 1993 das gesamte Bundesgebiet dargestellt wird. Interessant ist dabei, dass die rechtswidrige Erlangung von Kreditkarten als ein Teil der Computerkriminalität behandelt wird, obwohl dies aus technischer Sicht nur im entfernten Sinn mit Computern zu tun hat. Trotzdem macht dies den Großteil der erfassten Computerdelikte aus und der Anstieg verläuft hierbei sogar parallel zum Anstieg rechtswidrig erlangter Kreditkarten.

Im Jahr 1998 kommt es laut PKS erstmals zu einem leichten Rückgang der Computerkriminalität. In den beiden darauffolgenden Jahren ist ein sprunghafter Anstieg der Fallzahlen zu verzeichnen, da das Delikt Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten in die PKS aufgenommen wurde. Ein Vergleich mit den Zahlen aus den Vorjahren ist daher nur bedingt möglich. Für den erheblichen Anstieg könnten außerdem auch technische Verbesserungen in den Ermittlungsbehörden verantwortlich sein. Grundsätzlich sollte bei der Entwicklung der Computerkriminalität die Zunahme der Internetnutzung in der Bevölkerung berücksichtigt werden. Der Anteil der Internetnutzer lag 1999 in der deutschen Bevölkerung bei 13 Prozent und ist bis 2003 auf 51 Prozent gestiegen.

Im Jahr 2001 ist ein weiterer Bruch der Verlaufslinie zu beobachten. Dies liegt wiederum an einer Änderung der Erfassung der Computerdelikte. Bis zum Jahr 2001 spiegelt die blaue Verlauflinie Betrugsformen mittels rechtswidrig erlangter Karten für Geldausgabe- bzw. Kassenautomaten wieder. Ab dem Jahr 2002 wird hiermit die Zahl der Betrüge mittels rechtswidrig erlangter Debitkarten mit PIN (Schlüssel: 5163) gezeigt. Zudem ist durch die zusätzliche Aufnahme von Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten und der Veränderung im Jahr 2002 zu erkennen, dass die Computerdelikte einem schnellen Wandel unterzogen sind und die PKS nur schwer diesem Fortschritt nachkommen und ihn widerspiegeln kann.

In diesem Zusammenhang stellt sich die Frage, wie groß das Dunkelfeld im Bereich der Computerdelikte ausfällt. Die meisten digitalen „Einbrüche“ bleiben unentdeckt, da Beweismittel im Computer leicht manipuliert oder vernichtet werden können.[25] Werden sie jedoch aufgespürt, zeigen viele Unternehmen die Täter aufgrund des befürchteten Imageschadens erst gar nicht an.[26] Das Dunkelfeld wird überwiegend als sehr hoch eingeschätzt.[27] Bereits in einer Studie des Landesamtes für Verfassungsschutz Baden Württemberg aus dem Jahr 1996 wird eine Dunkelziffer von 85 Prozent genannt. Durch die vermehrte Internetnutzung und die Weiterentwicklung digitaler Endgeräte wird die Dunkelziffer heute noch höher ausfallen.

Aufgrund dieser Probleme und des hohen Dunkelfeldes sagen die Zahlen der PKS über die absolute Verbreitung der Computerdelikte nur relativ wenig aus. Jedoch ist der erhebliche Anstieg vor allem im Hinblick auf die mittel- und langfristige Entwicklung der Computerdelikte interessant. Der steile Anstieg der Computerdeliktsfälle und die Hinzunahme von neuen Schlüsselnummern in der PKS zeigt die rasante Entwicklung im Bereich der Computerdelikte.

Den höchsten Anteil der erfassten Computerdelikte nehmen die Betrugsfälle mittels rechtswidrig erfasster Debitkarten und der Computerbetrug ein. Allein diese Betrugsfälle machen über 60 Prozent der gesamten Computerkriminalität aus. Dabei stellt sich die Frage, ob es sich bei diesen Tätern um Jugendliche oder eher um Erwachsene handelt. Erstaunlich niedrig erscheinen die erfassten Fälle im Bereich der Datenveränderung/Computersabotage und des Datenausspähens, die zusammen nur einen Anteil von ca. 4 Prozent der gesamten Computerkriminalität ergeben. Im Bereich des Ausspähens von Daten ist die Zahl der erfassten Fälle von 806 auf 781 Fälle im Jahr 2003 gesunken. Es ergibt sich die Frage, ob tatsächlich so wenige Fälle des Datenausspähens stattfinden oder ob die geringe Zahl vielmehr auf andere Faktoren zurückzuführen ist. Diese Frage stellt sich vor allem vor dem Hintergrund der im Jahre 2003 vom Bundeskriminalamt erstellten Studie zum Account-Missbrauch im Internet.[28] Laut dieser Studie wird Computerkriminalität „als neue Massen- und Jugendkriminalität“ bezeichnet.[29] Die Zahlen der PKS geben jedoch keine Anhaltspunkte dafür, dass es sich hierbei um eine neue Form der Massenkriminalität handeln könnte. Die niedrigen Fallzahlen lassen vermuten, dass andere Gründe hierfür ursächlich sind und es ein sehr hohes Dunkelfeld gibt. Bei

[25] http://www.fuhs.de/de/fachartikel/artikel_de/millionending.shtml (zuletzt abgerufen am 07.07.2004).
[26] http://derstandard.at/?id=1695800 (zuletzt abgerufen am 07.07.2004).
[27] Beukelmann 2001 S. 56; Jessen 1994, S.19.
[28] Vick/Roters 2003.
[29] Die Studie wird im dritten Abschnitt der Arbeit genauer dargestellt und erläutert.

der Datenveränderung, Computersabotage und beim Ausspähen von Daten könnte ein nennenswerter Grund das Anzeigeverhalten der Opfer sein. Private Nutzer bemerken oft ein Eindringen erst gar nicht, und veränderte Daten führen sie oft auf ein mangelndes Technikverständnis zurück. Unternehmen wiederum wollen einen Imageschaden vermeiden und zeigen deshalb viele Übergriffe nicht an. Zudem könnte ein mittlerweile entstandenes Selbstverständnis ursächlich für ein geringes Anzeigeverhalten sein. Man akzeptiert es mittlerweile und hält es für normal, dass heutzutage in fremde Rechner geschaut und versucht wird, Daten zu verändern.

Trotz alledem muss berücksichtigt werden, dass die eigentlichen Gefahren der Computerkriminalität weniger in quantitativen, sondern eher in qualitativen Gesichtspunkten begründet sind. Sie beruhen insbesondere auf der Verletzlichkeit der modernen Informationsgesellschaft, die aus der Tatsache resultiert, dass Wirtschaft, Verwaltung und in zunehmendem Maße auch der private Sektor heute in hohem Maße von der Sicherheit der modernen Informationstechnologien abhängen. Wichtig ist somit nicht, wie oft mittels rechtswidrig erlangter Debitkarten ein Betrug verübt wird oder wie oft Daten in fremden Systemen ausgespäht werden. Vielmehr ist im Bereich der Computerkriminalität von Bedeutung, dass ein Einzelner immensen Schaden anrichten kann. Es stellt einen großen qualitativen Unterschied dar, ob ein Hacker Daten eines Privatrechners oder die einer staatlichen Einrichtung ausspäht, ob ein einzelner Rechner zum Absturz gebracht wird oder weltweit ganze Netzwerke ausfallen. Trotz der unterschiedlichen Qualität der einzelnen Delikte werden die Taten in der PKS nur als jeweils ein erfasster Fall gespeichert. Die qualitativen Unterschiede der Delikte werden durch die PKS keineswegs angezeigt. Im Bereich der Gewaltdelikte findet eine Abstufung der Gewaltqualität von leichter Körperverletzung bis hin zum Mord statt. Wenn auch eine strafrechtliche Unterteilung der Deliktqualität noch nicht stattfindet, so sollte zumindest die PKS auf diese Problematik eingehen.

1.4.2 Computer Emergency Response Team (CERT)

Das CERT, mit dem Sitz an der Carnegie Mellon University of Pittsburgh/U.S.A, wird als der Vorreiter bei der Verbreitung von Informationen über Sicherheitsfragen im Internet angesehen. Der Informationsfluss erfolgt dabei zumeist über Mailinglisten. Dort werden sicherheitskritische Themen erörtert und aktuelle Warnungen ausgegeben. Bislang handelt es sich dabei um Meldungen, die von Unternehmen an das CERT weitergeleitet werden.

In Deutschland hat sich neben dem CERT der Universität Stuttgart und dem CERT des Deutschen Fortschungsnetzes auch das Mcert etabliert. Dies richtet sich vor allem an klein- und mittelständische Unternehmen und wurde von der BITKOM in Zusammenarbeit mit dem Bundesministerium des Innern und dem Bundesministerium für Wirtschaft und Arbeit gegründet. Aufgaben rund um die Computersicherheit in den Institutionen der BRD übernimmt seit dem 1. September 2001 das eigens hierfür gegründete CERT des Bundesamts für Sicherheit in der Informationstechnik.

1988-1989

Jahr	1988	1989
Zwischenfälle	6	132

1990-1999

Jahr	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999
Zwischenfälle	252	406	773	1.334	2.340	2.412	2.573	2.134	3.734	9.859

2000-2003

Jahr	2000	2001	2002	2003
Zwischenfälle	21.756	52.658	82.094	137.529

Anzahl der gemeldeten Zwischenfälle.
Gesamtzahl der gemeldeten Zwischenfälle (1988-2003): 319 992
Quelle: CERT/CC-Statistik 1988-2003

Seit 1988 mit ganzen 6 Übergriffen nimmt die Anzahl der Zwischenfälle exponentiell zu. Bei den Zwischenfällen kann es sich um Virenattacken, Datenausspähversuche, Datensabotagehandlungen oder alle sonstigen Übergriffe handeln, die darauf abzielen, in ein System einzudringen, dort Daten zu erfassen oder zu manipulieren. Allein vom Jahr 2001 bis 2003 haben sich die Übergriffe verdreifacht. Die starke Steigerung an Zwischenfällen ab dem Jahr 1999 stärkt die Vermutung, dass dies mit der erheblichen Zunahme von Internetnutzern ab dem Jahr 1999 zusammenhängt. Zu beachten bleibt hierbei, dass dies nur die von Unternehmen gemeldeten Zwischenfälle sind. Es kann vermutet werden, dass nur ein geringer Prozentsatz

an Unternehmen Übergriffe an CERT überhaupt meldet. Wie viele noch nicht gemeldete existieren, ist unsicher. Zudem werden Zwischenfälle auf privaten Rechnern nicht erfasst, so dass die eigentliche Zahl der Übergriffe erheblich höher sein wird. Jedenfalls lässt der Anstieg der Computerkriminalität in der PKS sich durch die CERT-Ergebnisse bestätigen, auch wenn eine unterschiedliche Datenerfassung stattfindet. Ebenfalls spielt eine Rolle, dass in einigen Ländern, wie auch in Deutschland, Computersabotage und das Ausspähen von Daten Antragsdelikte sind, so dass die Strafverfolgungsbehörden diesen Taten nicht selbstständig nachgehen können. Zudem muss bedacht werden, dass private Nutzer hier kaum miterfasst werden. Dies mag daran liegen, dass die Vielzahl der Privatnutzer nicht die Zeit hat und sich die Mühe macht, Daten über Zugriffe zu analysieren und diese weiterzuleiten. Es kann vermutet werden, dass die Mehrzahl der Nutzer Übergriffe erst gar nicht registriert, so dass von einer weitaus höheren Gesamtanzahl an Übergriffen ausgegangen werden muss, als diese Statistik zeigt.

1.4.3 CSI/FBI-Untersuchungen

Die Untersuchungen des Computersicherheitsinstituts Computer Security Institute (CSI) in Zusammenarbeit mit dem FBI haben zum Ziel, das Sicherheitsbewusstsein der Öffentlichkeit zu stärken und bei der Bestimmung des Ausmaßes der Computerkriminalität in den USA zu unterstützen. Die CSI/FBI-Berichte gelten als die meist zitierten Untersuchungen über das Ausmaß und die Reichweite der Computerkriminalität. Dabei wurden die Antworten von Praktikern der Datensicherheit in amerikanischen Unternehmen und Behörden analysiert. Hierbei deckten die Studien eine große Bandbreite an Angriffen auf, die erhebliche finanzielle Schäden verursachten.[30]

Anzahl der Vorfälle von Außerhalb	1 bis 5	6 bis 10	mehr als 10	Weiß nicht
1999	43%	8%	9%	39%
2000	39%	11%	8%	42%
2001	41%	14%	7%	39%
2002	49%	14%	9%	27%
2003	46%	10%	13%	31%
2004	52%	9%	9%	30%

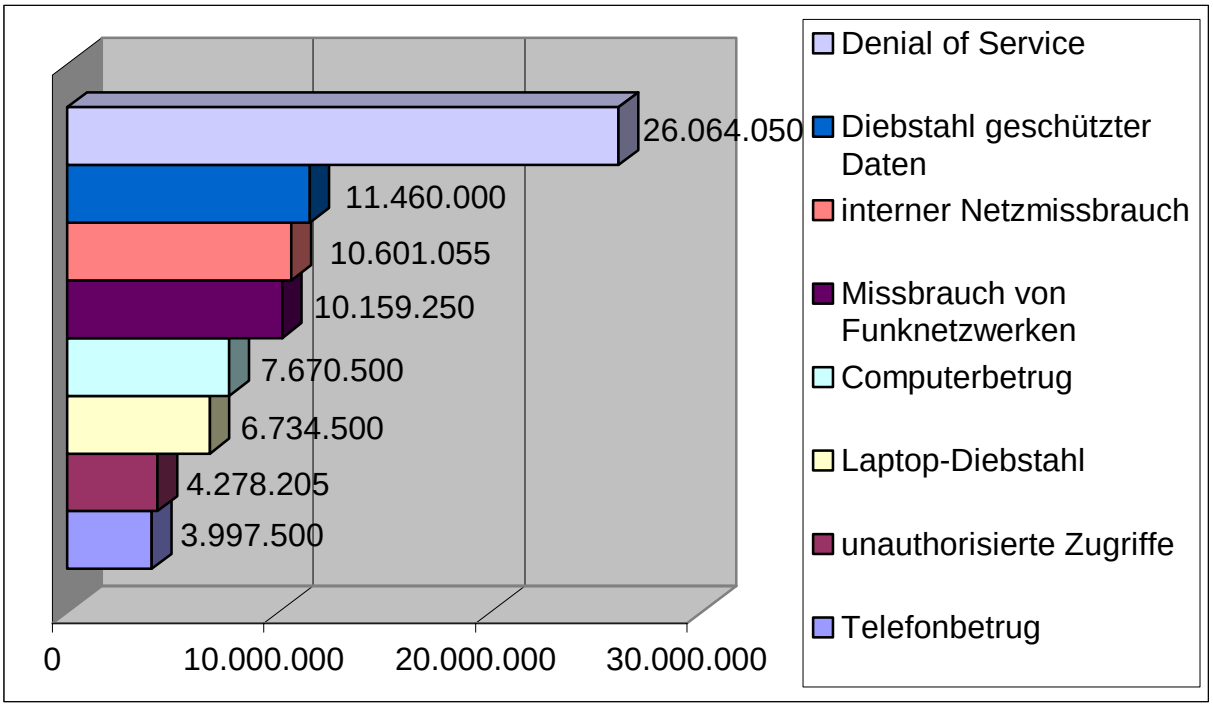
[30] Power 2001, S. 44 ff.

Anzahl der Vorfälle von Innerhalb	1 bis 5	6 bis 10	mehr als 10	Weiß nicht
1999	37%	16%	12%	35%
2000	38%	16%	9%	37%
2001	40%	12%	7%	41%
2002	42%	13%	9%	35%
2003	45%	11%	12%	33%
2004	52%	6%	8%	34%

Anzahl der internen und externen Vorfälle (1999-2004)
Quelle: CSI/FBI-Untersuchung 2004-07-27

Die Tabelle zeigt, dass die Anzahl der Unternehmen, die 1 bis 5 Übergriffe pro Jahr zu verzeichnen haben, von 1999 mit 43 Prozent bis 2004 auf 52 Prozent gestiegen ist. Rund ein Zehntel der Unternehmen hat jeweils 6 bis 10 oder mehr Übergriffe zu verzeichnen. Dabei ist auffällig, dass die Anzahl der Übergriffe von außen und diejenigen der Übergriffe von innen im Wesentlichen gleich hoch sind. Dies legt nahe, dass es eine gleich hohe Anzahl an internen Mitarbeitern wie an externen Hackern gibt, die versuchen, an Daten zu gelangen oder diese zu manipulieren. Auffällig ist, dass rund ein Drittel der Unternehmen nicht weiß, wie viele Übergriffe auf ihre Systeme stattfinden – möglicherweise ein Zeichen dafür, dass sich viele Unternehmen noch nicht mit Fragen der Computersicherheit beschäftigt haben. Ihnen ist somit nicht bewusst, dass interne und externe Übergriffe auf ihre Rechner stattfinden und die darauf befindlichen Daten gefährdet sind. Die Zahlen lassen vermuten, dass einem noch höheren Anteil an privaten Nutzern nicht bekannt ist, wie viele und welche Übergriffe auf ihre Rechner stattfinden. Das Problembewusstsein muss somit anscheinend als immer noch sehr gering eingeschätzt werden.

Wirtschaftliche Schäden der USA 2004



Höhe der Schäden in den USA in Dollar und nach Angriffsarten gegliedert
Gesamtschäden der USA im Jahre 2004: 141.496.560 Dollar
Quelle: CSI/FBI-Untersuchung 2004-07-27

Insgesamt wurde in den USA im Jahr 2004 ein Gesamtschaden von 141.496.560 Dollar ermittelt. Die höchsten Schäden weisen die so genannten Denial-of-Service-Attacken (DoS-Attacken) auf. DoS-Attacken sind Angriffe, die zum Ziel haben, den betroffenen Rechner zu schädigen. Sie existieren schon seit den Anfängen des Internets. Mit ihnen soll die Verfügbarkeit bestimmter Server und deren Dienste eingeschränkt oder verhindert werden. Ein Rechner kann auf unterschiedlichen Wegen unerreichbar gemacht werden. Man bombardiert ihn mit Softwarepaketen, die seine Ressourcen völlig ausschöpfen und ihn sogar zum Absturz bringen können.[31] Es stellt sich in diesem Zusammenhang die Frage, von welcher Tätergruppe die DoS-Attacken ausgehen. In Frage kämen neben Hackern auch andere Unternehmen, die versuchen, auf diesem Weg konkurrierende Firmen zu schädigen. Daneben erweist sich der Datendiebstahl als zweitwichtigster Faktor. Im ganzen zeigt diese Tabelle, dass Übergriffe von außen erhebliche Schäden anrichten. Interessant ist hierbei auch der Vergleich zur PKS. DoS-Attacken sind Übergriffe, die in den Bereich der Computersabotage fallen, welche in der PKS

[31] Eine vollständige Erklärung der Vorgehensweise und der daraus resultierenden Schäden wird unter dem Thema DoS-Attacken genauer dargestellt.

jedoch nur einen geringen Anteil an der gesamten Computerkriminalität hat. Dort sind vielmehr Kreditkartenmissbrauch sowie Computerbetrug ausschlaggebend. Ein Grund hierfür könnte sein, dass einzelne Deliktbereiche unterschiedlich definiert werden. Zudem liegt die Vermutung nahe, dass die PKS nur einen sehr kleinen Ausschnitt an Computerdelikten zeigt und der eigentlich große Bereich von ihr nicht abgedeckt wird. Die Gründe hierfür können unterschiedlichster Art sein. Die CSI/FBI-Tabelle mit internen und externen Vorfällen zeigt, dass etwa ein Drittel der Unternehmen nicht über die Vorfälle in ihrem Unternehmen Bescheid weiß, so dass es insofern zu keiner Anzeige kommen kann. Selbst Unternehmen, die alle Vorfälle registrieren, werden sich aus Befürchtung vor Imageschäden oftmals zurückhalten, Attacken anzuzeigen. Zu beachten ist zudem, dass die Tabellen nur Übergriffe auf Unternehmen und Behörden beinhalten. Private Nutzer werden hier nicht erfasst, so dass die eigentliche Quantität der Übergriffe ein weit höheres Maß darstellen wird, als dies aus den Statistiken ersichtlich wird.

1.5 Aktueller Bezug

1.5.1 Der Sasser-Wurm

Am 04.05.2004 häuften sich die Meldungen über einen neuen Computervirus.[32] Der Wurm mit der Bezeichnung „Sasser“ kann jeden mit dem Internet verbundenen Computer betreffen und verbreitet sich nicht per E-Mail. Sein „offizieller“ Name ist W32.Sasser.[33] Es handelt sich dabei um eine neue Art eines Computerwurms, der sich automatisch verbreitet. Es genügt, dass ein PC angeschaltet ist und sich mit dem Internet verbindet. Der ca. 15KB große Wurm verbreitet sich über das Netzwerk und nutzt dabei eine Sicherheitslücke im Local Security Authority Subsystem Service (LSASS) des Windows-Betriebssystems. Erkennbare Anzeichen einer Infektion sind dabei, dass ausführende Dateien mit den Bezeichnungen „avserve.exe“, „avserve2.exe“ oder „skynetave.exe“ im Windows-Verzeichnis gespeichert werden und eine Fehlermeldung, die den Absturz des Dienstes LSA Shell ankündigt, angezeigt wird. Sasser scannt[34] nach weiteren Rechnern, die ebenfalls diese Sicherheitslücke aufweisen und verbreitet sich über diesen Weg weiter. Er legt einen Eintrag in der Registry ab, um einen Autostart zu initiieren und kopiert sich mehrfach unter verschiedenen Namen in das Windows-Verzeichnis. Die Infizierung mit dem Wurm führt dazu, dass sich die betroffenen Computer

[32] http://www.spiegel.de/netzwelt/technologie/0,1518,298314,00.html (zuletzt abgerufen am 05.07.2004).
[33] http://de.wikipedia.org/wiki/Sasser (zuletzt abgerufen am 05.07.2004).
[34] Sasser scannt über den Port TCP 445 / TCP 9996.

mehrfach hintereinander automatisch aus- und wieder einschalten. Obwohl der Wurm aus technischer Sicht als harmlos einzustufen ist,[35] verursachte Sasser in den darauf folgenden Tagen einen beträchtlichen Schaden.

Einen erheblichen Effekt hatte Sasser im Computersystem der Post in Taiwan. Die dortige Post wurde am Dienstagmorgen zu einem Drittel lahmgelegt, 430 Filialen stellten auf handschriftliche Notizen um. Auch die taiwanesische Postbank stellte den Betrieb weitgehend ein, nur die Geldautomaten liefen weiter.[36] Zu den weiteren Banken, die von Sasser befallen wurden, zählen die Goldman Sachs[37], die australische Westpac Bank[38] und der finnische Finanzdienstleister Sampo[39]. Dort liefen zeitweilig keine Computersysteme mehr. Sasser infizierte daneben 1.200 Computer bei der EU-Kommission und verursachte erhebliche Probleme.[40] In Hongkong wurden zwei Ministerien und mehrere Krankenhäuser infiziert.[41] Unter den betroffenen Systemen waren Computer von Reiseunternehmen und öffentlichen Einrichtungen.[42] US-Flugunternehmen wie Delta Airlines, Air Canada oder British Airways meldeten zeitweilige Totalausfälle.[43] Regelrecht versenkt hat es nach einem Bericht der BBC auch die britische Küstenwache, die einen Totalausfall zu verzeichnen hatte. Alle Außenstationen waren demnach offline.[44] Daneben gab es Ausfälle an Schulen, Universitäten und Kreditinstituten.[45] Insgesamt befiel der Sasser-Wurm über sechs Millionen Rechner.[46] Beunruhigend ist die Tatsache, dass viele Informatiker die Auswirkungen von „Sasser“ noch als vergleichsweise harmlos einstufen. Für die Zukunft erwarten Sicherheitsexperten noch wesentlich verheerendere digitale Angriffe.[47]

Seit Anfang Mai 2004 jagten Ermittler den Schöpfer des Sasser-Wurms. Auch CIA, FBI[48] und der Softwaregigant Microsoft waren an der Suche beteiligt. Doch kein Computerexperte

[35] http://www.onlinekosten.de/news/artikel/14420/0 (zuletzt abgerufen am 05.07.2004).
[36] http://www.onlinekosten.de/news/artikel/14426 (zuletzt abgerufen am 05.07.2004).
[37] http://www.nwfusion.com/news/2004/0510sasser.html (zuletzt abgerufen am 05.07.2004).
[38] http://www.zdnet.com.au/news/security/0,2000061744,39146543,00.htm (zuletzt abgerufen am 05.07.2004).
[39] http://www.badische-zeitung.de/aktionen/2004/virus/126,1097278.html (zuletzt abgerufen am 05.07.2004).
[40] http://www.heute.t-online.de/ZDFheute/artikel/0/0,1367,COMP-0-2123808,00.html (zuletzt abgerufen am 05.07.2004).
[41] http://www.stern.de/computer-technik/internet/?id=523556 (zuletzt abgerufen am 05.07.2004).
[42] http://de.wikipedia.org/wiki/Sasser (zuletzt abgerufen am 05.07.2004).
[43] http://www.nwfusion.com/news/2004/0510sasser.html (zuletzt abgerufen am 05.07.2004).
[44] http://www.dslteam.de/news1380.html (zuletzt abgerufen am 05.07.2004).
[45] http://www.nwfusion.com/news/2004/0510sasser.html (zuletzt abgerufen am 05.07.2004).
[46] http://www.onlinekosten.de/news/artikel/14426 (zuletzt abgerufen am 05.07.2004).
[47] http://www.freenet.de/freenet/computer_und_technik/internet/antivirus/sasser/ (zuletzt abgerufen am 05.07.2004).
[48] http://www.tagesschau.de/aktuell/meldungen/0,1185,OID21781_TYP6_THE_NAVSPM1_REF1_BAB,00.html (zuletzt abgerufen am 05.07.2004).

aus Russland oder den USA ist der Vater von „Sasser“; bei dem Programmierer des Wurms handelt es sich um den 18-jährigen Schüler Sven J. aus Waffensen, einem kleinen Dorf mit 800 Einwohnern in der Nähe von Rotenburg in Niedersachsen.[49] Angespornt durch Gespräche mit ebenfalls computerbegeisterten Klassenkameraden entwickelte er den zuvor selbst entworfenen „Netsky-Wurm“ weiter. Durch eine Modifikation des Virus „Netsky“ entstand der Virus "Sasser". Über die dadurch entstandenen Folgen beziehungsweise Schäden soll sich der Schüler keine Gedanken gemacht haben.[50] Gegen den Programmierer des Computerwurms Sasser wurde im September 2004 Klage eingereicht.[51] Allerdings hatten die Ermittler einige Mühe, von den Unternehmen Auskunft über Schäden zu bekommen, da durchaus die Tendenz besteht, mit Sicherheitsproblemen nicht an die Öffentlichkeit zu gehen.[52] Das Verfahren, welches das Landgericht Verden im Januar 2005 wegen des besonderen Umfangs vom Amtsgericht Rotenburg übernommen hat, dauert bis zum jetzigen Zeitpunkt an.[53]

Als zweites soll ein Hackerangriff dargestellt werden. Trotz der vielen und auch aktuelleren Hackerangriffe auf kommerzielle Institute, wobei Microsoft hierbei bevorzugt wird, soll im Folgenden ein Hackerangriff auf eine politische Einrichtung dargestellt werden um zu zeigen, dass die Gefährlichkeit und das kriminelle Interesse ein gefährliches Ausmaß haben. Auch wenn die Masse der Hackerangriffe kleineren Umfang haben, sich auf das Hacken von Webseiten, Kreditkartennummern oder Informationen mit recht geringer Brisanz konzentrieren, so soll die folgende Darstellung zeigen, dass durch die Digitalisierung und Vernetzung der Systeme und Lebensbereiche kriminelle Übergriffe von Hackern auf politischen und wirtschaftlichen Ebenen möglich sind und aus diesem Grund besser verstanden werden müssen als dies bislang der Fall ist.

1.5.2 Der Pentagon-Hack

Am 25.02.1998 kam eine Zeitungsmeldung mit dem Titel „Hacker durchstöberten Pentagon-Computer“ heraus.[54] Ihr zufolge hatten Hacker zwei Wochen lang die Computer des US-Militärs im ganzen Land durchstöbert. Seit Oktober 1997 hatten Versuche, in Systeme des Verteidigungsministeriums einzudringen, dramatisch zugenommen. John Hamre, der damali-

[49] http://www.freenet.de/freenet/computer_und_technik/internet/antivirus/sasser/ (zuletzt abgerufen am 05.07.2004).
[50] http://www.net-tribune.de/article/080504-03.php (zuletzt abgerufen am 05.07.2004).
[51] http://www.netzeitung.de/internet/291366.html (zuletzt abgerufen am 05.07.2004).
[52] http://www.heise.de/security/news/meldung/48294 (zuletzt abgerufen am 05.07.2004).
[53] http://www.heise.de/security/news/meldung/55589 (zuletzt abgerufen am 15.05.2005).
[54] http://www.heise.de/newsticker/meldung/2007 (zuletzt abgerufen am 06.07.2004).

ge stellvertretende Verteidigungsminister, gab bekannt, dass dies bislang der am besten organisierte und systematischste Angriff gewesen sei, auch wenn er alle Anzeichen eines Spiels gezeigt habe.[55] Der Vorfall sei ein Warnsignal, dass erheblich mehr Anstrengungen zur Absicherung der Systeme und zur schnelleren Identifizierung der Hacker unternommen werden müssten.[56]

Die Angriffe geschahen in der Zeit, als die Krise zwischen den USA und Großbritannien und dem Irak wegen der Waffeninspektionen einen zwischenzeitlichen Höhepunkt erreichte. Beobachtet wurde ein Eindringen in viele Computersysteme aufgrund einer Sicherheitslücke des Solaris-Betriebssystems von Sun. Einige der Crackversuche ließen sich in den Nahen Osten zurückverfolgen. Daher nahm man im Pentagon an, dass der Angriff vom Irak ausgehen könnte, um die Stationierung und den Einsatz der amerikanischen Truppen zu stören.[57] Schon nach einigen Tagen stellte sich aber heraus, dass die Angriffe nicht vom Irak ausgegangen waren. Schließlich stieß man auf zwei kalifornische Teenager, die in die Computer des Militärs eingedrungen waren. Für sie sei das ein Spiel, ein Abenteuer gewesen, bekannte Makaveli, einer der beiden Täter, in einem Chat. Das Eindringen verleihe Macht.[58]

Als eigentlicher Kopf entpuppte sich der zunächst als „Pentagon-Hacker" bezeichnete „Analyzer", der sich meldete, als der Fall in den amerikanischen Medien Aufmerksamkeit fand.[59] 47 Agenten des FBI hatten sich an die Fersen des 18-jährigen geheftet.[60] Den entstandenen Medienrummel und Ruhm wollte „Analyzer", der als Lehrer der beiden Hacker gilt, nicht an sich vorbei ziehen lassen. Dank seiner Eitelkeit also wurde seine Identität bekannt. Dadurch konnte der „Analyzer" schließlich als der damals 18-jährige Ehud Tenenbaum aus Tel Aviv identifiziert werden.[61] Ehud Tenenbaum soll daneben auch in iranische und Hisbollah-Systeme eingedrungen sein.[62]

Die möglichen Folgen und Schäden solcher Übergriffe hängen dabei von der jeweiligen Motivation des Täters ab. Dabei kann ein Hacker einfach nur in das System hineinschauen und nichts weiter verändern, jedoch kann er auch wichtige Daten manipulieren und löschen oder

---

[55] Janet Reno gab kurz nach der Bekanntgabe der Angriffe die Absicht bekannt, eine neue nationale Behörde zur Verfolgung von Cyberkriminalität zu schaffen. Hervor ging daraus das National Infrastructure Protection Center (NIPC).

[56] http://www.heise.de/newsticker/meldung/2007 (zuletzt abgerufen am 06.07.2004).

[57] http://www.heise.de/tp/deutsch/special/info/7910/1.html (zuletzt abgerufen am 06.07.2004).

[58] Ebd.

[59] http://www.e-media.at/home/meldung.asp?ID=669 (zuletzt abgerufen am 06.07.2004).

[60] http://rhein-zeitung.de/on/98/03/20/topnews/penthack.html (zuletzt abgerufen am 06.07.2004).

[61] http://www.e-media.at/home/meldung.asp?ID=669 (zuletzt abgerufen am 06.07.2004); http://www.lv1.ifkomhessen.de/hacker.htm#israelischer(zuletzt abgerufen am 06.07.2004).

[62] http://www.lv1.ifkomhessen.de/hacker.htm#israelischer (zuletzt abgerufen am 06.07.2004); http://www.hagalil.com/archiv/98/02/hacker.htm (zuletzt abgerufen am 06.07.2004).

diese Daten an andere Organisationen weitergeben.[63] Ehud Tenenbaum erklärte, er habe nur seine Fähigkeiten weiterentwickeln wollen, wenn er sich in die Informationsnetze großer Organisationen einschleiche. Am Ausspähen von Geheimnissen sei er hingegen nicht interessiert gewesen.[64] Er hatte Zugang zu mehr als 1.000 Internet-Servern und etwa 120.000 Passwörtern. Tenebaum erklärte, er habe sich erst in israelische Computersysteme gehackt, später aber auch Schlupflöcher in Systemen amerikanischer Computer gesucht und gefunden. Allerdings habe er nie im Sinn gehabt, größere Schäden anzurichten. Wenn er in ein System eingedrungen sei, habe er die Sicherheitslöcher wieder verschlossen, damit keine anderen Hacker mehr eindringen könnten.[65] Es ist nach seiner Ansicht eine Herausforderung, in die Systeme einzudringen und auf die Schwachstellen hinzuweisen. Das käme doch schließlich den Betroffenen zugute, da er dabei nichts lösche oder verändere.[66]

1999 wurde er nach dem israelischen Gesetz für Computerkriminalität angeklagt. Ende 2000 bekannte sich der Hacker der Verschwörung, des unerlaubten Eindringens in Computer, der Störung von Computersystemen und der Zerstörung von Beweisen für schuldig.[67] Er wurde sodann verurteilt und musste nach dem Urteil des Gerichts in Tel Aviv ein halbes Jahr unbezahlt einer gemeinnützigen Tätigkeit nachgehen. Dieses Urteil wurde von den Behörden der USA als nicht angemessen angesehen. Das FBI bezeichnete die Attacke als den „bislang am besten organisierten und systematischsten Angriff“ auf ein Computersystem.[68] Ehud Tenenbaum wurde aber trotz Drängens der USA nicht ausgeliefert, leistete seinen Militärdienst ab und gründete dann eine Sicherheitsfirma.[69] Der Fall gilt den amerikanischen Sicherheitsbehörden auch als Beleg dafür, wie schwer es sein kann, Hackerangriffe, die aus jugendlichem Überschwang geschehen, von solchen zu unterscheiden, die von einer feindlichen Organisation ausgehen.[70]

2. Computerkriminalität

Um Computerdelikte in ihrer ganzen Bandbreite verstehen zu können, werden im Folgenden der Begriff der Computerkriminalität definiert, die Geschichte des Computers vorgestellt und

[63] Das Pentagon hat den Cyberspace neben Land, Wasser, Luft und Weltraum längst zum „fünften Battleground“ erklärt.
[64] http://rhein-zeitung.de/on/98/03/20/topnews/penthack.html (zuletzt abgerufen am 06.07.2004).
[65] http://memopolis.uni-regensburg.de/speicher/memo369/public/verlust1998/public/analyzer/analyzer.html (zuletzt abgerufen am 06.07.2004).
[66] http://www.heise.de/tp/deutsch/inhalt/te/1420/1.html (zuletzt abgerufen am 06.07.2004).
[67] http://www.heise.de/tp/deutsch/special/info/7910/1.html (zuletzt abgerufen am 06.07.2004).
[68] http://www.e-media.at/home/meldung.asp?ID=669 (zuletzt abgerufen am 06.07.2004).
[69] http://www.heise.de/tp/deutsch/special/info/7910/1.html (zuletzt abgerufen am 06.07.2004).
[70] http://www.heise.de/tp/deutsch/special/info/7910/1.html (zuletzt abgerufen am 06.07.2004).

sodann ausgewählte deliktische Handlungen dargestellt und erläutert. Da Computerkriminalität in alle Bereiche des Lebens eingreifen kann, sobald der Computer als Medium in einer gewissen Art und Weise eingesetzt wird, müsste der Vollständigkeit halber das gesamte Strafgesetzbuch durchgeprüft werden und zu den jeweiligen Paragraphen einzelne und seltene darauf bezogene Fälle genannt werden. Dieses soll nicht Ziel der Arbeit und des folgenden Kapitels sein. Vielmehr sollen ausgewählte und bislang wenig dokumentierte und verstandene Delikte genauer betrachtet und dargestellt werden. Dabei werden nicht alle Delikte gleichgewichtig bearbeitet, sondern erfahren durch ihre Historie, ihren Stellenwert und ihre unterschiedliche technische Ausprägung eine jeweils unterschiedlich lange und intensive Bearbeitung.[71] Die einzelnen Delikte werden zudem durch Fallbeispiele in ihren kriminologischen Kontext gesetzt. Ebenfalls ist die Überwindung der begrifflichen Barrieren ein weiteres Ziel der folgenden Ausführungen.

2.1 Der Begriff der Computerkriminalität

Die Ausdehnung der Computerdelikte auf die verschiedensten Deliktsformen, vor allem auch durch das Internet, bestätigte die bereits in den 1980er Jahren festgestellte Erkenntnis, dass der Begriff Computerkriminalität ein überaus weites Spektrum von Delikten umfasst. Dabei ist der Begriff „Computerkriminalität“ sprachlich und juristisch uneindeutig. Trotz vieler Definitionsversuche in der Vergangenheit ist der Begriff bis heute nicht präzise kriminologisch bestimmt. Der Begriff soll als ein typisierendes Gliederungsmerkmal der Kriminalität gekennzeichnet werden, wie es ähnlich bei der Wirtschafts- und Rauschgiftkriminalität der Fall ist.

Schon bei der Begriffsbildung erkennt man unzählige Varianten, die den Begriff Computerkriminalität oder zumindest Teilaspekte dessen beschreiben und ihn unklar erscheinen lassen. Es wird dabei von Internetkriminalität, Multimedia-Kriminalität, Cybercrime oder gar Informations- und Kommunikationskriminalität gesprochen.[72]

Eine Legaldefinition dieses Begriffs existiert weder im materiellen Strafrecht noch im Prozessrecht, was darauf zurückzuführen ist, dass an diesen Begriff keine Rechtsfolgen geknüpft

[71] So beschränken sich die meisten Ausführungen zur Computerkriminalität darauf, kurz Viren, Trojaner und Hacker als Tätergruppe zu bezeichnen. Wie diese Formen genau zu definieren und voneinander abzugrenzen sind, wie sie benutzt werden und welche Schäden und Folgen sie verursachen können, bleibt bei den meisten Ausführungen im Dunklen.
[72] Kubica 2001, S. 75 ff.; Engel 2003, S. 83 ff.; Gerlach 2003, S.1 ff.

sind. Um im Folgenden Klarheit über den Begriff Computerkriminalität zu bekommen und zu verstehen, in welchem Sinne er in dieser Arbeit verwendet wird, sollen die wichtigsten Definitionen angesprochen und im Anschluss daran versucht werden, eine eigene Definition zu erarbeiten.

2.1.1 OECD-Definition

Eine Expertengruppe der Organisation für wirtschaftliche Zusammenarbeit (OECD) definierte den Begriff der Computerkriminalität sehr weit: als „any illegal, unethical, or unauthorized behaviour relating to the automatic processing and the transmission of data".[73]
Diese sehr weit gefasste Definition hat den Vorteil, dass sie alle Taten erfasst, die in irgendeiner Weise mit dem Computer im Zusammenhang stehen. Zudem bezieht sich diese Definition nicht allein auf den Begriff Computer, sondern bezieht allgemein Angriffe auf die Datenverarbeitung und deren Systeme mit ein. Ein wesentlicher Nachteil dieser Definition ist jedoch, dass ethisch verwerfliche Verhaltensweisen von der Definition mitumfasst sind. Ethik ist ein zeitlich stark wandelbarer und schwer zu definierender Begriff. Diese offene und weit gefasste Definition zieht Probleme hinsichtlich einer Eingrenzung nach sich, da direkte Rückschlüsse auf das verletzte Rechtsgut nicht mehr möglich sind.

2.1.2 Werkzeug oder Ziel der Tat

Vielfach wird unter Computerkriminalität jedes deliktische Handeln verstanden, bei dem der Computer Werkzeug oder Ziel der Tat ist.[74] Diese Begriffsbestimmungen sind sehr weitreichend, da sie auch solche Verhaltensweisen der Computerkriminalität zuordnen, die unter die „klassischen Straftatbestände" zu subsumieren sind und sich nur dadurch von anderen Fällen unterscheiden, dass die sich des Computers als Tatmittel bedienen bzw. zu der elektronischen Datenverarbeitung in einem unmittelbaren oder mittelbaren Zusammenhang stehen. Danach würde die Computerkriminalität in zahlreiche Deliktbereiche hineinreichen und wäre nicht auf bestimmte Straftatbestände beschränkt.

[73] Möhrenschlager 1991, S. 321, Fußnote 1; http://www.rz.uni-augsburg.de/connect/1997-01/compstrf/ (zuletzt abgerufen am 21.07.2004).
[74] Eisenberg 2005, S. 757; Schneider 1997, S. 165;

2.1.3 Vermögensverletzungen

Ebenfalls wird vertreten[75], dass es sich im Einzelfall um Computerkriminalität nur dann handelt, wenn am Ende der per Computer begangenen Tathandlung eine Vermögensverletzung steht: Demnach umfasst der Begriff Computerkriminalität alle vorsätzlichen, in einem Sachzusammenhang mit den Daten der EDV stehenden rechtswidrigen Vermögensverletzungen.[76] Er wird auf gegen fremdes Vermögen gerichtete computerspezifische Verhaltensweisen eingegrenzt und damit auf strafgesetzliche Bestimmungen ausgerichtet. Im Hinblick jedoch auf die schnell fortschreitende Technologie und die damit verbundenen Möglichkeiten krimineller Handlungen scheint ein solch enger Definitionsansatz nur einen bescheidenen Teil der möglichen computerbezogenen Deliktsformen zu erfassen.

Bei Anwendung dieses Rasters würden solche Fälle herausfallen, in denen mit Computerhilfe extern in Netzwerke eingedrungen wird, um dort Daten zu manipulieren, die erhebliche Folgen auf die Gesundheit von Menschen haben. Dabei kann es sich um Eingriffe in die Flugsicherheit, Eingriffe in Krankenhausnetzwerke und deren Patientendatenbanken oder Eingriffe gegen militärische Einrichtungen handeln. Zudem sollten Delikte, die vor der Digitalisierung und der Verbreitung des Internets offline erfolgt waren, aber sich zunehmend oder zum Teil nur noch digital und unter Zuhilfenahme des Internets ereignen, wie zum Beispiel die Kinderpornographie oder Urheberrechtsverletzungen, nicht gänzlich aus dieser Definition herausgenommen werden.

2.1.4 Netzkriminalität

Unter Netzkriminalität versteht man alle kriminellen Handlungen, die unter Zuhilfenahme von Computern und Netzwerken geschehen. Als Synonyme werden unter anderem Internetkriminalität und Cyber-Kriminalität[77] gebraucht.[78]

Netzwerke wie das Internet können für eine Vielzahl von Straftaten missbraucht werden. Dabei meint der Begriff Netzkriminalität hauptsächlich typische Computerdelikte, bei denen

[75] Sieber 1980.
[76] Sieber 1980, S. 29.
[77] International auch als Cybercrime bezeichnet. Dieser Begriff wurde auch auf dem G8-Cybercrime-Gipfel vom 15.-17. Mai 2004 in Paris benutzt.
[78] http://www.datenschutzzentrum.de/material/themen/cybercri/cyber_mv.htm (zuletzt abgerufen am 21.07.2004), http://www.heise.de/newsticker/meldung/21413 (zuletzt abgerufen am 21.07.2004).

Netzwerke durch Hackerangriffe, Viren und Würmer beschädigt werden (Ausspähen, Verfälschung und Löschung von Daten und andere destruktive Eingriffe in fremde Datenverarbeitungssysteme). Klassische Delikte wie der Betrug werden aber gerade heutzutage unter Ausnutzung von netzwerkgestützten Systemen begangen.[79]

Hinzu kommen Verstöße gegen das Datenschutzrecht, etwa die unzulässige Verarbeitung und Nutzung personenbezogener Daten in Netzwerken. Schließlich können Computernetze auch als Tatwerkzeuge für eine Vielzahl anderer unerlaubter Handlungen – von der Beleidigung bis zur Geldwäsche – verwendet werden. Weitere Delikte, bei denen unerlaubte Inhalte ins Netz gestellt werden, etwa rechtsextremistische Propaganda oder pornografische Abbildungen, sind nicht nur von besonderer Bedeutung, sondern finden zudem erhebliche öffentliche Beachtung. Somit erscheint auch diese Definition und Eingrenzung der Computerdelikte auf Netzwerke ungenügend.

2.1.5 Multimedia-Kriminalität

Der Begriff „Multimedia-Kriminalität“ stellt die Eigenarten der Verschmelzung von Computern, Netzwerken und herkömmlichen Geräten in den Vordergrund.[80]
Multimedia-Kriminalität beruht auf der Tatsache, dass die Computerkriminalität durch die Konvergenz der verschiedenen Medien zunehmend an Trennschärfe verliert. Mit der Verschmelzung der unterschiedlichen technischen Geräte wie Personal Computer, Fernsehempfänger, Handys, GPS-Systeme für Autos steht nicht mehr eine bestimmte Hardwarekomponente bzw. deren Missbrauch im Mittelpunkt, sondern der Einsatz digitaler Technik zur Darstellung multimedialer Elemente wie statischer Bilder, Videos oder Töne. Es gibt heutzutage bereits Fernsehgeräte und Mobiltelefone, die eine Nutzung der wichtigsten Internetdienste wie WWW und E-Mail ermöglichen. Bei dieser erweiterten Begriffsbildung geht es jedoch immer noch um Computerkriminalität, da die Nutzung digitaler Informationen auf der Hardwareseite stets den Einsatz von Computertechnik voraussetzt.
Jedoch wird durch eine solch allgemeine Definition der Bereich der Computerkriminalität derart weit geöffnet, dass es schwer fällt, Deliktformen diesem Bereich auf längere Sicht zuzuordnen. Die Frage, ob Handlungen der Computerkriminalität zuzuordnen sind, hängt somit davon ab, inwieweit das jeweilige mediale Gerät computertechnisch unterstützt wird. Allein

[79] Berühmtes Beispiel ist das Auktionshaus Ebay.
[80] Barton 1999; Sieber 1999.

auf eine technische Abgrenzung sollte jedoch der Begriff der Computerkriminalität nicht beschränkt werden.

2.1.6 Eigene Definition und Typologie

Einerseits ist die Computertechnologie ein sehr dynamischer und sich ständig verändernder Prozess, und zum anderen ist der Begriff Computerkriminalität ein typisierendes Gliederungsmerkmal der Kriminalität. Es erscheint im Bereich der Computerkriminalität sinnvoll, eine Trennung vorzunehmen. Erstens sollten alle typischen Computerdelikte von diesem Begriff erfasst werden können. Darunter wären alle Delikte zu verstehen, die sich gegen jede Form des ordnungsgemäßen Funktionierens einer elektronischen Datenverarbeitung richten.[81] Der Vorteil dieser Definition wäre, dass sie sich einerseits ausschließlich auf Datenverarbeitungsvorgänge konzentriert und Handlungen ausschließt, bei denen Computer als reines Tatmittel zur Begehung klassischer Delikte benutzt werden, und andererseits offen ist für zukünftige technische Neuerungen, die die Datenverarbeitung als zentrales System nutzen.[82] Hierunter würden die Computerspionage, -sabotage und die -manipulation fallen. Nicht hiervon erfasst wären hingegen der Computerbetrug und alle klassischen Delikte.

Zweitens sollten jedoch auch alle klassischen Delikte, die durch den Computer und die Digitalisierung der Daten einen derartigen Strukturwechsel erfahren haben, dass diese Delikte nur noch oder zu einem überwiegenden Teil mit computertechnischen Mitteln erfolgen können, von dem Begriff Computerkriminalität erfasst werden können. Es erscheint nicht sinnvoll, die veränderte Schwerpunktsetzung im deutschen Urheberrechtsgesetz in Bezug auf den Tausch von Musik und Filmdateien im Bereich der Computerkriminalität unberücksichtigt zu lassen. Musikstücke wurden zuerst digital in Netzwerken und auf digitalen Plattformen wie dem früheren Napster getauscht, diese wurden digital auf Computer geladen, um mit digitalen Endgeräten abgespielt werden zu können. Erst die Digitalisierung der Musik- und Filmdateien, die allgegenwärtige Nutzung von PCs in jedem Haushalt und die Vernetzung dieser Rechner un-

[81] Darunter würden bislang Angriffe mittels des Hackings, Viren, Würmer und Trojaner zählen.

[82] So darf es im Zusammenhang mit der Definition von Computerkriminalität keinen Unterschied machen, ob sich Hacker in Computernetze oder Satellitennetze einhacken, ob sie Viren für den Rechner oder für Handys erstellen, und ob Multimediageräte wie die heutigen Organizer (z.B. Palm) betroffen sind, da diese zwar nicht als Computer bezeichnet werden, im Grunde aber leistungsstärker und vielseitiger sind als Computer in den 1990er-Jahren. Allein der Eingriff in die Datenverarbeitung sollte somit den Bezug zur Computerkriminalität darstellen.

tereinander (z.B. Internet) ermöglichte die Entstehung einer neuen Form der Kriminalität.[83] Solche und kommende Entwicklungen müssen aus diesem Grund ebenfalls von dem Begriff Computerkriminalität erfasst werden, da sie ohne diese nie zustande gekommen wären. Es scheint somit sinnvoll, alle Deliktbereiche, bei denen die elektronische Datenverarbeitung eine gewichtige Rolle einnimmt, weil eine Begehung gerade nur mittels des Computers möglich wird, mit in den Begriff Computerkriminalität aufzunehmen. Hierunter würden alle Handlungen fallen, bei denen die elektronische Datenverarbeitung zur Planung, Vorbereitung oder zur Ausführung eingesetzt wird und einen wesentlichen Bestandteil der deliktischen Handlung ausmacht. Damit wären unter anderem Urheberrechtsverstöße, Computerbetrugsfälle oder die Verbreitung strafbarer Inhalte im Internet erfasst. Es soll zwischen Computerkriminalität im engeren und weiteren Sinne unterschieden werden, um beide Bereiche voneinander trennen zu können.

Computerkriminalität im engeren Sinn beinhaltet alle Delikte, die sich gegen jede Form des ordnungsgemäßen Funktionierens einer elektronischen Datenverarbeitung richten. Als Beispiele sind hier die Computerspionage, -sabotage und die -manipulation zu nennen.

Computerkriminalität im weiteren Sinn beinhaltet alle Deliktbereiche, bei denen die elektronische Datenverarbeitung eine so gewichtige Bedeutung einnimmt, dass eine Begehung nur mittels des Computers möglich wird. Als Beispiel sind hier Urheberrechtsverstöße, Computerbetrugsfälle oder die Kinderpornographie zu nennen. Diese Definition könnte auch allen zukünftigen computertechnischen und deliktischen Neuerungen genügen. Im Folgenden werden deliktische Handlungen beschrieben und dargestellt, die Computerkriminalität im engeren und weiteren Sinne aufzeigen.

2.2 Entstehungsgeschichten des Computers und des Internets

Die Entwicklung der Computerkriminalität ist immer auch eine Entwicklung des Computers. Neue technische Erfindungen führen zu neuen Tatgelegenheiten. Der Begriff der Computerkriminalität beinhaltet den Begriff des Computers. Deshalb wird zunächst der Begriff des Computers definiert. Daneben ist die Geschichte des Computers von Bedeutung, da hiermit auch die Entwicklung der Computerkriminalität verstanden werden kann und sich somit auch

[83] Wobei dabei natürlich gesehen wird, dass das Urhebergesetz bis zu seiner jetzigen Fassung recht unklar mit solchen Verstößen umgegangen ist, so dass auch von einer Kriminalisierung bislang legitimer Handlungen gesprochen werden kann.

Vermutungen über deren weiteren Verlauf anstellen lassen. Die Computerkriminalität hat nicht allein durch die Digitalisierung ihre Bedeutung erlangt, sondern vor allem durch die Vernetzung der jeweiligen Systeme. Hierbei ist das Internet von besonderer Wichtigkeit und wird im Anschluss an die Entwicklung des Computers dargestellt. Diese Zukunftsprognosen sind wiederum dringend notwendig, um der Kriminalität schon im Entstehen zu begegnen. Daher möchte ich im Anschluss an die Definition des Computers dessen Geschichte darstellen.

Ein Computer[84] oder Rechner ist ein Apparat, der Informationen mit Hilfe einer programmierbaren Rechenvorschrift verarbeiten kann (Datenverarbeitungsanlage). Computer sind frei programmierbare Rechenmaschinen – d.h. die Eingabe, Verarbeitung und Ausgabe von Daten ist frei programmierbar.[85]

Da die Geschichte des Computers eine sehr umfangreiche Materie ist und die Entwicklung derart rasch voranschreitet, dass es nahezu unmöglich ist, sie vollständig darzustellen, beschränkt sich dieser Bereich lediglich auf die wichtigsten geschichtlichen Entwicklungen des Computers; auf einzelne Unternehmen und deren Produkte wird nur bedingt eingegangen.

Seine Entstehungsgeschichte kann dabei in fünf Generationen eingeteilt werden.[86] Die erste Rechenmaschine[87], die diesen Anforderungen genügte, entwarf Konrad Zuse im Jahre 1934. Als Zahlenformat nutzte er das für die Informatik am besten geeignete Dualzahlsystem. Seine Maschine konnte bereits boolsche Operationen wie UND, ODER und die NEGATION ausführen. Im Jahre 1941 entwickelte Zuse für die Deutsche Versuchsanstalt für Luftfahrt den

[84] lat. computare, dt. (zusammen-)rechnen

[85] http://www.net-lexikon.de/Computer.html (zuletzt abgerufen am 28.06.2004); aus diesem Grund soll auf eine Darstellung früherer Rechenapparate wie Rechenstäbe, Rechenschieber, Zahlentafeln und Lochkartenmaschienen verzichtet werden, auch wenn sie zur Entstehungsgeschichte des Computers beigetragen haben mögen.

[86] http://www.iwi.uni-sb.de/lehre/vorlesung/PDV/vorlesung/27102003/vorlesung27102003.pdf (zuletzt abgerufen am 28.06.2004).

[87] Es gibt unter Computer-Historikern keine einheitliche Meinung darüber, welcher Computer „der erste" gewesen ist. Der Hauptgrund liegt darin, dass der Begriff Computer für diese Gattung von Rechenmaschinen noch gar nicht verwendet wurde und aus heutiger Sicht diese Maschinen noch wenig mit den modernen Computern ab den 1950er-Jahren zu tun hatten. Erstmals wurde auf der „1st International Conference on the History of Computing" in Paderborn gemeinsam von etwa 70 Historikern aus allen Nationen, die an der Entwicklung der ersten Computer beteiligt waren, der Versuch unternommen, sich darauf zu verständigen, welche Merkmale eine Rechenmaschine haben musste, um „Computer" genannt zu werden. Es gab abschließend eine Abstimmung, bei der allerdings einige internationale Gäste bereits abgereist waren und die deutschen Teilnehmer überwogen. Als erster Computer wurde der Z3 gewählt. Unabhängig von dieser Abstimmung wird der Z3 seit Ende der 1990er-Jahre tatsächlich immer öfter als der erste Computer genannt, weil er einige herausragende Merkmale eines modernen Computers hatte, die andere Maschinen dieser Zeit nicht hatten. Der Z3 war „nur" der auf Relais basierende Nachbau des vollmechanischen Z1. Der Z1 war aber nicht praxistauglich, zeigte aber bereits die geniale Konzeption, die Konrad Zuse für seine Maschine entwickelte.

Z3. Dieser Computer besaß 64 Speicherplätze für Zahlen mit cirka sieben Dezimalstellen und brauchte für eine Multiplikation zweier solcher Zahlen immerhin nur 4-5 Sekunden. Die Programme wurden damals auf Lochstreifen gespeichert. Mit dem Bau von Z4 begann Zuse 1942 und stellte den Rechner im März 1945 fertig. Dieser mit einem mechanischen Speicher ausgestattete Rechner war noch bis Ende der 1950er-Jahre im Einsatz.
Mit dem ENIAC[88] entstand der erste Röhrenrechner[89] im Jahre 1946. Dieser war ursprünglich zur Berechnung von Raketenflugbahnen konstruiert worden und wies folgende technische Daten auf: Gewicht 30 Tonnen, Röhrenanzahl 18.000, Relaisanzahl 1.500, Stromverbrauch 140 kW, Kosten 3 Mio. Dollar, Taktfrequenz 3kHz. Der Bau des ENIAC leitete die Entwicklung der elektronischen Rechner und hierbei die erste Rechnergeneration (1946-1955) ein. [90]

Die zweite Rechnergeneration (1956-1965) war durch den Einsatz von Transistoren geprägt, die 1957 erfunden wurden. Weiterhin verbesserte man die Speicherfunktionen, wodurch schnellere Zugriffszeiten erreicht werden konnten.[91] Große Fortschritte gelangen auch in der Softwareentwicklung. Mit Algol, Cobol und Fortran kamen die ersten Programmiersprachen auf den Markt, und auch die ersten Betriebssysteme entstanden zu jener Zeit.[92] Weiterhin kamen zahlreiche neue Anwendungsgebiete wie Ingenieurs- und diverse Büroarbeiten zu den Aufgaben der Computer hinzu. Durch den verstärkten Einsatz in Unternehmen entstand das Berufsbild des Informatikers. Prägnant für diese Periode ist die Möglichkeit, größere Datenmengen verarbeiten und speichern zu können, die vor allem in Verwaltung und Kundenbereichen in Banken genutzt werden.[93]

Angesichts dieser Entwicklung wurde es notwendig, eine verstärkte Forschung auf dem Gebiet der Datensicherung vorzunehmen und auch die Gesetze den neu entstandenen Formen der

[88] (Electronic Numerial Integrator and Computer); Der ENIAC wurde in einer US-Wochenschau als „Elektronisches Gehirn“ vorgestellt, blieb aber dennoch von der Öffentlichkeit unbeachtet, da man damals den Bedarf an solchen Rechnern nur als sehr gering einschätzte. Die Maschine ist ein u-förmiger Zusammenbau von 40 Teilen, welche so gruppiert sind, dass sie 30 Einheiten formen. Jede dieser Einheiten leitet eine oder mehrere der Funktionen, die Voraussetzung für eine automatische Berechnungsmaschine sind. Die Einheiten, die sich hauptsächlich auf die Rechenoperationen beziehen, sind 20 Akkumulatoren (für Addition und Subtraktion), ein Multiplizierer und eine Kombination aus Division und Quadratwurzel.
[89] Statt wie bisher üblich mit Relais zu arbeiten, wurden beim Bau des ENIAC Elektronenröhren verwendet.
[90] Die Jahreszahlen sollen lediglich einen ungefähren zeitlichen Rahmen aufzeigen, spiegeln jedoch nicht ein exaktes Datum für einen Generationwechsel wider. Auch bezüglich der Anzahl der Generationswechsel gibt es unterschiedliche Auffassungen, so dass diese hier lediglich als Orientierungshilfe und eine ungefähre zeitliche Leitlinie dienen können; http://home.t-online.de/home/cyrill.cmk/eniac.htm (zuletzt abgerufen am 28.06.2004).
[91] http://privat.swol.de/SvenBandel/ (zuletzt abgerufen am 28.06.2004).
[92] http://www.bernd-leitenberger.de/programmiersprachen-geschichte.html (zuletzt abgerufen am 28.06.2004)
[93] Dennoch musste man sparsam mit dem vorhandenen Speicherplatz umgehen, was unter anderem zu einem bis zur Jahrtausendwende bestehenden Problem führte, nämlich der Speicherung des Datums. Man beschloss damals nur 6 Byte für das Datum zu reservieren und somit nur zwei Stellen der Jahreszahl festzuhalten.

Kriminalität anzupassen bzw. diesbezüglich neue Gesetze zu formulieren. Es wurde offenbar, dass mit dem Verlauf der technischen Entwicklung ein neues Rechtsgut entstanden war, welches durch die alten Gesetze keinen ausreichenden Schutz genoss. Unkörperliche Werte wie beispielsweise Wirtschaftsdaten und Urheberschutz sowie Informationen im Allgemeinen hatten stark an Bedeutung zugenommen.[94]

Eingeleitet wurde die dritte Rechnergeneration (1966-1970) durch die Entwicklung von integrierten Schaltkreisen, wobei die Firma IBM eine Vorreiterrolle einnahm. Man brachte damals 25 Transistoren und 40 Widerstände auf einem $1mm^2$ großen Chip unter. Dies zog sowohl einen Preisverfall nach sich wie auch eine Geschwindigkeitserhöhung der Speicherzugriffszeiten. Die Kosten für eine Transistorfunktion sanken von 1960 30 DM bis 1970 auf 0,30 DM herab.[95] Im Jahre 1971 stellte Intel den ersten Mikroprozessor mit einer Datenbreite von 4 Bit unter dem Namen 4004 vor. In einem solchen Zentralprozessor oder auch CPU (Central Processing Unit) befinden sich sowohl das Steuerwerk als auch das Rechenwerk. Die Verbindung aus Hauptspeicher und Zentralprozessor stellt die Zentraleinheit eines Rechners dar.[96] Die Computer lernten erstmals miteinander zu kommunizieren, da nun ganze Rechnernetze aufgebaut wurden.[97] Die Rechnernetze und höhere Leistungsfähigkeit brachten allerdings auch große Probleme bei der Softwareentwicklung mit sich, so dass neue Entwicklungskonzepte und neue bis heute aktuelle Programmiersprachen (Pascal, Prolog, Smalltalk, C) entstanden. Durch den verstärkten Bau von Echtzeitrechnern kamen auch Echtzeitbetriebssysteme auf den Markt. [98]

Die Entwicklung hochintegrierter Schaltkreise ermöglichte in der vierten Computergeneration (1971-1979) den Bau von Mikrorechnern.[99] Der erste in Deutschland zu erwerbende Rechner dieser Art war der PET 2001 der Firma Commodore.[100] Aber nicht nur die Integrationsdichte ist wichtig für die Entwicklung immer kleinerer Rechner, auch der Stromverbrauch spielt

---

[94] Sieber, 1996 S.643.

[95] http://wwwstud.fh-zwickau.de/~alma/sven/skripte/grundlagen/1_3.htm (zuletzt abgerufen am 28.06.2004); http://www.th.schule.de/th/lfk-informatik/ideen/arnoldi/moeg_gre.htm (zuletzt abgerufen am 28.06.2004).

[96] http://www.intel.com/corporate/education/emea/deu/sections/section6/mpuworks/ (zuletzt abgerufen am 28.06.2004).

[97] Das wohl bis heute bekannteste konstruierte 1969 das amerikanische Verteidigungsministerium unter dem Namen ARPANET (Advanced Research Projects Agency NET). Mit der Veröffentlichung dieses Netzes 1972 avancierte es zu dem heute bekannten Internet, an welches sich zunächst Universitäten und Forschungseinrichtungen anschlossen.

[98] http://irb.cs.tu-berlin.de/~zuse/history/Programmiersprachen.html (zuletzt abgerufen am 28.06.2004).

[99] http://www-ti.informatik.uni-tuebingen.de/~schroedm/proseminar/PDFs/geschichte_des_computers.pdf (zuletzt abgerufen am 28.06.2004).

[100] http://members.aol.com/CompHist/cbmhistory.html (zuletzt abgerufen am 28.06.2004).

diesbezüglich eine große Rolle. Deshalb war die Erfindung der MOS-FET-Transistoren[101] ein wichtiger Schritt für die Weiterentwicklung der Elektronik. Mitte der siebziger Jahre entwickelte sich eine Technik, Computer über Modems oder mit Hilfe des Telefonnetzes fern zu steuern. Damit verbunden war auch eine neue Art der Kriminalität. Diese Neuerung in der Computerkriminalität, das Begehen einer Straftat ohne physische Anwesenheit eines Täters, machte den entscheidenden Unterschied zu der „traditionellen Kriminalität" aus. Man begann daraufhin erstmals, dieses Phänomen wissenschaftlich zu untersuchen. Dabei stellte sich jedoch heraus, dass die reelle Zahl gemeldeter Straftaten mit Computerbezug sehr gering war. Dies ist eine Tatsache, die schon damals zu der Vermutung veranlasste, dass die Statistiken für diese Form der Kriminalität keine starke Aussagekraft haben, da viele Fälle der Polizei wahrscheinlich aus verschiedenen Gründen nicht gemeldet, beziehungsweise gar nicht entdeckt wurden.[102]

Von dem Zeitraum ab 1980 kann von der fünften Computergeneration gesprochen werden. Mehrere Prozessoren wurden in Transputer (= Transistor + Computer) auf einem Chip – integrierter Schaltkreis – verbunden. Die Prozessoren arbeiten bei Rechenoperationen gemeinsam und teilen sich somit die Arbeit, wodurch die Rechengeschwindigkeit drastisch gesteigert werden konnte.[103] Im Bereich der Software kamen erstmalig grafische Benutzeroberflächen und interaktive Systeme auf. Dies ermöglichte eine anwenderfreundliche Gestaltung und eröffnete so auch für Nicht-Computerexperten neue Möglichkeiten, wie zum Beispiel Textverarbeitung und elektronische Datenverwaltung. Der wohl am weitesten verbreitete Heimcomputer der 1980er-Jahre kam von der Firma Commodore und trug den Namen C64.[104] Den ersten Personalcomputer stellte die Firma IBM 1981 her.[105] IBM bringt mit dem PS/2 eine neue Rechnerarchitektur und mit OS/2 ein neues Betriebssystem. 1985 entstand durch Bjarne Stroustrup die bis heute bekannteste objektorientierte Sprache C++.

In den achtziger Jahren setzte mit der Entwicklung verschiedenster Programmiersprachen erneut eine Verstärkung des öffentlichen Interesses an dem Thema Computerkriminalität ein, da in dieser Zeit eine rasche Entwicklung auf diesem Gebiet stattfand. Erstmals wurden Berichte über Computerviren, Hacking und Kreditkartenmissbrauch veröffentlicht. Zum Beispiel

[101] Metal Oxide Semiconductor Field Effect Transistor - auch als Feldeffekttransistor bekannt. Im Gegensatz zu Bipolartransistoren wird bei FETs stromlos geschaltet.
[102] Sieber 1999, S.18 ff.
[103] http://www.iwi.uni-sb.de/lehre/vorlesung/PDV/vorlesung/27102003/vorlesung27102003.pdf (zuletzt abgerufen am 28.06.2004).
[104] http://www.adp-gmbh.ch/personal/histoire/histoire.html (zuletzt abgerufen am 28.06.2004).
[105] http://www.hardwaregrundlagen.de/oben10.htm (zuletzt abgerufen am 28.06.2004).

fand 1980 das wahrscheinlich erste bekannt gewordene Hacking statt, bei dem Kevin Mitnick mit der Roscoe-Bande in das Computersystem der Firma US-Leasing eindrang.[106] Das erste illegale Virus wurde 1986 programmiert. Es war das Virus „Pakistani Brain", das den Bootsektor des Computers befiel. Hiermit wurde erstmals die Möglichkeit genutzt, diese Art der Programmierung zu Sabotagezwecken einzusetzen. Verschiedene Arten von Virenvorgängern waren seit Beginn der siebziger Jahre programmiert worden. Das erste sich selbst reproduzierende Virus wurde jedoch 1983 von Fred Cohen im Rahmen seiner sehr umstrittenen Doktorarbeit veröffentlicht.[107]

1990 wird Windows 3.0 zum großen Erfolg. Das Ende der zu diesem Zeitpunkt sehr erfolgreichen und gegenüber handelsüblichen PCs leistungsfähigeren Heimcomputer Atari ST und Commodore Amiga bahnt sich an.[108] In dieser bis heute andauernden Rechnergeneration gelang es, immer mehr Transistoren auf einen Prozessor zu integrieren. Die Speicherzugriffszeiten sind dank SD-RAM gesunken und die Kapazität der RAM-Module stieg zugleich stark an. Der Telekommunikations- und Informationstechnikmarkt erlebte einen Umsatzboom, vor allem der Personalcomputer fand regen Absatz. Dies liegt neben der stetigen Leistungssteigerung der Rechner auch an der einfachen Handhabung und den zahlreichen Anwendungsmöglichkeiten. Diese zunehmende Miniaturisierung der Chipstrukturen hält bis heute an. Man hat zwar jeder neuen „Generation", die kleiner war als die vorhergehende, eine neue Bezeichnung gegeben, aber das Prinzip hat sich seit den 1980er-Jahren nicht geändert. Inzwischen sind die Chipstrukturen kleiner als 0,13¹m, und es gibt in der Theorie bereits Verfahren, diese noch weiter zu verkleinern.[109] Der Computer dient aufgrund seiner heute ausreichenden Speicherkapazitäten und CPU-Leistungen als Grundvoraussetzung für die immer stärker in den Vordergrund getretene Softwareherstellung.[110] Ende des 20. Jahrhunderts beginnt mit dem Internet abermals eine technische Revolution, die dem Computer und der Computerkriminalität ganz neue Erscheinungsformen ermöglicht.[111]

[106] http://www.osoc.de/sicherheit/ubcokrim.htm (zuletzt abgerufen am 29.06.2004).
[107] http://www.computerviren-info.de/Geschichte.htm (zuletzt abgerufen am 30.03.2004); http://www.etymologie.info/~e/_n/in-plan18.html (zuletzt abgerufen am 30.03.2004).
[108] http://www.weller.to/his/h13-85-90-leistungsfaehige-homecomputer.htm (zuletzt abgerufen am 29.06.2004).
[109] http://www.computergeschichte.net/geschichte_des_computers_12.html (zuletzt abgerufen am 28.06.2004).
[110] Die Software ist als zunehmend zukunftsweisender Faktor zu werten. Auf die Entwicklung und den heutigen Stand der Software möchte ich verzichten, da dies den Rahmen der Arbeit sprengen würde. Daher wird an dieser Stelle auf eine weiterführende Darstellung des Computers verzichtet. Diese müsste sich in rein technischer Form gestalten und es wären allenfalls CPU-Geschwindigkeiten und Speichereigenschaften darzustellen.
[111] http://www.weller.to/ (zuletzt abgerufen am 29.06.2004).

Trotz seiner jungen Erfolgsgeschichte lassen sich die Anfänge des Internet bis in die Zeit des Kalten Krieges zurückverfolgen. 1957 beschlossen die USA, mehr Informationen über die Erdoberfläche zu sammeln. Zu diesem Zweck beabsichtigte man, einen Satelliten in die Erdumlaufbahn zu bringen. Doch die UdSSR kam diesen Plänen zuvor und sandte im selben Jahr ihren Sputnik 1 ins Weltall. Der augenfällige technologische Fortschritt der UdSSR versetzte den USA einen ernüchternden Schock. Sie reagierten unverzüglich mit der Gründung der Advanced Research Projects Agency (ARPA)[112], um den Rückstand aufzuholen. Aufgabe dieser Institution war es, die technischen Voraussetzungen zu schaffen, damit die USA die führende Rolle in Wissenschaft und Technologie zurück gewinnen und das Militär die Erkenntnisse der Wissenschaftler für ihre Interessen verwenden konnte.[113]

Eine neuartige Netzwerktopologie schlug Paul Baran (1964) von der RAND Corporation vor. Baran versuchte, der Sorge der US Air Force um die Überlebensfähigkeit ihrer Kommandostruktur im Fall eines sowjetischen Nuklearangriffs Rechnung zu tragen. Anstelle des konventionellen Sterns sah Baran ein „distributed network“ vor, bei dem spinnwebförmig eine Vielzahl von Verbindungen zwischen den in das Netzwerk eingebundenen Rechnern vorgesehen war.[114] Durch den Wegfall eines Zentralrechners sollte das Datenaufkommen im Netzwerk gleichmäßig auf die einzelnen Leitungen aufgeteilt werden. Da viele Leitungen redundant sind, gibt es in einem verteilten Netzwerk stets mehrere Wege von einem Start- zu einem Zielrechner. Ein Totalausfall des Netzes kann deshalb erst auftreten, wenn jeder einzelne mögliche Pfad ausfällt. Damit ist eine höhere Zuverlässigkeit als etwa bei einem Telefonnetz mit festen Leitungsverbindungen möglich.[115]
Ein weiterer Punkt in Barans Idee ist das „Parcel-Switching-System“. Auf Grundlage dieser Idee entwickelten die Forscher der ARPA eine Software, die die Daten in viele kleine Pakete

[112] Die ARPA hatte ihren Sitz im Verteidigungsministerium, und mit ihr stellte man Forschung und Technologie in den Dienst der Landesverteidigung, denn in Zukunft wollte man gegen den Vormarsch des 'Feindes' in Wissenschaft und Technik gewappnet sein. Die ARPA arbeitete mit einem ansehnlichen Budget und beschäftigte rund 200 Forscher, die auf verschiedene wissenschaftliche Richtungen verteilt waren. In der computerwissenschaftlichen Abteilung der ARPA setzte man sich mit der Datenübermittlung im Fall eines nuklearen Krieges auseinander: Es galt, die elektronischen Kommunikationswege gegen die Folgen eines atomaren Schlags zu sichern. Weiter Informationen unter http://www.arpa.mil/ .
[113] http://mitglied.lycos.de/rapidwien/intges1.htm (zuletzt abgerufen am 29.06.2004).
[114] Bis dahin bestanden die Kommunikationsnetzwerke aus aneinander gekettete Knoten, und jeder Knoten im Netzwerk hing von der systemsteuernden Zentrale ab. Wurde nun die Zentrale zerstört, so war das gesamte Netzwerk unbrauchbar. Um im Fall einer Zerstörung den Datenfluss zwischen den vernetzten Computern gewährleisten zu können, musste ein Netzwerk ohne Zentrale, in dem alle Netzwerkknoten gleichberechtigt waren, geschaffen werden.
[115] http://www.psychologie.uni-bonn.de/sozial/staff/musch/history.htm#1 (zuletzt abgerufen am 29.06.2004).

aufteilt (Protokoll).[116] Jeder Datenblock wird nummeriert, mit Absender und Empfangsadresse versehen und dann auf den Weg von einem Computer zum anderen geschickt. Stößt nun eines dieser Pakete auf ein Hindernis im Netzwerk, zum Beispiel auf eine zerstörte Leitung, endet der Weg des Pakets nicht wie früher an diesem Punkt, sondern es erfolgt sofort eine Rückmeldung an den aussendenden Computer. Dieser verschickt die Pakete automatisch über einen anderen Weg, also über einen oder mehrere andere der vernetzten Computer. So erreichen die Botschaften auch ihr Ziel, wenn große Teile des Netzwerks ausgefallen sind.[117] Damit war der Grundstein für die Entwicklung des ARPANET gelegt. Als Ziel des ARPANET-Projekts wurde die Errichtung eines zuverlässigen, störungsresistenten Netzes auf der Basis der neuen Pakettechnik, die gemeinsame Nutzung vorhandener Hardware-Ressourcen und die Möglichkeit des Datenaustauschs zwischen Rechnern unterschiedlicher Hersteller benannt. Anders als bei früheren Anläufen bestand bei der Entwicklung des ARPANET von Anfang an die Absicht, in das entstehende Netz vollkommen heterogene Hardwareplattformen zu integrieren.[118]

1969 gelang es den Forschern der UCLA schließlich, die erste Version eines funktionstüchtigen Netzwerks zu entwickeln. Es verband vier Rechner der „University of California at Los Angeles“, des „Stanford Research Institutes“, der „UCSB“ und der „University of Utah“.[119] Zeitgleich wurde der erste „Request for Comment“ (RFC) veröffentlicht.[120] In den 1970er-Jahren wurden auch die ersten Dienste für das ARPANET entwickelt. Im Jahr 1971 wurde von Ray Tomlinson das erste E-Mail-Programm entwickelt, das auf einem Rechner mit internem Mailprogramm und einer experimentellen FTP-Version basierte. Erst sechs Jahre später wurde E-Mail erstmals spezifiziert. Im RFC 733 wurde daraufhin die genaue Spezifikation

[116] Viele Skeptiker zweifelten zunächst am Sinn des „parcel-switching“. Der nicht unerhebliche zusätzliche Aufwand, alle einzelnen Pakete mit dem Zielort zu beschriften und an jedem Knotenpunkt im Netzwerk neu zu bestimmen, wohin ein Paket am besten weitergeleitet wird, schien das System unnötig komplex und störanfällig zu machen. Fraglich schien weiter, ob die Speicherkapazität der Zielrechner immer ausreichen würde, um die einzelnen Teile mehrerer Nachrichten bis zum Eintreffen des letzten Pakets aufzunehmen. Besonders Telefontechniker bezweifelten, dass das Eintreffen jedes einzelnen Pakets auf dem Zielrechner gewährleistet werden könne, wenn der gewählte Weg für jedes Paket neu bestimmt wird.
[117] Zehnder 1998, S. 30.
[118] http://www.psychologie.uni-bonn.de/sozial/staff/musch/history.htm#1 (zuletzt abgerufen am 29.06.2004).
[119] http://www.informatik.uni-bremen.de/grp/unitel/referat/timeline/timeline-2.html (zuletzt abgerufen am 30.06.2004).
[120] Ein junger Student, der am Projekt mitarbeitete, Steve Crocker, hatte erkannt, dass viele der Mitarbeiter noch Studenten waren und eine übergeordnete Autorität fehlte. So musste er einen Weg finden, um den Fortgang der Arbeiten zu dokumentieren, und schrieb den ersten „Request for Comment“. Das Ziel der RFC ist es, eine bestimmte Position oder einen Vorschlag öffentlich zur Diskussion zu bringen, damit ihn andere Personen kommentieren konnten. Der erste Request for Comment wurde am 7. April 1969 mit dem Titel „Host Software“ veröffentlicht.

festgehalten.[121] Ein Jahr nach dem ersten E-Mail-Programm wurde Telnet im RFC 318 spezifiziert. Wiederum ein Jahr später gab es dann die Spezifikation des „File Transfer Protocol“ im RFC 454. Ungefähr zur selben Zeit wurde der RFC 741 geschrieben, in dem die Spezifikation des „Network Voice Protocol“ stand.[122]
Auf der Basis dieser Dienste und dem Versuch des ARPANET wurde 1974 Telnet frei gegeben, eine kommerzielle Version des ARPANET.[123] Es ist das erste kommerzielle, paketorientierte Netz, das jedoch außer für Forscher und Private mit ausgezeichneten Computerkenntnissen von geringem Interesse war. Dies ist verständlich, denn zur Nutzung des ARPANET musste man die dazu unentbehrliche, komplizierte Computersprache beherrschen. Außerdem benötigten Anwender der neuen Technologie zur damaligen Zeit einen Rechner von der Größe eines ganzen Zimmers. Allein die Kostenfrage machte das ARPANET für die meisten Menschen unerreichbar und deshalb war die spektakuläre Erfindung kaum populär. Unter Forschern jedoch war das ARPANET ein großer Erfolg und interessierte Wissenschaftler aus der ganzen Welt halfen, die Entwicklung des Internets voranzutreiben.[124]

Die dezentrale Struktur des Netzes machte eine Erweiterung sehr einfach. Solange neu hinzukommende Maschinen nur die paketorientierte „Sprache“ dieses neuen Netzwerks beherrschten, war es gleichgültig, wem sie gehörten, welchen Inhalt sie hatten, oder wie ihr Name war.
Die Forschergruppe musste sich jedoch in der Folge auf ein weiteres Problem des ARPANET konzentrieren. Da die rund 30 amerikanischen Universitäten, die sich im Lauf der 1970er-Jahre vernetzten, über verschiedene Rechnertypen und Betriebssysteme verfügten, wurde sehr viel Zeit darauf verwendet, ihre Protokolle aufeinander abzustimmen. Die ursprünglich entwickelte „Sprache“, das Protokoll, mit dem sich zwei Nachbarknoten unterhalten, wurde NCP genannt, „Network Control Protocol“. Doch bereits 1972 hatte sich die INTER-Network Working Group formiert, um auf der Grundlage von NCP ein gemeinsames Protokoll zu erstellen, das die Datenübertragung zwischen unterschiedlichsten Hardware-Plattformen und vor allem zwischen autonomen Netzen ermöglichen sollte. Es entstand ein Standard, der unter dem Namen „Transmission Control Protocol/Internet Protocol“ (TCP/IP) bekannt wurde. TCP beschreibt, wie Nachrichten in Pakete zerlegt und am Ziel wieder zur Originalnachricht zusammengesetzt werden können. IP wird benötigt, um die Pakete so zu adressieren, dass sie

[121] Kevin MacKenzie kam später auf die Idee, Emotionen im Text auszudrücken. Hierzu erfand er die ersten Smilies :-).
[122] http://www.informatik.uni-bremen.de/grp/unitel/referat/timeline/timeline-2.html (zuletzt abgerufen am 30.06.2004).
[123] http://mitglied.lycos.de/rapidwien/intges3.htm (zuletzt abgerufen am 30.06.2004).
[124] http://www.informatik.uni-bremen.de/grp/unitel/referat/timeline/timeline-2.html (zuletzt abgerufen am 30.06.2004).

über diverse Knoten oder auch Netzwerke mit unterschiedlichen Übertragungsstandards (also nicht nur ARPA's NCP, sondern auch andere, wie z.B.: Ethernet, X.25,...) ihren Weg zum Empfänger finden.[125] Das zweigleisige Protokoll TCP/IP erwies sich als so erfolgreich, dass 1982 alle Systeme des ARPANET von NCP auf TCP/IP umstellten.

1987 erlitten das ARPANET und seine Gründer den ersten Rückschlag. Der Virus „Christmas Tree" infizierte in wenigen Sekunden das gesamte Netz und legte es lahm. Außerdem brach auch das weltweite IBM-Netzwerk zusammen.[126] Zwei Jahre später wurde der berühmte KGB-Hack aufgeklärt. KGB-Hack ist die Bezeichnung für eine Reihe von Einbrüchen in westliche Computersysteme zwischen 1985 und 1989. Die Hacker drangen in die Rechenzentren großer Institutionen und Militäreinrichtungen in den USA ein, stahlen dort Daten und verkauften sie an den sowjetischen Geheimdienst KGB. Es waren die Taten einer Hackergruppe um Karl Koch[127] und Markus Hess in Hannover. [128]

Trotz des zeitweiligen Ausfalls des ARPANETS ist mit der Umstellung von NCP auf TCP/IP das moderne Internet geboren, denn nun war es möglich, auch kleinere Netzwerke an das Internet anzuschließen. 1990 wurde das ARPANET aufgelöst.[129] Anfang der 1990er-Jahre bestand somit bereits eine globale Vernetzung, das Internet, doch war sie nicht so einfach benutzbar, wie man dies heute gewohnt ist. Der Gebrauch war viel umständlicher, es gab zwar Dienste auf dem Internet wie Terminal Emulation (Telnet), File Transfer (FTP), Usenet (Newsgroups), Wide Area Information Server (WAIS), Informationssystem für Textdaten (Gopher) oder Elektronic Mail (E-Mail), jedoch keine einfachen, benutzerfreundlichen Oberflächen. Der breiten Masse war das Internet somit verschlossen.

Mit der Möglichkeit der Vernetzung unterschiedlichster Netzwerke entstand auch die Möglichkeit, von jedem Rechner aus in andere miteinander vernetzte Systeme einzudringen. Schon im Jahr 1989 drangen Hacker in Computer ein, die das USAF-Satellite-Positon der

[125] http://home.t-online.de/home/horibo/history.htm#Einleitung (zuletzt abgerufen am 30.06.2004).
[126] http://kbs.cs.tu-berlin.de/teaching/sose2004/sirs/vortraege/b3-viren-entwicklung.pdf (zuletzt abgerufen am 30.08.2004).
[127] Karl Koch stirbt am 23. Mai 1989, gerade einmal 23 Jahre alt. Die Todesumstände sind bis heute ungeklärt. Ob es nun Mord oder Selbstmord war, eins zumindest steht fest, die „23" gilt in den Illuminatengeschichten als magische Zahl und Todesdatum „aller großen Anarchisten". Die Lektüre des dreibändigen Werks „Illuminatus" prägte das Leben des jungen Mannes sehr stark. Im Alter von 14 Jahren schenkte ihm sein Vater die Trilogie, nach deren Hauptfigur er sich schließlich nannte. Karl Koch nimmt die Bücher wörtlich und glaubte an eine weltweite politische Verschwörung.
[128] http://de.wikipedia.org/wiki/KGB-Hack (zuletzt abgerufen am 30.08.2004).
[129] http://www.michaelkaul.de/Geschichte/zakon/zakon.html (zuletzt abgerufen am 30.06.2004).

USA steuerten.[130] Im selben Jahr hackten zwei Schweizer die Computer des Bundesamts für Gesundheit.[131] Im folgenden Jahr hackten niederländische Hacker die Computersysteme des amerikanischen Unternehmens DOD Computer Systems.[132]

Im Jahre 1989/90 entwickelte Tim Berners-Lee am CERN-Institut in der Schweiz das auf Hypertext basierende World Wide Web (WWW), um die Fülle von Informationen im Internet besser nutzen zu können.[133] Durch den Hypertext konnte man den Benutzer von einem Dokument zum nächsten weiterleiten, ohne dass irgendwelche schwer verständlichen Kommandos eingegeben werden mussten. Dabei konnten die Dokumente auch auf weit entfernten Servern liegen. Man benötigte lediglich einen „Browser" als Hilfprogamm, um die angeforderten Informationen darzustellen.[134] Mit dem WWW lassen sich Dokumente, die in der Sprache HTML geschrieben sind, ebenso verbreiten wie Bilder, Videos und Musik. Um diese Seiten betrachten zu können, müssen sie nicht erst auf den eigenen Rechner geladen und dazu explizit abgespeichert werden (wenn man das Browser-Cache außer Acht lässt), um erst dann die Dateien in einem entsprechenden Programm ansehen zu können. Das WWW bietet die Möglichkeit der Onlinebetrachtung, die auch die Voraussetzung für das Surfen darstellt, das fortlaufende Verfolgen von Links, die auf Dokumente verweisen, die sich auf einem WWW-Server irgendwo im Internet befinden.

Die vielleicht wichtigste Voraussetzung für die ab etwa 1993 einsetzende explosionsartige Ausweitung des WWW war die Freigabe der WWW-Technologie durch das CERN im April 1993: Jedermann konnte die Technologie benutzen, ohne irgendwelche Patentrechte erwerben oder Copyrightgebühren entrichten zu müssen. Das WWW war so vollständig der Öffentlichkeit zugänglich gemacht worden, der Boom des Web war nicht mehr zu bremsen: Während 1993 weltweit 50 HTTP-Server existierten, waren es Ende 1994 schon 100.000. Und 1995 war WWW der führende Dienst im Internet: Der Umfang der Datentransfers des WWW hatte denjenigen von FTP überflügelt. Neben Universitäten bauten auch immer mehr Unternehmen einen Webserver auf, Schwerpunkt war die Computerbranche. Heute hat wohl jedes größere

[130] http://www.sinisterhand.com/files/12 (zuletzt abgerufen am 30.08.2004).
[131] Hartmann 2001, S. 48.
[132] http://www.net-security.org/article.php?id=30 (zuletzt abgerufen am 30.08.2004).
[133] Häufig werden Internet und das World Wide Web – WWW – in ein und denselben Topf geworfen, es bestehen aber gravierende Unterschiede: Das Internet stellt das physische Netzwerk dar, es ist der greifbare Teil der globalen Vernetzung, bestehend aus Rechnern und Verbindungen zwischen diesen einzelnen Maschinen, seien es nun Kabel oder irgendwelche Funkverbindungen, z.B. Satellitenverbindungen. Das WWW hingegen ist kein Netzwerk im Sinn des Internets, es ist ein virtuelles Netzwerk, es ist lediglich ein Dienst, der das Internet benutzt, ein Dienst wie beispielsweise FTP oder E-Mail.
[134] http://spot.fho-emden.de/alge/museum/index.htm (zuletzt abgerufen am 30.06.2004).

Unternehmen eigene Webseiten, und das Internet ist aus der „Informationsgesellschaft“ nicht mehr wegzudenken.

Durch die Entwicklung des Computers und des Internets entstand auch eine neue Kriminalitätsform. Im Jahr 1989 wurde Kevin Minick verhaftet. Nach ihm wurde Anfang der 1990-er Jahre wegen mehrerer Einbrüche in Computersysteme des Militärs und großer US-Konzerne als „meist gesuchter Krimineller der USA“ gefahndet.[135] Er drang in die Computersysteme der Unternehmen Motorola, Sun Microsystems, Nokia, Fujitsu und NEC ein und spionierte unter anderem über zwanzigtausend Kreditkartennummern aus. Er wurde zu fünf Jahren Haft verurteilt. Um einen "Rückfall" zu vermeiden, wurde zur Auflage gemacht, dass er zudem drei Jahre lang keinen Computer benutzen durfte.[136]

Im Jahr 1996 durchstöberte ein 18-jähriger israelischer Hacker zwei Wochen lang die Computer der US-Armee. Im selben Jahr knackte ein Student aus Bremerhaven die Zugangscodes eines Unternehmens in Miami und stahl elftausend Kundendaten. Für die Rückgabe forderte er fünfzigtausend D-Mark.[137] Ein Jahr darauf durchsuchte ein 15-jähriger Hacker aus Kroatien die Computer der U.S. Air Force.[138]

1998 entschlüsselte der Chaos Computer Club den Identifikationscode von Mobilfunk-Karten des Unternehmens D2 Mannesmann. Zudem entschlüsselte ein 18-jähriger Schüler aus Hannover die Sicherheitscodes des Pagerdienstes Scall der Deutschen Telekom. Er zog einen vierstelligen Betrag von einer Scall-Nummer ab und konnte alle Nachrichten des jeweiligen Besitzers verfolgen und die Daten ändern. Im selben Jahr verschafften sich die beiden 16-jährigen Kölner Marcel Henning und Aaron Spohr mehr als sechshundert Passwörter von T-Online-Teilnehmern. Als dies bekannt wurde, verschärfte der Online-Dienst die Sicherheitsvorkehrungen. Zwei Wochen später drangen die beiden Hacker wieder ein.[139]

1999 brachte die texanische Hackervereinigung Cult of the dead cow (Kult der toten Kühe) Back Orifice in Umlauf. Das Programm läuft unsichtbar im Hintergrund unter Windows 95 und 98 und ermöglicht die Kontrolle fremder Rechner. Während der Hackerkonferenz Def-

[135] http://www.userchannel.de/wissen/docs/KevinMitnick (zuletzt abgerufen am 30.08.2004).
[136] http://it-academy.cc/content/glossary_browse.php?ID=1023 (zuletzt abgerufen am 30.08.2004).
[137] Hartmann 2001, S. 49.
[138] http://edition.cnn.com/TECH/specials/hackers/cyberterror/ (zuletzt abgerufen am 30.08.2004).
[139] Hartmann 2001, S. 49.

Con zeigten sich auch Geheimdienstler an dem Hacker-Programm interessiert.[140] Zudem wurde im selben Jahr die CSS-Verschlüsselung der DVD-Filme von Hackern geknackt, die entscheidend für künftige Filmpiraterie war.[141]

Im Oktober 2000 wurden die Server von Microsoft mit dem „QAZ-Trojaner" von Hackern aus St. Petersburg angegriffen, die sodann in das Computer-Netzwerk von Microsoft eindrangen und den Quellcode der aktuellen Versionen von Windows 2000, NT 4.0 und Office 2000 stahlen. Quellcodes (source codes) sind Programmanweisungen, die in einer höheren Programmiersprache oder in Assembler geschrieben sind, und vom Menschen gelesen, aber nicht direkt von einem Computer verarbeitet werden können, sozusagen der Klar-Text des Betriebssystems.[142] Wird ein Quellcode offen gelegt, bedeutet dies einen hohen finanziellen Schaden und kann ein Softwareunternehmen in den Ruin führen.

Im Jahr 2001 starteten Hacker unter Ausnutzung der Schwachstellen im Microsoft-IIS-Server eine Denial-of-Service-Attacke gegen das Weiße Haus.[143] Unbekannten Hackern gelang es, die Webseite des Weißen Hauses für mehrere Stunden ganz oder teilweise lahmzulegen.[144] Im April desselben Jahres wurde auch der Berliner Internet-Hoster Strato AG Opfer eines Denial-of-Service-Angriffs.[145]

Im Februar des Jahres 2003 verschafften sich Hacker in den USA einen Zugang über das Internet zu mehr als fünf Millionen Kreditkarten-Konten von Visa und MasterCard. Die Täter gelangten an die sensiblen Daten über ein Drittunternehmen, das in Nordamerika Kreditkartenabrechnungen bearbeitet. Visa erklärte, den Hackern seien die Daten von 3,4 Millionen Kartenkonten in die Hände gefallen. Bei MasterCard sprach man von mehr als zwei Millionen Kartendaten. Im September desselben Jahres verhaftete die Tokioter Polizei zwei Männer, die sich per Hacking von Online-Bankkonten umgerechnet 136.000 Dollar ergaunert hatten. Die beiden Männer stahlen Geld von verschiedenen Konten, während sie in einem Internet-Café in Tokio saßen.[146] Mit dem Start der Fußball-EM 2004 sind zahlreiche Wettangebote im Internet von Denial-of-Service-Attacken manipuliert worden. Hintergrund der Attacken waren

[140] Hartmann 2001, S. 50.
[141] Medosch/Röttgers 2001 S. 26.
[142] http://www.giza-web.de/html/programm-code-microsoft.html (zuletzt abgerufen am 30.08.2004); http://www.heise.de/newsticker/meldung/12802 (zuletzt abgerufen am 30.08.2004);
[143] http://www.spiegel.de/netzwelt/technologie/0,1518,146105,00.html (zuletzt abgerufen am 30.08.2004).
[144] http://www.tecchannel.de/news/20010506/thema20010506-4321.html (zuletzt abgerufen am 30.08.2004).
[145] http://www.hausbau-anleitung.de/index.php3?action=Internet-News&link=news/news752&jahr=2001 (zuletzt abgerufen am 30.08.2004).
[146] http://www.computer-security.ch/ids/default.asp?TopicID=78&Page=3 (zuletzt abgerufen am 30.08.2004).

Schutzgeldforderungen, denen die Seitenbetreiber nicht nachkamen. Angeblich soll es sich um Forderungen zwischen 15.000 und 30.000 Euro gehandelt haben.[147] Neben DoS-Angriffen und Meldungen über unsicheres Online-Homebanking scheint im Jahr 2004 vor allem eine neue Generation von Hackerangriffen zu starten. Dies hängt mit der Computerisierung neuer Hardwareendgeräte zusammen. Nicht nur PCs, sondern auch Mobiltelefone und Organizer bieten unzureichenden Schutz gegen Hacker-Angriffe. Alles wird mit allem vernetzt. Computer mit dem Handy, das Handy mit der Alarmanlage.[148] Erste Handydialer erscheinen und machen auch reine Handynutzer zu möglichen Opfern.[149] Bestimmte Handy-Modelle können von einem Angreifer dabei ferngesteuert werden. Er kann persönliche Daten auslesen, SMS über das Handy verschicken, 0190er-Nummern anrufen und theoretisch sogar Gespräche auf sein Notebook oder seinen PDA umleiten.[150] Das Handy hat sich mittlerweile zu einem Multifunktionsgerät gewandelt.[151]

Die folgende Graphik einer Studie der efacts/forsa zeigt den rasanten Anstieg der privaten Nutzung des Internets allein in Deutschland.[152] Hiernach nutzen im Jahr 2004 schon über 55 Prozent der Deutschen das Internet. Vier Jahre zuvor waren es noch knappe 13 Prozent. Dies zeigt den Bedeutungswandel des Internets allein in den letzten Jahren.

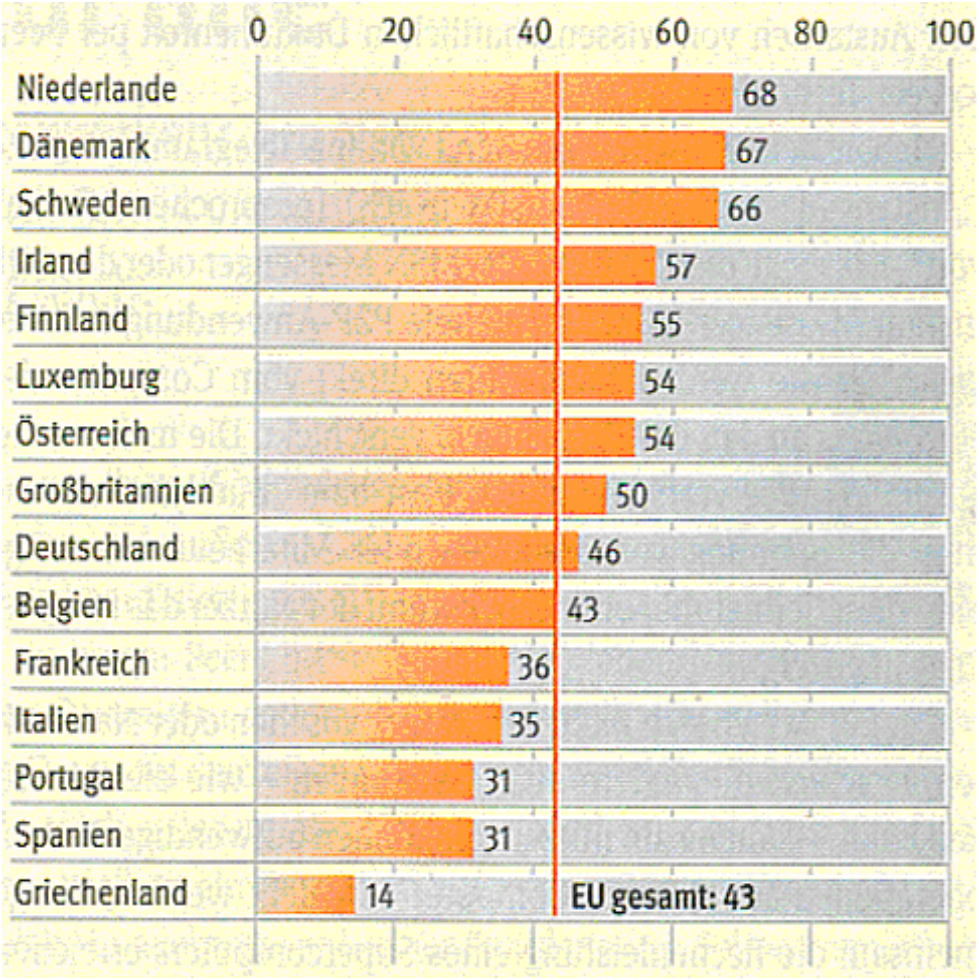
[147] http://www.chip.de/news/c_news_12048957.html (zuletzt abgerufen am 30.08.2004).
[148] Opaschowski 2001, S.11.
[149] http://www.chip.de/news/c_news_11881374.html (zuletzt abgerufen am 30.08.2004).
[150] http://www.xonio.com/features/feature_unterseite_11876679.html (zuletzt abgerufen am 30.08.2004).
[151] Das Bezahlen per Handy, im Fachjargon „Mobile Payment“ genannt, wird sich nach einer Expertenstudie im Jahre 2004 des Verbandes der deutschen Internetwirtschaft, ECO Forum e.V. vor allem auf Reisen und am Automaten durchsetzen. Es ist somit nur eine Frage der Zeit, bis unzählige neue Hackerangriffe die Runde machen.
[152] http://www.atfacts.de/001/pdf_studies/atfacts_q1_2004.pdf (zuletzt abgerufen am 30.08.2004).

Quelle: efact/forsa

Nach einer Studie der TechConsult GmbH ist der deutsche Mittelstand im Jahre 2004 nahezu komplett „online“. Lediglich ein Prozent der Mittelstandsunternehmen verweilen noch auf der untersten Stufe der E-Business-Skala und nutzen somit weder Internet noch E-Mail („offline“).[153]

[153] http://www.impulse.de/downloads/E-Business_2004.pdf (zuletzt abgerufen am 30.08.2004).

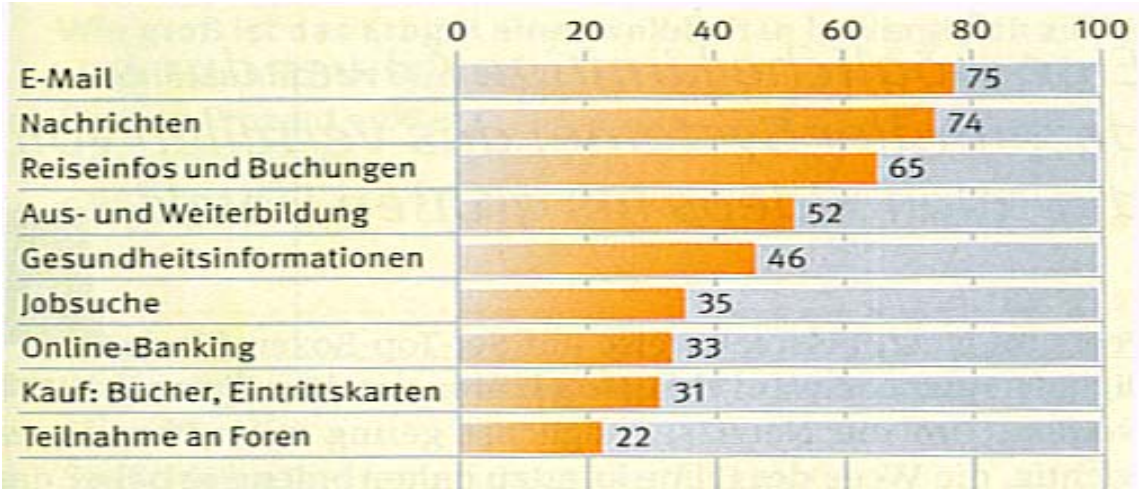
Anteile der Haushalte mit Internet-Anschluss in Prozent



Quelle: Gallup Europe 2002

Fast jeder zweite Haushalt in der Europäischen Union besaß Ende 2002 einen Internet-Anschluss. Auffällig ist dabei, dass in den nordeuropäischen Ländern der Anteil derer, die online sind, deutlich höher ist als im Süden. Deutschland liegt im Mittelfeld der 15 EU-Staaten.

Anteile der Nutzungsformen des Internets in Prozent



Quelle: Gallup Europe 2002

Die Hauptanwendungsform des Internets ist das Versenden von E-Mails. Ebenfalls begehrt sind bei den Web-Nutzern Nachrichtendienste und Reise-Dienstleistungen. Für das Online-Banking fehlt vielen offenbar noch das Vertrauen in die Sicherheit.

Man kann also davon ausgehen, dass das Internet mittlerweile alle wichtigen Lebens- und Wirtschaftbereiche miteinander verbindet. Die fortschreitende Digitalisierung noch analoger Lebensbereiche wird diesen Trend verstärken. Mit der Vernetzung steigen aber auch die Möglichkeiten krimineller Art. Die Beschäftigung mit Viren, Trojanern oder Spoofing-Formen gewinnt hierdurch an Bedeutung. Dadurch wird eine zunehmende Beschäftigung mit der hiermit verbundenen Tätergruppierung der Hackerszene notwendig. So stellen Autoren wie Prof. Dr. Horst W. Opaschowski die berechtigte Frage, ob der nächste Krieg über das Web geführt wird und ob im Zeitalter des Internets ein Laptop als alleinige Waffe genügt.[154]

[154] Opaschowski 2001, S. 9ff.

2.3 Computerkriminalität im weiteren Sinn

2.3.1 Spam

2.3.1.1 Definition und Formen

Allgemein nennt man das Versenden unverlangter Botschaften an eine Vielzahl von Internetnutzern „Spam“[155]. Derjenige, der diese unerwünschten Botschaften verschickt, wird als Spammer bezeichnet.[156] Laut EU-Kommission versteht man unter Spam unverlangt zugestellte E-Mails.[157] Diese Definition kann jedoch der Formenvielfalt der heutigen Spamversendungen nicht genügen und muss somit verworfen werden. Ursprünglich wurden mit dem Begriff Spamming unpassende und kommerzielle Beiträge in Newsgroups bezeichnet. Mittlerweile ist damit am häufigsten das „Zumüllen“ eines elektronischen Briefkastens mit „unerwünschten Werbebotschaften“ gemeint.[158] Man spricht dann auch von Junk-Mail, Bulk-Mail oder Unsolicited Commercial Email (UCE).[159] Spam betrifft auch das Handy: einerseits durch verstärkten Einsatz von Mobile Marketing zur Marktforschung, andererseits durch unerwünschte SMS, die in Japan schon bis zu 90 Prozent der Spams ausmachen.[160] Daneben gibt es noch das so genannte Suchmaschinen- oder Index-Spamming, bei dem ein Spammer die Ergebnisse, die eine Internetsuchmaschine auf eine Stichworteingabe hin ausgibt, derart manipuliert, dass auf den vordersten Plätzen Webseiten angezeigt werden, die keine für den Surfer relevanten Informationen enthalten.[161]

Ein Grund für das Zustandekommen dieser rapiden Vermehrung an Spam-Mails in letzter Zeit konnte kürzlich von einer Fachzeitschrift aufgedeckt werden: Autoren und absichtliche Verbreiter von Computerviren arbeiten seit Mitte 2003 mit Versendern von Spams zusammen. Die

---

[155] Spam ist ursprünglich der Name eines vor allem in Großbritannien beliebten Büchsenfleisches. In einem Monty Python Sketch wird dieser Begriff auf missbräuchliche Newsartikel angewendet und wurde später auf elektronischen „Müll“ (in diesem Fall für „Mail-Müll“) übertragen. In dem Sketch macht ein lautstarker Wikinger-Chor am Ende jede Kommunikation unmöglich – genau wie der E-Mail-Müll die Kommunikation immer schwerer macht. Der genannte Sketch ist unter http://www.detritus.org/spam/skit.html in Wort und Ton zu finden.

[156] http://de.wikipedia.org/wiki/Spam (zuletzt abgerufen am 27.04.2004).

[157] Richtlinie für den Schutz persönlicher Daten und der Privatsphäre auf dem Feld der elektronischen Kommunikation (RL 2002/58/EG)

[158] Jaeger 2002 S. 189 ff. Dabei treten diese E-Mails als Kettenbriefe, Pyramidenspiele oder Werbung für Pornografie auf.

[159] http://www.hrz.uni-dortmund.de/computerPostille/September2003/012.html (zuletzt abgerufen am 17.06.2004).

[160] http://de.wikipedia.org/wiki/Spam (zuletzt abgerufen am 17.06.2004).

[161] Ebd.

Computerviren werden dazu so programmiert, dass dem Benutzer die Virenverseuchung des Rechners nicht auffällt: Der Virus enthält keine offensichtliche Schadfunktion und zerstört keine Dokumente. Er nistet sich aber in das Betriebssystem ein, kann dieses fernsteuern und reagiert auf Befehle des Virenautors.[162]

Spam wird mittlerweile als ein ernstzunehmendes Problem angesehen. Da die meisten Spams ihren Ursprung in den USA haben, häufen sich dort Klagen gegen Spamversender.[163] Im Mai 2004 wurde der unter dem Pseudonym „Buffalo Spammer" bekannt gewordene US-Amerikaner Howard Carmack zu sieben Jahren Gefängnis verurteilt. Zudem ist er vom Bundesgericht in Atlanta zu einer Zahlung von 16,4 Millionen US-Dollar an den US-Internet-Provider Earthlink verurteilt worden. Carmack hatte sich die Identitäten von zwei Bürgern der Stadt Buffalo angeeignet und über den Provider Earthlink mehr als 850 Millionen Spams verschickt.[164]
Auch deutsche Gerichte beschäftigen sich zunehmend mit der Spamproblematik. In einem Rechtsstreit zwischen zwei Internet-Dienstleistern, die zueinander im Wettbewerb stehen, entschied der Bundesgerichtshofs am 11. März 2004, dass die unerbetene Zusendung von Werbung enthaltenden E-Mails gegen die guten Sitten im Wettbewerb verstößt und eine unzumutbare Belästigung darstellt. Die Beklagte hatte Ende 1998 über ein Dutzend unangeforderte gewerbliche Newsletter an verschiedene Mail-Accounts der Klägerin versandt.[165] Deutsche Parteien fordern zum Teil, Gefängnisstrafen für Spammer einzuführen.[166]

2.3.1.2 Verbreitungsarten

Spam wird mit diversen automatisierten Tools verschickt, die frei im Internet verfügbar sind.[167] Diese ähneln strukturell und bedienungstechnisch den Virenbaukästen und sind auch mit wenig technischem Wissen von jedermann zu bedienen. Das größere Problem liegt in der Beschaffung geeigneter E-Mailadressen. Um diese ausfindig zu machen, bedienen sich Spammer verschiedener Techniken, die im Folgenden aufgezeigt werden sollen.

---

[162] http://www.heise.de/kiosk/archiv/ct/2004/5/18 (zuletzt abgerufen am 17.06.2004).
[163] http://www.nachrichten.ch/detail/188136.htm (zuletzt abgerufen am 26.08.2004).
[164] http://www.heise.de/newsticker/meldung/47764 (zuletzt abgerufen am 26.08.2004).
[165] http://www.heise.de/newsticker/result.xhtml?url=/newsticker/meldung/46627&words=Spam%20Urteil (zuletzt abgerufen am 26.08.2004).
[166] Zimprich 2004.
[167] Siehe zum Beispiel http://www.oddthunder.com/n.antivirus.htm (zuletzt abgerufen am 18.06.2004); http://www.bioniciberica.com/dir.viren.htm (zuletzt abgerufen am 18.06.2004); http://bau2.uibk.ac.at/matic/security.htm (zuletzt abgerufen am 18.06.2004).

2.3.1.2.1 Adresshandel

Nicht professionelle Spammer haben die Möglichkeit über Tauschbörsen, wie z.B. Emule und Edonkey, mit E-Mail-Adressen zu handeln und zu tauschen. Suchbegriffe wie „Spam Mails“ oder „E-Mail-Adressen“ führen hierbei zum gewünschten Erfolg. Die Tauschbörsen werden aber auch von den professionellen Spammern genutzt, um ihre Datenbanken zu vervollständigen oder einfach Tauschmöglichkeiten zu haben.[168]

2.3.1.2.2 Scannen

Die automatisierte Suche nach E-Mail-Adressen mit speziell dafür geschriebenen Programmen, auch Harvesting genannt, nennt man Scannen. Solche Programme werden meist für wenig Geld von Unternehmen angeboten und bieten diverse Funktionen, mit denen man den Sammelvorgang optimieren kann. Verbreitet ist das Scannen von so genannten Newsgroups, aber auch das Scannen von Webseiten ist nicht selten. Besonders ärgerlich an dieser Sammelmethode ist, dass es für Nutzer kaum Ausweichmöglichkeiten gibt. Der Grund, wieso man eine Adresse im Usenet oder auf einer Webseite angibt ist, dass andere Internetbenutzer per E-Mail Kontakt aufnehmen können. Gibt man seine Adresse nicht oder nur verfälscht an, wird die Kontaktaufnahme für andere schwierig oder gar unmöglich.[169]

2.3.1.2.3 Brute Force

Mit sinkenden Versandkosten wird es für die Spammer vermehrt attraktiv, durch systematisches Durchprobieren von gängigen Kombinationen (z.B. üblichen Accountnamen wie info@..., webmaster@... oder verbreiteten Vornamen) an gültige Adressen zu kommen, das wegen der brachialen Methode als Brute Force bezeichnet wird. Besonders lästig an dieser Methode ist, dass man selbst dann Spams erhalten kann, wenn man seine Adresse nirgendwo veröffentlicht hat. Eine Abhilfe schafft bestenfalls die Verwendung von kryptischen E-Mail-Adressen, die den Charakter eines Passworts haben, was aber dazu führt, dass sich Freunde und Bekannte kaum die E-Mail-Adresse merken können.[170]

---

[168] http://www.teltarif.de/i/spam-methoden.html (zuletzt abgerufen am 18.06.2004).
[169] http://www.teltarif.de/i/spam-methoden.html (zuletzt abgerufen am 18.06.2004)
[170] Ebd.

2.3.1.2.4 SMTP-Harvesting

Eine Methode, die es erst gibt, seit ADSL- und Kabelanschlüsse für wenig Geld zu haben sind, ist das so genannte SMTP-Harvesting. Dabei werden SMTP-Server, die für den Versand und den Empfang von E-Mails zuständig sind, gezielt nach möglichen Buchstabenkombinationen abgefragt. Gemäß SMTP-Standard meldet ein empfangender Server dem Sender, wenn er eine E-Mail nicht ausliefern kann, weil die Adresse nicht existiert. Spammer können nun je nach Antwort des Servers darauf schließen, ob eine angegebene E-Mail-Adresse existiert. Existiert zum Beispiel die Adresse abc@provider1, so probieren Spammer aus, ob auch abc@provider2 existiert. Diesen Angriffen sind vor allem die bekannten Provider ausgesetzt, denn dort ist die Wahrscheinlichkeit, dass eine Adresse existiert, am größten. Abhilfe gegen solche Praktiken schafft praktisch nur noch die Verwendung einer E-Mail-Adresse, die in dieser Form nicht existiert, und solche mit gängigen Vornamen müssen dagegen in Zukunft wahrscheinlich gemieden werden.[171]

2.3.1.3 Schäden

Spam erzeugt eine Vielzahl von Problemen: Spam ist in der Hinsicht einzigartig, dass die Empfänger viel mehr dafür bezahlen als der Absender. Der Absender bezahlt nur für ein Account bei seinem Provider und verhältnismäßig wenig Telefongebühren. Der Rest wird von den Empfängern bezahlt. Dabei sind nicht nur Zeit und Telefongebühren zum Herunterladen der Spam zu berücksichtigen. Spam verstopft auch die Leitungen und füllt die Festplatten der Mail- und News-Server des Providers. Spams mit ungültigen Adressen erzeugen Fehlermeldungen, die der Provider erhält. Diese Kosten des Providers belasten die Konten der Kunden. Aber auch die Zeit des Empfängers ist ein Faktor. Das wäre kein Problem bei einem einzigen Spam, aber ab einer bestimmten Anzahl an Spam stellt auch der Zeitfaktor zunehmend ein Problem dar. Die Menschen, die noch keinen Breitbandanschluss besitzen, zahlen sehr viel Geld dafür, dass die unerwünschte Mail geladen wird. Der Spammer bezahlt nur einige Sekunden Onlinezeit. Zu beachten bleibt ferner, dass Mailserver verstopft werden können und dadurch der E-Mail-Versand gestoppt wird. Ebenfalls ist daran zu denken, dass heutzutage schon viele Minderjährige eigene E-Mail-Adressen besitzen. Hardcore-Porno-Mails, die von 10-jähigen Kindern gelesen werden, sollten somit ebenfalls als ein Spam-Problem betrachtet werden. Zudem stellt sich die Frage, ob das Medium E-Mail an Bedeutung verliert oder sogar

[171] Ebd.

in Zukunft gänzlich lahm gelegt wird, wenn die Nutzer die eigentlich relevanten E-Mails nicht mehr herausfiltern können oder sogar löschen, da sie diese irrtümlich als Spam behandelt haben.

Das Thema beschäftigt nicht nur viele einzelne Internetnutzer, sondern auch Dutzende nationale Gesetzgeber und internationale Organisationen wie die UNO, die EU-Institutionen und die OECD.[172] Spam ist nicht nur kein Kavaliersdelikt, sondern muss als Problem ernst genommen und bekämpft werden. Der Stellenwert von Spam zeigt sich unter anderem dadurch, dass die Europäische Kommission eine Erweiterung der EU-Maßnahmen zur Bekämpfung von Kinderpornographie, Rassismus und Spam im Internet vorschlägt.[173]

Das Ausmaß der Belästigung ist in den letzten Jahren massiv gestiegen. 2001 wurde das Spam-Aufkommen auf „lediglich" 7 Prozent des gesamten E-Mail- Verkehrs geschätzt, 2002 auf 29 Prozent und die Prognosen für 2003 lauteten auf 51 Prozent.[174] Dieser Wert war laut dem Internet-Sicherheitsunternehmen Messagelabs[175] im Februar 2004 bereits erreicht, als jeder zweite E-Mail-Inhalt als Spam angesehen werden musste. Von Juni 2003 bis März 2004 vermehrte sich das Aufkommen von Spam um rund 600 Prozent.[176] Die FAZ berichtet, dass 65 Prozent aller E-Mails unerwünschte Werbeinhalte enthielten.[177]

2.3.1.4 Verbote

Spam ist in der Regel strafbar. So verstoßen unerwünschte E-Mails mit Werbeinhalten in Deutschland nicht nur gegen das Wettbewerbs- und Persönlichkeitsrecht[178], sondern auch gegen § 118 des Gesetzes gegen Ordnungswidrigkeiten (OWiG). Das Versenden von Porno-Spam kann man sogar nach § 119 OWiG behandeln. Neben dem OWiG kann man sich im Fall von Sex-Spam auch an § 184 StGB (Verbreitung pornographischer Schriften) halten, da

[172] http://www.rechtsprobleme.at/doks/laga-e-mail-werbung-endg.pdf (zuletzt abgerufen am 17.06.2004).
[173] IP/04/333, Brüssel, den 12. März 2004, im Internet unter http://europa.eu.int/rapid/start/cgi/guesten.ksh?p_action.getfile=gf&doc=IP/04/333|0|RAPID&lg=DE&type=PDF (zuletzt abgerufen am 17.06.2004).
[174] Mitteilung der Kommission über unerbetene Werbenachrichten (Spam), Brüssel, den 22.01.2004, KOM(2004) 28.
[175] http://www.messagelabs.com. (zuletzt abgerufen am 17.06.2004).
[176] Gemäß laufend aktualisierter Statistik von Messagelabs, im Internet unter http://www.messagelabs.com/viruseye/threats/default.asp?tabIt=spam&spamduration=Last+12+months&spamgraphtype=bar&spamdata=volume (zuletzt abgerufen am 17.06.2004).
[177] Frankfurter Allgemeine Zeitung, 20.03.2004, Nr. 68 S. 17.
[178] http://www.uni-kassel.de/~seidler/LEX_S.HTM#Spam (zuletzt abgerufen am 17.06.2004).

es schließlich nicht auszuschließen ist, dass auch Minderjährige solche Spam-Mails erhalten.[179]

2.3.2 Betrugsformen

2.3.2.1 Allgemein

Die grenzüberschreitende wirtschaftliche Betätigung per Internet bietet den Unternehmen neue und gewinnbringende Möglichkeiten des Handels mit Waren und Dienstleistungen. Das Internet ist aufgrund seiner Eigenschaft als Kommunikationsforum besonders zum schnellen Informationsaustausch für die wirtschaftliche Nutzung geeignet. Die Virtualität und Vielfalt des E-Commerce bieten jedoch auch Raum für Wirtschaftskriminalität und Betrugsdelikte unterschiedlichster Ausprägung.[180] Grundsätzlich weisen diese Betrugsdelikte nichts speziell Neues auf, so dass auf eine ausführliche Erläuterung verzichtet werden soll. Stattdessen sind durch den Computer und das Internet vielseitige Eigenarten und Gelegenheiten aufgetaucht, die eine Darstellung einzelner Betrugsformen mit ihren spezifischen Eigenarten erfordern.

Seit nunmehr über 15 Jahren gibt es mit § 263a StGB eine Vorschrift, die den Computerbetrug unter Strafe stellt. Bis zu diesem Zeitpunkt gab es nur den normalen Betrug, so dass Fälle nicht erfasst werden konnten, in denen nicht ein Mensch, sondern ein Computer „betrogen" worden ist. Da jedoch viele wirtschaftliche Bereiche durch den Computer und das Internet automatisiert wurden, war eine Gesetzesänderung notwendig. Der Computerbetrug erfasst alle Fälle, in denen das Ergebnis eines Datenverarbeitungsvorgangs beeinflusst wird durch

- die unrichtige Gestaltung eines Programms,
- Verwendung unrichtiger oder unvollständiger Daten,
- unbefugte Verwendung von Daten oder
- unbefugte Einwirkung auf den Ablauf des Programms.[181]

Durch die Digitalisierung von Daten und Geldtransfers und die Nutzung des Internets werden länderübergreifende kriminelle Handlungen vereinfacht. Im Mai 2001 ist ein vom FBI in eine Falle gelockter russischer Hacker zu drei Jahren Haft verurteilt worden. Der 24-jährige Wassili Gorschkow aus Tscheljabinsk muss außerdem 700.000 Dollar Schadenersatz an die Firmen

[179] http://spam.blueslayah.de/?content=definition (zuletzt abgerufen am 17.06.2004).
[180] Siehe hierzu auch http://www.fraud.org/welcome.htm (zuletzt abgerufen am 05.06.2004).
[181] Jaeger, 1992, S. 55.

Speakeasy Network und PayPal zahlen. Gorschkov wurde vorgeworfen, zusammen mit seinem Komplizen Alexey Ivanov Kreditkartennummern von US-Amerikanern bei 11 Unternehmen, die in den Bereichen E-Banking, E-Commerce und Internet Service Providern tätig sind, gestohlen zu haben.[182]

Die Digitalisierung von Wirtschaftsprozessen führt zu immer neueren Betrugsformen. Im Folgenden sollen die Wichtigsten dargestellt werden.

2.3.2.2 Spezielle Formen

2.3.2.2.1 Kreditkartenmissbrauch

Beim Kreditkartenmissbrauch handelt es sich um die betrügerische Erlangung von Waren oder Dienstleistungen durch Nutzung missbräuchlich erlangter Kreditkartendaten. Die Kreditkarte hat sich in den letzten Jahren zu dem wichtigsten Zahlungsmittel im Internet entwickelt, obwohl sie eigentlich gerade für die Bezahlung kleinerer Beträge aufgrund ihrer relativ hohen Transaktionsgebühren nur bedingt geeignet ist.[183] Kreditkartenbetrug gibt es schon länger in diversen konventionellen Varianten, sowohl mit rechtswidrig erlangten echten als auch mit gefälschten Karten. Dort hängt alles von der rechtswidrigen Erlangung bzw. Herstellung und am physischen Einsatz der falschen bzw. echten Kreditkarte gegenüber einem Vertragspartner ab. Das Besondere am Internetbetrug ist, dass Kartendaten losgelöst von der Karte als Zahlungssurrogat übermittelt werden.[184] Zur Kreditkartenzahlung reichen folgende Angaben:

- Name des Karteninhabers
- Gültigkeitsende der Karte
- Kartennummer
- Anschrift des Kartenbesitzers oder die Sicherheitsnummer.[185]

Die Täter erhalten die Kartendaten unbefugt über im Internet erhältliche Software-Tools, mittels derer authentische Kartennummern erzeugt werden können oder durch Ausspähen bzw. Hacking-Angriffe, z.B. bei Internet-Händlern, wodurch dann dort gespeicherte echte Kartendaten erlangt werden.[186] Eine weitere Möglichkeit wäre das Ausspähen der Daten bei der Übertragung. Bei unverschlüsselten Verbindungen oder in unverschlüsselten E-Mails werden

[182] http://www.e-media.at/home/meldung.asp?ID=2652 (zuletzt abgerufen am 15.08.2004).
[183] http://www.computerbetrug.de/kk/allgemeines.php?p=0|32| (zuletzt abgerufen am 05.06.2004).
[184] Janovsky 1998, S. 501.
[185] http://www.computerbetrug.de/kk/allgemeines.php?p=0|32| (zuletzt abgerufen am 05.06.2004).
[186] Kubica 2001, S. 76.

die Daten im Klartext übertragen.[187] Die Erstellung einer Kartenkopie ist eine weitere Variante. Die Daten einer Kreditkarte können mittels eines Magnetstreifenlesers kopiert werden. Mit Hilfe dieser Daten kann ein Kartenduplikat erstellt werden. Solche Blankokarten werden auch als „White Plastic“ bezeichnet.[188] Daneben kursieren im Internet diverse Programme, mit denen sich Kartennummern errechnen lassen, die potenziell real existieren können. Die Prüfungsprogramme der Verkäufer fallen dann auf diese Kartennummern herein und bestätigen die Echtheit der Karten.[189] Es reicht jedoch auch, wenn jemand die Kartendaten – z.B. an der Tankstelle von weggeworfenen Belegen – abschreibt und zusätzlich den Namen in Erfahrung bringt.[190]

Genutzt werden können diese Kartendaten für kostenpflichtige Internetzugänge oder für Warenbestellungen, insbesondere im Bereich Elektronik oder Reisen. In der Regel trägt der Internethändler bzw. -anbieter den Schaden. Die Kartendaten werden bei Transaktionen ausschließlich im Hinblick auf Authentizität der Daten und auf einen möglichen Ablehnungsgrund (z.B. Limitüberschreitung, Sperre) überprüft, aber nicht in Kombination mit dem dazu angegebenen Namen. Die Lieferanschriften liegen im Betrugsfall häufig in osteuropäischen Ländern. Belastete rechtmäßige Karteninhaber werden die Transaktion reklamieren. Der Kartenemittent bucht den Umsatz zu Gunsten des rechtmäßigen Karteninhabers zurück. Belastet bleibt der Händler oder Anbieter, der die Waren oder Dienstleistungen bereits geliefert hat.[191]
Im Dezember 2000 wurde bekannt, dass Hacker in das IT-System des Internethändlers „egghead.com“, Kalifornien/USA, eingedrungen waren und ca. 3,5 Millionen Kreditkartendaten kopiert hatten. Die Kartendaten wurden anschließend für betrügerische Umsätze in Russland, Großbritannien, den USA, Deutschland, Frankreich, Italien, Irland, den Niederlanden und Israel eingesetzt.[192]

2.3.2.2.2 Onlineauktionen

Bei Onlineauktionen entstehen die Betrugsschäden dadurch, dass jemand unter Verwendung fiktiver Personalien Waren oder Dienstleistungen zur Versteigerung bei Online-

[187] Verschlüsselte Verbindungen erkennt man grundsätzlich daran, dass die Adressen mit https:// beginnen. Zudem sollte man E-Mails verschlüsseln, wenn darin Kreditkarteninformationen enthalten sind.
[188] http://www.computerbetrug.de/kk/allgemeines.php?p=0|32| (zuletzt abgerufen am 05.06.2004).
[189] Ebd.
[190] Ebd.
[191] Janovsky 1998, S. 501.
[192] Kubica 2001, S. 76.

Auktionshäusern anbietet, wobei der Käufer, der den Zuschlag erhält, zunächst das Geld auf ein angegebenes Konto überweisen muss.[193] Die Lieferung oder Leistung bleibt aber aus. Der analoge Modus Operandi ist auch bei direkten Kaufangeboten in einschlägigen Internetforen festzustellen. Hier gibt es spezielle Ausprägungen in Richtung „Schnäppchen-Angebote", bei denen von vornherein längere Lieferfristen avisiert werden, die den ersichtlichen Vorteil haben, dass die Täter in Ruhe verschwinden können, bevor überhaupt der Schaden bemerkt wird.[194]

Im „Traumreisen-Fall" hatte die Tätergruppe Karibik-Reisen zu Topkonditionen angeboten. Je Auktion kamen in der Regel mehr als DM 3.000 auf ein spanisches Konto. Reisen gab es nie. Über 30 Schadenfälle sind dem Bundeskriminalamt bekannt, ca. 100 werden vermutet.[195]

2.3.2.2.3 Onlinebanking

Viele Homebanking-Anwender setzen heute das PIN/TAN-System ein, das auf der Nutzung von Persönlichen Identifikationsnummern (PIN) und Transaktionsnummern (TAN) beruht. Dabei ruft der Benutzer mittels einer verschlüsselten Verbindung die Internetseite seiner Bank auf.[196] Java-Programme stellen dann die eigentliche Banking-Funktionalität zur Verfügung. Der Benutzer gibt daraufhin seine Kontonummer und seine PIN an. Die PIN ist meist eine ca. fünfstellige Zahl, manchmal kann man auch Kombinationen aus Zahlen und Buchstaben verwenden. Jetzt kann der Benutzer seine Kontodaten (Kontostand, getätigte Überweisungen und Abhebungen etc.) anschauen und allgemeine Einstellungen vornehmen. Für die Ausführung von Aufträgen werden wiederum die Transaktionsnummern (TAN) benötigt. Transaktionsnummern sind nur einmalig verwendbar und verfallen danach. Der Kunde erhält die Transaktionsnummern normalerweise per Brief in Blöcken zu ca. 50 Stück (variiert leicht von Bank zu Bank). Üblicherweise benötigt man pro Überweisung eine TAN. Nach Anbruch eines neuen Blocks werden normalerweise alle TAN des vorher verwendeten Blocks ungültig.[197]

Neben dem PIN/TAN-System existiert eine Modifikation und Erweiterung: HomeBanking Computer Interface (HBCI). HBCI funktioniert nicht über einen normalen Browser, sondern setzt die Nutzung einer zusätzlichen Software voraus. Der Kunde authentifiziert sich bei der

[193] Bei diesem Konto handelt es sich zumeist um ein Auslandskonto.
[194] Kubica 2001, S. 76f.
[195] Kubica 2001, S. 77.
[196] Dabei handelt es sich meist um eine Verschlüsselung über https.
[197] http://www.computerbetrug.de/homebanking/pin-tan.php?p=0|32|38|44|47| (zuletzt abgerufen am 05.06.2004).

Anmeldung mit Hilfe einer Chipkarte oder eine Schlüsseldiskette und einer PIN. Falls die Authentifizierung mittels Chipkarte erfolgen soll, ist selbstverständlich auch ein Chipkartenleser erforderlich. Der Kunde erfasst seine Aufträge in seinem Homebankingprogramm und authentifiziert die Ausführung wieder mit Chipkarte und PIN; und das Homebankingprogramm gibt die Aufträge gesammelt und verschlüsselt an den Bankrechner weiter.[198]

Grundsätzlich bieten diese Verfahren genügend Schutz vor Missbrauch und stellen dem Angreifer ein ausreichendes Hindernis in den Weg. Diese Verschlüsselungen sind nach dem derzeitigen Stand in den meisten Fällen hinreichend sicher. Der Aufwand, diese zu knacken, rechtfertigt häufig nicht das zu erwartende Ergebnis bei einem Privatnutzer.[199] Vielmehr müssen konventionelle Benutzerfehler wie die unzureichend sichere Verwahrung der PIN und der TAN als Schwachstellen in diesen Systemen angesehen werden.

2.3.2.2.4 Dialer

Dialer sind Programme, die eine Einwahlverbindung ins Internet über 0190-Rufnummern aufbauen und Zugang zu kommerziellen Internetangeboten schaffen. Sie werden z.B. von Anbietern kostenpflichtiger Internetseiten als Alternative zur Übermittlung der Kreditkartennummer oder der Kontoverbindung verbreitet.[200] Um Zugriff auf eine bestimmte Homepage des Anbieters zu erhalten und damit auch auf die kostenpflichtigen Inhalte zugreifen zu können, muss der Kunde ein spezielles Programm herunterladen. Dabei ist eine Eingabe eines Nutzernamens oder eines Passworts in der Regel nicht erforderlich, da die Abrechnung über die Telefonrechnung erfolgt.[201] Durch die Telefonverbindung entstehen zeitabhängig unterschiedlich hohe Kosten.[202]

Dialer werden unter anderem auf Homepages angeboten, deren Gestaltung den arglosen Kunden weder beim Download noch bei der Installation erkennen lassen, dass später besondere Kosten entstehen werden. Einige Internetseiten enthalten im Quelltext Skripte (ActiveX) oder Programme (Java), die aktive Inhalte ausführen können, sobald die Seite von einem Browser aufgerufen wird. Besucht ein Nutzer eine solche Seite, öffnet sich eine Vielzahl neuer Browser- und Dialogfenster. Im Bemühen der überraschten Nutzer, alle Fenster wieder zu schlie-

[198] http://www.computerbetrug.de/homebanking/hbci.php?p=0|32|38|44|47| (zuletzt abgerufen am 05.06.2004).
[199] Diese Verbindung wird gewöhnlich mit einem 128bit-Schlüssel verschlüsselt.
[200] Dabei tarnen diese sich auch als „Highspeed-Zugang“ oder „Zugangstool“.
[201] Picko, 2002 S. 282.
[202] http://www.computerbetrug.de/dialer/kosten.php?p=0|32|38|44|47|59| (zuletzt abgerufen am 05.06.2004).

ßen, stimmen sie unbeabsichtigt auch dem Download eines Dialers zu. ActiveX-Skripte können bei entsprechender Konfiguration des Internetbrowsers sogar den Download und die Installation des Dialers unbemerkt und ohne das Zutun des Nutzers ausführen.[203]

Immer häufiger werden Dialer auch in Spam-Mails[204] verbreitet. Die Dialer werden als Attachment (Dateianhang) oder in Form einer HTML-E-Mail[205] auf den Rechner der arglosen Kunden befördert. Den Nutzern wird vorgetäuscht, es handle sich dabei um eine nützliche Software oder ein Update, oder es wird bei Verwendung des Dialers ein schnellerer Zugang zu einem Erotikangebot versprochen. Durch die Computerisierung moderner Handys verbreitete sich der erste Handydialer im August 2004 auf Mobiltelefonen mit Symbian-Betriebssystemen Series 60. Der Trojaner verschickt ohne das Wissen des Handybesitzers SMS und steigert so die Telefonrechnung.[206] Die Varianten der Verbreitung, mit denen die Nutzer zur Installation und Nutzung der Dialer veranlasst werden sollen, ist vielfältig und ließe sich noch beliebig fortsetzen.

2.3.2.2.5 Sonstige Delikte

Der Computer und das Internet nehmen mehr und mehr alle wirtschaftlichen Bereiche ein, so dass durch die vielen computerspezifischen Neuerungen auch neue Betrugsformen auftauchen werden. In diesem Zusammenhang sollen an dieser Stelle andere betrugsähnliche Betätigungen, die durch den Computer und das Internet keine spezielle Neuerung erfahren haben, sondern nur auf ein neues Medium umgestiegen sind, lediglich erwähnt werden. Dazu zählen unter anderem das verbotene Betreiben von Bankgeschäften im Internet, das unerlaubte Betreiben von Onlinespielkasinos, Kapitalanlage- und Kreditbetrug im Internet, Manipulation von Bankkonten und anderen Wertformen, Anlagebetrug sowie neue Formen der Geldwäsche durch Onlinebanking.[207]

[203] Picko 2002, S. 282.
[204] Bei einer Spam-Mail handelt es sich um eine E-Mail, die zu Werbezwecken in großer Anzahl an beliebige Empfänger verschickt wird.
[205] Moderne E-Mail-Programme erlauben das Versenden und Empfangen von E-Mails, die wie eine World-Wide-Web-Seite formatiert werden.
[206] http://derstandard.at/?url=/?id=1757309 (zuletzt abgerufen am 26.08.2004).
[207] Wiedemann 2000, S. 231 ff.

2.3.3 Piraterie oder Urheberrechtsverletzungen

Im Januar 2004 wurden 14 jugendliche Hacker verhaftet, die mit einem Virus einen Windows-Fehler ausgenutzt hatten und sich so in den Rechner der Universität der galizischen Stadt Vigo eingeschlichen hatten. Von dort aus haben sie einen Handel mit Musik, Filmen und Softwareprogrammen betrieben. Den 14 Hackern werden Urheberrechtsdelikte und die Verbreitung von Geheimnissen vorgeworfen, worauf bis zu vier Jahre Haft stehen.[208]

Die Digitalisierung der Medien und das Internet ermöglicht es Nutzern, eine neue Qualität von Rechtsschutzverletzungen zu begehen. Dabei handelt es sich vornehmlich um Rechtsschutzverletzungen, die als Produktpiraterie bezeichnet werden. Darunter versteht man ein Produkt, das durch Urheberrecht und/oder verwandte Schutzrechte (Rechte der ausübenden Künstler, der Hersteller von Ton- und Tonbildträgern und der Sendeanstalten, Patent- und Markenrechte) geschützt ist und ohne oder gegen den Willen des Rechtsinhabers verwendet wird.[209] Der Reiz und die Problematik der neuen Medien liegen in der einfachen und komfortablen Handhabung der transportierten Inhalte. Seit Lösungen vorhanden sind, wie man z.B. Texte, Musikstücke, Bilder und vielleicht bald Gerüche digitalisieren kann, lassen sich diese in hoher Geschwindigkeit ohne Qualitätsverluste und ohne nennenswerten Aufwand vervielfältigen, verteilen und verarbeiten. Die Digitalisierung und deren Vorzüge trennen den Inhalt und die durch das Medium bestimmte Form von Werken geistigen Eigentums in zunehmendem Maße. Das heißt, die Form ist sehr wandelbar geworden und verliert an Bedeutung. Aber gerade die Form, wie etwa ein gedrucktes Buch, ermöglicht es Urhebern, ihre Werke zu verwerten. Inhaber von Urheberrechten und verwandten Schutzrechten beklagen seit Jahren die Problematik der Produktpiraterie und Honorarausfälle in Milliardenhöhe.[210] Grund dafür sind in erster Linie die neuen Informationstechnologien wie Internet und MP3-Geräte. Auch die Software-Industrie ist von der Problematik betroffen und bekämpft zunehmend das Problem. Durch „Gratisdownloads“ werden geschützte Werke und Leistungen ohne Gegenleistung verwendet oder kopiert. Dadurch werden die Inhaber von Urheberrechten und verwandten Schutzrechten um ihr Einkommen gebracht.[211]

---

[208] Streck 2004.

[209] http://www.ifpi.org/site-content/antipiracy/what_is_piracy.html. (zuletzt abgerufen am 09.06.2004).

[210] Wolf/Wolf 2000; einen zusätzlichen Überblick über die globalen Schadenshöhen findet man in der Studie des unabhängigen Marktforschungsinstituts IPR. Zu finden unter http://global.bsa.org/germany/piraterie/ipr-studie.php (zuletzt abgerufen am 09.06.2004).

[211] http://www.ifpi-schweiz.ch/main.html. (zuletzt abgerufen am 09.06.2004).

Im Folgenden werden die Rechtsschutzverletzungen, die mit dem Computer und dem Internet begangen werden können, in vier große Bereiche eingeteilt: Musik- und Filmrechtsverletzungen, Urheberrecht und Software, Verletzungen von Urheberrecht und WWW sowie Rechtschutz technischer Schutzmaßnahmen.

2.3.3.1 Überblick

Eine Folge der raschen Entwicklung digitaler Technologien, der Konvergenzen verschiedener Sektoren wie Telekommunikation, Computerindustrie und Medienunternehmen, ist die Entstehung spezifischer Marktplätze im Internet. Gerade die Musikindustrie kann als typische Branche für jene Verschiebungen und Transformationen angesehen werden. In digitalisierter Form angebotene Musik zählt zu den wenigen Gütern, die sich über das Internet nicht nur bestellen, sondern auch direkt über multimediale Netzwerke distribuieren lassen. Die Verbreitung von Musik als digitale Information ist in zunehmendem Maße unabhängig von herkömmlichen Produktions- und Vertriebsstrukturen. Mit im Internet erhältlichen Ausleseprogrammen[212] können Benutzer heute Filmdateien von der Original-DVD auslesen. Sie können also identische Kopien erstellen, indem sie die digitalen Informationen einfach auf der Festplatte des eigenen Rechners speichern. Danach kann der Film wie jede andere Datei von der PC-Festplatte gelesen und elektronisch weiterverbreitet werden. Wenn die Filmdatei im Internet angeboten wird, kann jeder beliebige Nutzer eine eigene Kopie anlegen.[213] Die Entwicklung des Kompressionsformats MP3[214] ist dabei die technische Innovation, die Musik im Netz populär machte und damit die Aufmerksamkeit sowohl der Nutzer als auch der Musikindustrie auf das Internet als neuen Vertriebsweg lenkte.[215] Interessant ist dabei, dass erst das massenhafte illegale Tauschen von Musikdateien durch jugendliche Nutzer, also die illegale Nutzung dieses Mediums, dazu führte, dass die Musikindustrie diesen Vertriebsweg für sich erkannte. MP3 ermöglicht es, digitale Musikinformation ohne merklich hörbaren Qualitätsverlust auf ein Zwölftel der jeweiligen Datengröße zu reduzieren.[216] Der Austausch

[212] Es gibt mittlerweile unzählige Programme, mit denen DVDs gerippt und kopiert werden können. Zu nennen sind unter anderem DVDx, DVD2one, DVD2SVCD, Gordian Knot, Clad DVD. Anleitungen findet man unter anderem auf der Seite http://www.dvdanleitung.de/UpDownload-index-req-viewsdownload-sid-34.html (zuletzt abgerufen am 10.06.2004).

[213] Europa- und verfassungsrechtliche Bedenken sowie Hintergründe zu Urheberrechtsverletzungen in Nikoltchev 2002.

[214] MP3 ist die Abkürzung für MPEG (Motion Picture Expert Group) Audio Layer 3. Oftmals wird fälschlicherweise die Bezeichnung MPEG 3 verwendet, wobei sich hinter MP3 ein Teil des MPEG- Standards, genaugenommen die „Tonspur" von digitalen Videos im MPEG-1 oder MPEG-2 Format verbirgt, und daher die korrekte Bezeichnung des Formats und der Kompressionstechnik MPEG Audio Layer 3 (MP3) lautet.

[215] Zum Wandel der Musikindustrie und der Digitalisierung der Ton- und Filmmedien siehe tor.at/resources/computer/net/internet/law/caterina_ceschi__musik_im_netz.pdf (zuletzt abgerufen am 09.06.2004).

verlust auf ein Zwölftel der jeweiligen Datengröße zu reduzieren.[216] Der Austausch derart komprimierter Dateien über multimediale Netzwerke kann somit wesentlich schneller und mit wenigen Ressourcen erfolgen.[217] Die zunehmende Verbreitung des MP3-Kompressionsverfahrens löste innerhalb kürzester Zeit einen Tauschboom von Musikfiles über verschiedene Filesharing-Plattformen[218] im Internet aus. Der Start der Musiktauschbörse Napster[219] im Mai 1999 hatte zur Folge, dass, bedingt durch die übersichtliche und bedienerfreundliche Benutzeroberfläche der Software, bereits nach wenigen Monaten mehrere Millionen Anwender das Programm auf ihren Festplatten abgespeichert hatten.[220]

Die Funktionsweise und der Erfolg von Filesharing-Programmen beruht darauf, dass sich eine große Zahl von Nutzern über das Internet zu einem Netzwerk zusammenschließt, dessen Zweck es ist, gegenseitig Dateien, im Speziellen MP3-Dateien auszutauschen. Beim ersten Start dieses Programms geben die Teilnehmer diejenigen Verzeichnisse auf ihrer Festplatte an, in denen sich MP3-Dateien befinden, die sie zum Tauschen zur Verfügung stellen wollen. Eine Liste dieser Dateien wird anschließend auf den zentralen Server gespeichert und dieser Suchindex kann von allen an das Netzwerk angeschlossenen Rechnern durchsucht werden. Wenn eine gewünschte Datei gefunden ist, wird sie direkt zwischen den einzelnen Teilnehmern übertragen.[221] Die hohen Datenübertragungsraten, die zusätzlich durch DSL[222] möglich sind und die neu entwickelten Datenkomprimierungsformate für Filmdateien[223] ermöglichen in zunehmendem Maße den Tausch von Filmen über Filesharing-Portale.

---

[216] Neben dem MP3-Format existieren noch weitere Datenkomprimierungsformate, wie das von Microsoft bereitgestellte WMA-Format und das Soundformat Real.
[217] Wischner 2000, S. 40ff.
[218] Filesharing ermöglicht die gemeinsame Nutzung bzw. den Austausch von Rechnerressourcen und kann daher auch als Überbegriff für das Tauschen von MP3-Dateien über das Netz gelten. Einem Filesharing kann sowohl eine zentrale und hierarchische Client/Server- Struktur als auch eine dezentrale mit gleichwertigen Partnern, eine sogenannte Peer-to-Peer-Struktur zu Grunde liegen.
[219] Die Napster-Software wurde von dem damals 19-jährigen College-Studenten Shawn Fanning entwickelt und war seit Mitte 1999 im Internet erhältlich.
[220] Die effektive Datenreduktion durch das MP3-Verfahren in Kombination mit der rasanten Ausbreitung der Napster-Software war somit der Auslöser für den aktuellen Interessenskonflikt zwischen den ökonomischen Strategien der Musikindustrie einerseits und den Filesharing-Usern, die von zu Hause aus kostenlos urheberrechtlich geschützte Musik downloaden können, andererseits. Die Musikindustrie reagierte auf den Tauschboom zunächst mit Klagen vor dem US-Bundesgericht wegen Urheberrechtsverletzung, mit Aufklärungskampagnen zum Thema Online-Musikpiraterie und mit Maßnahmen technologischer Natur.
[221] http://www.unet.univie.ac.at/~a0202424/files/Die%20Krise%20der%20Musikindustrie.pdf (Zuletzt abgerufen am 10.06.2004).
[222] DSL steht als Abkürzung für Digital Subscriber Line. Die von der US-Firma Bellcore in den 80er Jahren entwickelte DSL-Technik verwendet das Spektrum, das bei normalen Telefongesprächen ungenutzt bleibt. Mehr als 8 Megabit, also etwa 120-mal so viel wie mit ISDN, können theoretisch pro Sekunde empfangen und 768 Kbit gesendet werden.
[223] Die wichtigsten Komprimierungsformate für Filmdateien sind folgende: AVI, MPG, VCD, SVCD, MVCD, MSVCD und KVCD.

Mit dem Ende von Napster ist der Musiktausch über das Internet noch lange nicht zerstört. Nach dem Urteil im Napster-Prozess vom März 2001 scheint es zwar sicher, dass auch alle anderen zentralen Tauschbörsen früher oder später von der Musikindustrie geschlossen werden. Aber mit den P2P-Börsen[224] sind dezentrale Tauschbörsen entstanden, die nicht so einfach wie Napster durch ein Gericht verboten werden können. Am erfolgreichsten war und ist dabei das FastTrack-Netzwerk mit seinen drei auf ihm basierenden Tauschbörsen KaZaa, Morpheus und Grokster. Diese Netzwerke funktionieren nach dem gleichen Prinzip wie „Gnutella“, die erste dezentrale Tauschbörse.

2.3.3.2 Tauschbörsen-Modelle

Das Tauschen von Gegenständen und Informationen ist nicht erst mit der Entwicklung des Internets entstanden, sondern ist ein uralter Bestandteil des menschlichen Miteinanders. Bislang war es jedoch nötig, dass der jeweilige Gegenstand seinen Besitzer wechselte, so dass auf beiden Seiten der Verlust des Gegenstandes eintrat. Beim Tausch von Informationen, die nicht mündlich übertragen werden, muss zumindest das Medium, auf denen die Informationen gespeichert werden, übergeben werden. Noch heute werden Informationen mit dem Medium beim Tausch oder Verkauf übergeben. Das hier problematisierte Tauschen von Musik- und Filmstücken geschieht nicht nur im Internet, sondern auch durch das Überreichen von CD-ROMs oder DVDs, auf denen die jeweiligen Informationen gespeichert sind. Gerade bei Jugendlichen herrscht ein reger Tauschverkehr auf Schulhöfen und in ihrer Freizeit. Meines Erachtens gäbe es keine so schwerwiegenden Umsatzeinbußen, wenn der Tauschhandel auf dem konventionellen Weg weiter betrieben werden könnte. Erst die Internettauschbörsen ermöglichen eine neue Qualität des Tauschens in noch nie gesehener Form. Zum ersten Mal in der Geschichte müssen sich die Tauschpartner nicht gegenüberstehen, sondern können in Sekundenschnelle Informationen zur anderen Seite der Welt transportieren. Ein weiterer Vorteil liegt in der Digitalisierung der Informationen, so dass bei der Weitergabe des eigenen Tauschgegenstands dieser nicht wie früher verloren geht. Die Hemmschwelle, etwas zu tau-

[224] P2P steht als Kürzel für Peer-to-peer. Dabei handelt es sich um eine Netzwerkstruktur, bei der alle in einem solchen Netzwerk verbundenen Rechner gleichberechtigt sind. Sie können sowohl Server- als auch Client-Funktionen übernehmen, d.h. anderen Geräten Daten zur Verfügung stellen oder von diesen beziehen. Bei vielen Musiktauschbörsen müssen sich interessierte Nutzer zunächst eine spezielle Software auf ihrem Rechner installieren. Mit dieser erhalten sie Zugriff auf die Musikbestände anderer Anwender, die also nicht zentral auf einem Server gespeichert sind, sondern auf den Privatrechnern der Personen, die sich ebenfalls diese Software installiert haben. Das heißt, dass man selbst auch eigene Bestände anderen Nutzern zur Verfügung stellt.

schen, das nicht verloren geht, ist aus diesem Grunde sehr niedrig.[225] Das Tauschen ohne den Verlust des eigenen Gegenstandes und die unermessliche Fülle an Tauschgegenständen, die die Internetbörsen ermöglichen, machen sie so problematisch für die Wirtschaft. Die Unternehmen versuchen seitdem mit immer fortschrittlicheren Strategien, das Tauschen zu unterbinden. Die Raffinesse einzelner Programmierer zeigt sich in den immer moderneren Tauschbörsenmodellen. Wird eine Tauschbörse, wie zum Beispiel Napster, aus rechtlichen Gründen verboten, so werden neue Modelle programmiert, die sich diesen rechtlichen Gegebenheiten anpassen. Diese neuen Programme werden wiederum kostenlos im Internet allen Nutzern zur Verfügung gestellt. Interessant erscheint dabei, dass der Programmierer selbst nur einen kleinen materiellen Gewinn hat. Der große Vorteil kommt vielmehr der gesamten Internetgemeinschaft zu Gute. Es scheint ein Wettlauf der Tauschbörsenprogrammierer gegen die Film- und Musikindustrie zu entstehen. Daher sollen hier die gängigen Internettauschbörsen und ihre Funktionsweise dargestellt werden.

2.3.3.2.1 Zentrale Datenbank-Modelle

Als berühmtestes Beispiel für ein Zentrales Datenbank-Modell für das Filesharing kann Napster genannt werden. Napster unterhält eine zentrale Datenbank, welche eine Liste der zur Zeit verfügbaren Daten enthält. Als verfügbar gelten sämtliche Daten, welche von den Benutzern, die gerade online sind, mittels Filesharing zur Verfügung gestellt werden (wobei der Nutzer selbst wählen kann, welche Teile seiner Festplatte allgemein zugänglich sind). Eigentlich benutzt Napster nicht die klassische P2P-Technologie, denn sämtliche Anfragen werden zentral bearbeitet. Aufgrund der von Napster geführten Datenbank ist bekannt, welche Titel gerade angeboten werden, weshalb Napster sich als Drehscheibe des Systems als ein relativ einfaches Ziel für die Attacken der Musikindustrie darstellte.[226] Es sei jedoch erwähnt, dass auch zentral geführte P2P-Netze wie z.B. Audiogalaxy existieren, die zusätzlich auf Daten von Nutzern, welche nicht mehr online sind, verweisen. Diese Daten können dann erst heruntergeladen werden, wenn der Besitzer sich wieder im Netz angemeldet hat.

[225] Da dies auf beiden Seiten der Fall ist und beide oft den Tauschpartner nie kennen lernen, sondern viel mehr Dateien zur Verfügung stellen, ohne überhaupt Interesse daran zu haben, wer sich die Dateien herunter lädt, müsste weniger von Tauschbörsen als vielmehr von Geschenkbörsen gesprochen werden.
[226] Weitere Informationen dazu unter http://www.kefk.net/P2P/Infrastruktur/Protokolle/Napster/index.asp (zuletzt abgerufen am 10.06.2004).

2.3.3.2.2 Servants-Modelle

Bei Servants-Modellen fungieren alle Benutzer sowohl als Server als auch als Client. Berühmtheit hat hierbei Gnutella erlangt. Gnutella ist eigentlich nur die Bezeichnung für ein Kommunikationsprotokoll. Es handelt sich um eine Software, die das Gnutella-Protokoll verwendet. Im Gnutella-Netzwerk existiert kein zentraler Server, Suchanfragen werden vielmehr von Rechner zu Rechner weitergeleitet. Die Teilnehmer des Gnutella-Netzwerkes werden infolgedessen als Servants bezeichnet, eine Mischung aus Server und Client. Beim Start wird eine Verbindung zu einem Server hergestellt, der eine Reihe gültiger IP-Adressen von gerade eingeloggten Gnutella-Servants gespeichert hat, mit denen das System im Bedarfsfall Dateien austauschen kann. Wenn sich somit ein Benutzer anmeldet, so schickt er einfach eine Meldung an „benachbarte“ Benutzer. Sucht man nun eine Datei, so „fragt“ man zuerst beim „Nachbarn“ nach. Dieser schickt die Meldung, ob er im Besitz der gewünschten Datei ist, zurück und sendet die Anfrage an seine „Nachbarn“ weiter, die identisch vorgehen (Schneeballprinzip). Nach einer Weile sollte man eine Liste von Benutzern haben, die die gesuchte Datei besitzen, und kann die Daten direkt herunterladen. Aufgrund der dezentralen Struktur ist es praktisch unmöglich, ein Gnutella–Netzwerk auszuschalten, wie das bei Napster noch möglich war.[227]

2.3.3.2.3 Fasttrack-Modelle

Fasttrack arbeitet nach einem ähnlichen Prinzip wie Gnutella. Beide Technologien funktionieren dezentral. Während bei Gnutella alle Benutzer sowohl als Server als auch als Client fungieren, wird das Netz bei Fasttrack in so genannte Nodes und Superpeers unterteilt. Als Nodes gelten alle Benutzer, welche zwar nach Daten suchen und Daten anbieten, die aber keine Suchanfragen weiterleiten (im Gegensatz zu den Superpeers, welche zusätzlich Suchanfragen weiterleiten). Beim Einloggen meldet sich der Benutzer bei einem zentralen Server an, der bestimmt, ob man als Node oder Superpeer fungiert (abhängig davon, wie leistungsfähig die Rechenleistung des Computers und wie hoch die Netzwerkanbindung ist), und den Nutzern die Adressen der „benachbarten“ Teilnehmer mitteilt.[228] Damit eine Suche möglich ist, muss jeder Node eine Liste mit den zur Verfügung gestellten Daten an den Superpeer schicken, so dass dieser bei einer Anfrage weiß, ob die an ihn angeschlossenen Nodes die gesuchten Daten

[227] http://bolug.uni-bonn.de/wissen/schugt_gnutella/?printer (zuletzt abgerufen am 10.06.2004).
[228] http://www.kom.tu-darmstadt.de/~birck/workingArea/fasttrack/node1.html (zuletzt abgerufen am 10.06.2004).

besitzen. Bei der Suche nach Daten schickt man die Anfrage an den Superpeer, der die Suche an die anderen Superpeers weiterleitet. Das Herunterladen funktioniert wie bei anderen P2P-Varianten: Die Datei wird direkt von einem Node zu einem anderen transferiert. Durch diese Aufteilung in Node und Superpeer ist ein Fasttrack-Netzwerk v.a. bei einer großen Anzahl Nutzern leistungsfähiger als ein Gnutella-Netzwerk, denn die Suchanfragen, welche abhängig von der Zahl der Benutzer eine hohe Bandbreite benötigen können, gehen nur noch über die „schnellen" Superpeers, wodurch ein Benutzer mit einer „langsamen" Internetanbindung nicht das ganze Netz lahm legen kann.[229] Noch zu erwähnen sei, dass der Login-Server den einzigen zentralen Teil darstellt. Dieser koordiniert nur den Anmeldeprozess und ist für ein weiteres Funktionieren des Netzes nicht erforderlich. Wird der Server entfernt, so muss jeder Nutzer selbst ermitteln, wer die „benachbarten" Teilnehmer sind. Gelingt dies, so kann das Netz in gleicher Weise wie vorher genutzt werden. Aus diesem Grund kann man Fasttrack-Netzwerke nicht auf dieselbe Art ausschalten wie zentrale P2P-Systeme nach dem Zentralen Datenbank-Modell.

2.3.3.3 Urheberrecht und Software

Jährlich gehen der Musikindustrie viele Milliarden Euro durch Softwarepiraterie verloren.[230] Gemeint ist damit die illegale Verbreitung und/oder das Raubkopieren von Software für private und geschäftliche Zwecke. Raubkopien sind Vervielfältigungen eines Programms, die von dem Lizenzgeber weder ausdrücklich noch konkludent erlaubt worden sind.[231] Software ist leicht kopierbar, weil sie immer digital vorliegt. Das bedeutet, dass jede Kopie nicht mehr vom Original unterscheidbar und genauso nutzbar ist. Bei analogen Medien wie Schallplatten oder Büchern ist das Kopieren immer mit einem Verlust an Qualität verbunden. Die Digitalisierung auch dieser Bereiche durch CDs, ebooks usw. führt dazu, dass das (unerlaubte) Kopieren auch hier immer einfacher wird.

Nicht jede Software muss jedoch gekauft werden. Viele Softwarearten werden kostenlos programmiert. Zumeist handelt es sich dabei um jüngere Programmierer, die ihre Software der Internetgemeinschaft umsonst zur Verfügung stellen. Als Gegenbewegung zur kommerziellen Software haben sich dabei große Gemeinschaften wie die Linux-Community gebildet. Die Ursprünge der Internetgemeinschaften werden in der Hackerkultur gesehen. Im folgenden

[229] Ebd.
[230] http://global.bsa.org/germany/presseecke/2001/Bs061-11.html (zuletzt abgerufen am 10.06.2004).
[231] Meier 1992, S. 657.

Abschnitt werden die oft zu Verwirrung führenden Fachausdrücke kurz definiert und erklärt. Anschließend werden Formen der Software-Piraterie dargestellt.

2.3.3.3.1 Software-Arten

2.3.3.3.1.1 Kommerzielle Software

Kommerzielle Software ist Software, die von einem Unternehmen mit dem Ziel entwickelt wird, aus der Benutzung dieser Software Profit zu ziehen. Dazu gehören Produkte wie Microsofts Word, Excel, PowerPoint oder auch Photoshop und Pagemaker von Adobe. In die Source-Codes dieser Programme darf nur bedingt Einsicht genommen werden. Heute unterliegt kommerzielle Software automatisch dem Urheberschutz, zum Teil ist Software auch patentierbar. Das Kopieren und die Weitergabe (falls nicht vertraglich ausdrücklich erlaubt) von kommerzieller Software ist gemäß dem allgemeinen Urheberrecht verboten (bzw. dem Rechtsinhaber vorbehalten).

2.3.3.3.1.2 Open-Source Software

GNU[232], BSD[233], Mozilla[234], Apache[235] und viele mehr sind die Bezeichnungen für Software, die in den letzten Jahren eine neue Ära im Umgang mit Softwareprodukten und Software-Know-how einläuteten. Geheimhaltungsvereinbarungen bezüglich Softwarecodes sind vorbei. Am Markt gewinnt nicht der Eigentümer eines Produkts (Inhaber der Urheberrechte), sondern derjenige, der mit dem Softwareprodukt und den Marktbedürfnissen entsprechend umgehen kann. Wer den Source-Code seiner Software öffentlich zugänglich macht (sein Softwareprodukt als Open-Source deklariert), beschreitet neue Wege. Er macht über das Internet für alle Nutzer das so genannte Engineering seiner Software möglich und stellt sich den Diskussionen der News-Groups. Zudem schafft er dem Produkt die Möglichkeit, dass es weltweit eingesetzt

[232] Das GNU-Projekt wurde 1983 begonnen, um ein vollständiges Unix-artiges Betriebssystem zu entwickeln. GNU ist eine rekursive Abkürzung von „GNU is Not Unix!“ (http://www.gnu.org).
[233] BSD steht für Berkeley Software Distribution, die Weiterentwicklung von UNIX durch die Computer Systems Research Group (CSRG) an der University of California, Berkeley (UCB)
[234] Mozilla ist ein Open-Source Web Browser, der hauptsächlich für Web-Entwickler geschrieben wurde (http://www.mozilla.org).
[235] Apache ist ein kostenloser Open-Source Webserver, der weltweit am meisten verbreitet ist, da er sehr leistungsfähig und stabil läuft.

und weiterentwickelt werden kann, sowie sich gegenüber anderer, insbesondere kommerzieller Software am Markt zu behaupten und vielleicht sogar durchzusetzen.[236]

2.3.3.3.1.3 Freeware

Freeware hat keine allgemein akzeptierte Bedeutung. Man versteht jedoch darunter Software, die kostenlos verteilt oder aus dem Internet herunter geladen werden kann, aber nicht geändert werden darf und deren Source-Code nicht erhältlich ist.[237] Beispiele für solche Freeware sind der Acrobat Reader (Adobe) zum Lesen und Ausdrucken von PDF-Dateien[238] oder der Flash Player (Macromedia), um Webseiten, die auf Flash-Animationen aufgebaut sind, anzuschauen. Der rechtliche Rahmen wird durch individuelle Lizenzbestimmungen festgelegt (am Beispiel vom Acrobat Reader: http://www.adobe.com/products/acrobat/acrreula.html) und muss z.B. beim Herunterladen durch einen Mausklick bestätigt werden. Da aber jedermann kostenlos zu Freeware kommt, sind Probleme wie unerlaubtes Kopieren, wie das bei der kommerziellen Software der Fall ist, kaum vorhanden. Zudem ist der Source-Code ein offener Standard, und folglich hat niemand ein Interesse daran, den Source-Code zu ändern und als neue Software (nicht mehr dem Standard entsprechend) zu verkaufen.

2.3.3.3.1.4 Public Domain Software

„Public Domain“ ist ein Rechtsbegriff, der vor allem in den USA gebraucht wird. Software, die „Public Domain“ ist, unterliegt nicht dem Urheberrecht. Public Domain Software hat eine interessante rechtsgeschichtliche Entwicklung. In den USA wurden Softwareprojekte an Universitäten mit öffentlichen Mitteln gefördert. Die so geförderte Software durfte nicht verkauft werden, sondern gehörte der Allgemeinheit. Diese Idee fand auch Anklang im privaten Bereich. Viele Programmierer stellten ihre Software daraufhin ebenfalls als Public Domain Software zur Verfügung. Der Entwickler gibt das Copyright an seinem Programm auf und stellt es kostenlos der Allgemeinheit zur Verfügung. Jeder darf das Programm beliebig kopieren, weitergeben und sogar verändern. Allein die kommerzielle Verwertung bleibt untersagt.[239]

---

[236] www.wissen.de
[237] Ebd.
[238] Portable Document Format (PDF) ist ein offener Standard für die weltweite Distribution von Dokumenten in elektronischer Form.
[239] http://www.glossar.de/glossar/index.htm (zuletzt abgerufen am 10.06.2004).

2.3.3.3.1.5 Shareware

Shareware ist kommerzielle Software, die zunächst einmal für eine Testzeit benutzt werden darf, ohne dass dafür bezahlt werden muss. Erst wenn man sich dazu entschließt, das Programm dauerhaft zu benutzen, erhält der Urheber eine finanzielle Entschädigung. Da Shareware rechtlich gesehen gleich zu behandeln ist wie kommerzielle Software, unterliegt auch sie den Bestimmungen des Urheberrechts, wobei je nach Lizenzvertrag gewisse Abweichungen möglich sind.[240]

2.3.3.3.2 Arten der Software-Piraterie

Software-Piraterie ist das illegale Kopieren, Reproduzieren, Verwenden oder Herstellen von Software-Produkten.[241] Eine Raubkopie bezeichnet die illegale Vervielfältigung urheberrechtlich geschützter Software.[242] Hierbei können Handbücher, Datenträger, Aufschriften, Filme, Musikstücke, E-Books, Computerprogramme, ganze Datenbanken, Lizenzverträge und sogar Echtheitszertifikate gefälscht werden. Aber auch die bloße Vervielfältigung von Datenträgern (CD oder Diskette) oder sonstigen geschützten Bestandteilen eines Originalpakets ist denkbar, wenn hierfür nicht die erforderliche lizenzvertragliche Erlaubnis vorliegt.[243]

2.3.3.3.2.1 Lizenzmissbrauch

Oft kommt es gerade bei Unternehmen vor, dass eine gekaufte und offiziell registrierte Version eines Softwareprodukts mehr als nur einmal verwendet wird. Hierbei wird die Software zum Beispiel gleich auf mehrere Rechner installiert oder gar im Netzwerk betrieben, obwohl dies in der gekauften Lizenz nicht ausdrücklich vorgesehen ist. Viele Unternehmen nutzen diese Möglichkeit, um Kosten zu sparen. Da zumeist nur eine Lizenz gekauft wurde, wird

[240] http://de.wikipedia.org/wiki/Shareware (zuletzt abgerufen am 10.06.2004); eine spezielle Form der Shareware stellt Crippleware dar. Sie ist wie Shareware zu benutzen, allerdings mit eingeschränkter Funktionalität. Zum Beispiel lässt sich ein Dokument nicht drucken oder speichern, die Dimensionierung von Feldern oder Datensätzen könnte stark reduziert sein, oder besondere Zusatzfunktionen sind nicht aktiv. Nach einer bestimmten Zeit kann die Software auch den Dienst verweigern. Das Ganze hätte dann nur Demonstrationscharakter und soll zum Erwerb der Vollversion animieren.
[241] http://www.net-lexikon.de/Software-Piraterie.html (zuletzt abgerufen am 16.06.2004).
[242] http://www.net-lexikon.de/Raubkopie.html (zuletzt abgerufen am 16.06.2004); das Wort Raubkopie ist eigentlich eine sich selbst widersprechende Bezeichnung. Raub ist gewaltsames Wegnehmen, bei einer Kopie dagegen bleibt das Original bei seinem Besitzer. Im Fall der illegalen Kopie unterbleibt die Bezahlung des Urhebers oder des Rechteinhabers, die beim Kauf einer legalen Kopie erfolgt wäre. Nach dem Urheberrecht wird als Raubkopie eine unrechtmäßig erstellte Kopie von Daten bezeichnet.
[243] http://www.microsoft.com/oem/deutsch/risk.asp (zuletzt abgerufen am 16.06.2004).

hiermit ein halblegaler Zustand suggeriert, denn die mehrfache Nutzung einer einzigen Lizenz unterliegt dem Verbot und ist strafbar.

Im Gegensatz zur Mehrfachnutzung werden Lizenzen oft auch durch eine falsche Angabe von Vertragsbedingungen missbraucht: Dies ist zum Beispiel der Fall, wenn der Käufer einer Lizenz angibt, er wäre noch Student, jedoch in Wirklichkeit bereits seit einigen Semestern nicht mehr studiert. Auch die Nutzung nach Vertragsende bzw. Lizenzende zählt zu den Missbrauchsformen. So wird durch die Zurückstellung der Rechneruhr oft ein längerer Einsatz einer Software ermöglicht, deren Lizenz schon lange ungültig geworden ist. In vielen Fällen ist auch die Nutzung einer Software strafbar, wenn diese anders genutzt wird als vereinbart: So dürfen mit den meisten Schülerversionen von Programmiersprachen zum Beispiel keine kommerziellen Produkte hergestellt und vertrieben werden.[244]

2.3.3.3.2.2 Produktmanipulation

Unter einer Produktmanipulation, auch Counterfeiting genannt, versteht man die Veränderung der überlassenen Programme oder Komponenten. Die Einzelhandelsversionen von Software-Produkten bestehen üblicherweise aus der Originalverpackung, dem Computerprogramm, einem Handbuch, dem Endnutzerlizenzvertrag, der jedoch je nach Produkt auch online erhältlich sein kann, sowie zum Teil einem Echtheitszertifikat. Dies ist vielen Kunden nicht bekannt und eröffnet Software-Händlern zahlreiche Manipulationsmöglichkeiten. So werden die Bestandteile der Softwarepakete einzeln verkauft. Aus einem Originalprodukt werden dadurch mit großem Gewinn zahlreiche „neue Produkte“ generiert.[245]
Produkte des Herstellers werden ohne dessen Erlaubnis auf CDs oder andere selbstständig verkehrsfähige Datenträger kopiert. Dabei haben der Datenträger und/oder die Verpackung eine verblüffende Ähnlichkeit mit dem Originalprodukt. Auch originale Komponenten werden teilweise mit gefälschten kombiniert. In diesen Fällen handelt es sich um eine Teilfälschung. Produktmanipulationen findet man aufgrund der hohen Gewinne und der zunehmenden Fälschungssicherheit von Software immer häufiger. Oft werden die manipulierten Produkte als so genannte „OEM-Versionen“[246] verkauft, um die veränderte Erscheinungsform zu

[244] http://www.edv-feick.de/beratung/softwarepiraterie/hauptteil_softwarepiraterie.html (zuletzt abgerufen am 16.06.2004).
[245] Ebd.
[246] Original Equipment Manufacturer (Hersteller originaler Geräte od. Einrichtungen), Verfahren, bei dem ein Hersteller Originalgeräte anderer Unternehmen in seine Geräte oder Produkte integriert und unter seinem eigenen Namen in den Handel bringt.

rechtfertigen.[247] Zudem wird Software, die als Demoversion oder Update vorliegt, durch so genannte Cracks manipuliert. Das Programm wird hierbei so geändert, dass die Software sich verhält, als sei sie eine funktionsfähige Version des Originals.[248]

2.3.3.3.2.3 Compilation-CD

Eine Compilation-CD ist die Zusammenstellung von Softwarepaketen zu einer großen CD mit verschiedenen Raubkopien. Es werden hierbei so genannte Software-Sampler erstellt, die die Software vieler Hersteller enthält. Das Phänomen der Compilation-CD hat vor allem seit 1995 massiv an Bedeutung gewonnen. Zu diesem Zeitpunkt kamen erstmals kostengünstige CD-Brenner auf den Markt, welche die Erstellung von Compilation-CDs vereinfachten. Bei der Compilation-CD findet man unterschiedliche Varianten, von der goldenen CD-R (Recordable CD) bis hin zur professionell hergestellten silbernen CD-ROM (Read-Only Memory CD).

2.3.3.3.2.4 Hard Disk Loading

Beim Verkauf von Hardware wird vom Händler die Software auf die Festplatte gespielt und dabei dem Kunden nicht der Originaldatenträger mit Seriennummer, Lizenzvereinbarung und das dazugehörige Handbuch ausgehändigt. In einem solchen Fall hat der Händler eine unerlaubte Vervielfältigung durchgeführt und damit gegen das Urheberrecht verstoßen. Der Kunde hat keine Lizenz zur Nutzung dieser Software erworben. Software-Hersteller schließen teilweise auch OEM-Vereinbarungen mit Hardware-Herstellern, d.h., die Software wird dann vom Hardware-Hersteller oder vom Händler mit Erlaubnis des Software-Herstellers auf die Festplatte gespielt. Dem Kunden werden auch die oben genannten Unterlagen ausgehändigt. Dann nutzt der Kunde die Software rechtmäßig.

2.3.3.3.2.5 Internet-Piraterie

Der Begriff Internet-Piraterie beschreibt das illegale Downloaden oder den Vertrieb gefälschter Software über das Internet.[249] Der Download ist illegal, wenn keine entsprechende Ver-

[247] http://www.edv-feick.de/beratung/softwarepiraterie/hauptteil_softwarepiraterie.html (zuletzt abgerufen am 16.06.2004).
[248] Ebd.
[249] Ebd.

einbarung mit dem Urheber vorliegt. Der Softwarenutzer braucht also auch hier immer eine eigene Lizenz. Die Facetten von Urheberrechtsverletzungen, mit denen sich die internationalen Ermittler der Software-Verbände im Internet konfrontiert sehen, sind vielfältig. Sie reichen von kostenlosen Angeboten über so genannte Warez-Sites, Tauschbörsen oder E-Mails bis zum einfachen Herunterladen neuer Anwendungssoftware. Letzteres geschieht entweder direkt über gängige Browser von speziellen FTP-Webseiten oder indirekt anhand von Seriennummern, die für die gewünschte Programm-Installation erforderlich sind. Diese Seriennummern können mittels so genannter Cracks gefälscht werden. Dabei handelt es sich um Miniprogramme, die auf Conventionseiten zum Download zur Verfügung stehen und unter anderem zur Umgehung des Kopierschutzes genutzt werden. Sie überwinden unerlaubt den Kopierschutz oder die Zugangsberechtigung zu urheberrechtlich geschützter Software und kopieren das Programm in ein Software-Verzeichnis, um dort bestehende Dateien zu verändern oder zu überschreiben. Mit Hilfe von Cracks lässt sich zudem die zeitlich begrenzte Nutzung der Shareware überlisten.

Daneben werden Programme über Warez-Seiten bereitgestellt, die oftmals pornographisches Material beinhalten und den Traffic über entsprechende Banner an andere Seiten weiterleiten. Warez gehört zu den zehn häufigsten Suchbegriffen und ist bei Internet-Piraten sehr populär. Gibt man den Begriff bei einer Internet-Suchmaschine ein, erhält man unzählige Webseiten mit einer riesigen Auswahl an Software-Programmen.
Neben diesen kostenlosen Angeboten wird illegale Software auch vermehrt über Onlineauktionen angeboten: Sowohl oft unwissende Verbraucher als auch professionelle illegale Anbieter nutzen Onlineauktionen als Plattform, um ihre Produkte zu verkaufen. Oftmals verbirgt sich hinter einem vermeintlichen Schnäppchen ein illegales Produkt und hinter dem Verkäufer ein unseriöser Handelspartner.[250]

2.3.3.3.3 Urheberrecht und WWW

2.3.3.3.3.1 Texte, Bilder und Layouts

Das WWW umfasst im Allgemeinen vor allem Texte und Bilder. Daneben wird es jedoch auch durch das jeweilige Layout unterschiedlich gestaltet. Texte, Bilder und das Layout unterliegen ebenfalls urheberrechtlichen Schutzbestimmungen.

[250] http://www.edv-feick.de/beratung/softwarepiraterie/hauptteil_softwarepiraterie.html (zuletzt abgerufen am 16.06.2004).

Die Browser sind heutzutage, was den Benutzerkomfort angeht, sehr ausgereift. So lassen sich Webseiten mit wenigen Mausklicks speichern oder drucken, einzelne Textpassagen können markiert, kopiert und direkt weiterverwendet werden, Bilder können ebenfalls einfach gespeichert oder in eigene Dokumente eingebunden werden. Die Zugänglichkeit des WWW erlaubt den Zugriff auf unermessliche Datenmengen, die einfache Bedienung der Browser fördert das bedenkenlose Kopieren dieser Daten.

2.3.3.3.3.2 Programmcodes und HTML

Rechtsverstöße, die sich im Zusammenhang mit Software und dem dazugehörigen Programmcode ergeben, wurden bereits diskutiert. Dennoch soll hier noch einmal kurz auf das Thema eingegangen werden. Im Wesentlichen kann im WWW zwischen serverseitigen und clientseitigen Programmen unterschieden werden. Die serverseitigen Programme, die in Sprachen wie Java, Perl, PHP oder ASP verfasst sind, werden auf dem Server ausgeführt, der User bekommt nur das Resultat eines Programmaufrufs, meist in Form einer HTML-Seite zu sehen. Da der Nutzer nicht ohne weiteres an den Quelltext der serverseitigen Programme gelangen kann, ist hier die Gefahr von Urheberrechtsverletzungen gering.

Anders verhält es sich bei clientseitigen Programmen, wie Javascripten und HTML-Dokumenten. Diese werden auf den Rechner des Users heruntergeladen und dort lokal ausgeführt bzw. dargestellt. Der gesamte Quellcode kann mit jedem Browser eingesehen und dementsprechend auch kopiert werden.

HTML wird oft als Programmiersprache deklariert, in Wirklichkeit ist es aber eine so genannte Auszeichnungssprache (engl. Markup Language, in der vollen Länge Hypertext Markup Language). Bei einem HTML-Dokument handelt es sich um ein spezielles Textdokument, ein Hypertext-Dokument. Ein Hypertext-Dokument enthält neben dem eigentlichen Inhalt auch Elemente, die seine Struktur definieren. Diese so genannten Tags sind im Fall von HTML zum Beispiel <h1></h1> für eine Überschrift, für einen Absatz. Wesentliche Elemente, die eine Programmiersprache ausmachen und den Programmfluss definieren, sind jedoch nicht vorhanden.[251] Das bedeutet, dass sich die HTML-Dokumente eigentlich im Be-

[251] So fehlen HTML zum Beispiel Schleifen (for, while: mehrfaches Ausführen einer Instruktion) oder Bedingungen (if, else: Ausführen einer Instruktion, falls gewisse Bedingungen zutreffen).

reich von Textwerken bewegen und deshalb im Prinzip urheberrechtlichem Schutz unterliegen, auch wenn ein Urheberrecht (noch) keine Regelungen für Software enthält.

2.3.3.3.3.3 Deep-Linking

Der Hypertext zeichnet sich durch die Verlinkung einzelner HTML-Dokumente aus. Diese Verlinkung bringt aber auch urheberrechtliche Probleme mit sich. Unter Deep-Linking versteht man das Setzen eines Links von einer Seite in einer Domain auf eine Seite in einer anderen Domain, wobei der Link nicht auf die Hauptseite der Domain, sondern auf eine der Unterseiten zeigt. Dies ist an sich in den meisten Fällen nicht problematisch, im Gegenteil, die Idee besteht darin, möglichst direkt zu der gewünschten Information zu linken. Anders verhält es sich jedoch, wenn so viele Links von einer Domain zu einer Informationssammlung auf einer anderen Domain erstellt werden und die Daten den Nutzern der ersten Domain mehr oder weniger direkt zur Verfügung stehen, so dass dieser die fremden Webseiten wie seine eigenen nutzt. Inwieweit ein solches Deep-Linking urheberrechtliche Bestimmungen verletzt, ist in Deutschland bislang noch ungeklärt. Es gibt jedoch amerikanische Fälle, in denen es wegen exzessiven Deep-Linkings zu Prozessen kam. Am 28. April 1997 reichte der Online-Ticket-Händler Ticketmaster beim U.S. District Court for the Central District of California Klage gegen Microsoft ein. Microsoft hatte von seiner Microsoft Sidewalk-Seite, die Informationen zu verschiedenen amerikanischen Städten bietet, direkt zu den jeweiligen Event-Beschreibungen auf Unterseiten von www.ticketmaster.com gelinkt. Ticketmaster argumentierte, dass Microsoft sich der Daten bediene, die Ticketmaster mit erheblichem Aufwand zusammenstelle. Der Rechtsstreit wurde am 22. Januar 1999 durch einen Vergleich zwischen Microsoft und Ticketmaster gelöst. Microsofts Sidewalk linkte in der Folge nicht mehr zu Ticketmaster.

2.3.4 Zeitdiebstahl

Unter dem unzutreffenden Begriff „Zeitdiebstahl“ wird das Ausnutzen von Rechenressourcen auf fremden Rechnern zusammengefasst. Zeitdiebstahl ist das unberechtigte Verwenden von fremden Rechnern oder fremder Software. Der Täter stiehlt dabei den Wert der Nutzungseinheit für den Computer, um eigene Kosten einzusparen.[252] Der Begriff rührt daher, dass vielfach der Gebrauch der Computer bezahlt werden muss bzw. abgerechnet wird, und dabei als

[252] http://www.lexexakt.de/glossar/zeitdiebstahl.php (zuletzt abgerufen am 22.06.2004).

Maß die verbrauchte Rechenzeit herangezogen wird. In den Intranets der 1970er-Jahre geschah Zeitdiebstahl meist durch Angestellte eines Unternehmens oder einer Behörde, die auf den Rechnern eigene Programme laufen ließen. Meist waren dies lediglich Spiele oder kleine Anwendungen.[253] Heutzutage können Hacker und andere Personen zum Täterkreis dazugezählt werden, die von außen die Rechnerleistungen zu eigenen Zwecken unberechtigt ausnutzen. Dabei muss vor allem das Verschicken von Spam-Nachrichten von fremden Rechnern aus hervorgehoben werden.

Allerdings stellt Zeitdiebstahl keinen Diebstahl nach § 242 StGB dar, da keine beweglichen Sachen entwendet werden, sondern nur unbefugt Hard- und Software genutzt werden. Es kann also höchstens § 266 StGB (Untreue) Anwendung finden. Dazu müsste aber ein Pflichtverhältnis zwischen dem Besitzer der Hard- bzw. Software und dem Nutzer bestehen, sowie die Nutzung vorsätzlich mit dem Ziel erfolgen, das Vermögen des Besitzers zu schädigen.[254] Andererseits käme auch das Erschleichen von Leistungen gem. § 265a StGB als Deliktform in Betracht.

Durch die hohen Rechenleistungen und die vielfach genutzten Standleitungen verliert diese Art der Computerkriminalität aber zunehmend an Bedeutung und soll daher auch hier nicht weiter behandelt werden.[255]

2.3.5 Harte Pornografie

In den letzten Jahren wurde der Vertriebsweg via Internet sehr populär. Dieser bietet nämlich die Möglichkeit, kinder- und tierpornografisches Material, seien es Fotos oder Filme, digital über Datennetze zu verbreiten. Diese Bilder und Videosequenzen werden dann in so genannten Newsgroups und Chaträumen angeboten und getauscht oder auf Webseiten, geschützt durch Passwörter, im Tausch gegen anderes kinderpornografisches Material freigegeben.[256] Derzeit fungiert das Netz hauptsächlich als Tauschbörse von kinderpornografischem Material oder als Austauschstelle von Kontaktadressen für den späteren Handel außerhalb des Netzes.[257] Dabei ist (Kinder-)Pornografie kein Phänomen seit der Entstehung des Internets; doch haben dessen neue Techniken auch neue Dimensionen und Gefährdungslagen geschaffen: Sowohl Verteiler als auch Abnehmer können (relativ) anonym bleiben. Ein Postversand oder

[253] http://md.hudora.de/jura/rechtstatsachen/node15.html#SECTION00331000000000000000 (zuletzt abgerufen am 22.06.2004).
[254] http://members.fortunecity.de/geniuz/text/book/node11.html (zuletzt abgerufen am 22.06.2004).
[255] http://irb.cs.uni-magdeburg.de/bs/lehre/wise0304/ds/folien/vds09-03-1.pdf (zuletzt abgerufen am 22.06.2004).
[256] Janovsky, 1998 S. 502.
[257] Wiedemann 2000, S. 232f.

stationäre Händler müssen nicht in Anspruch genommen werden; der Zugriff auf inkriminierte Inhalte ist mit praktisch jedem handelsüblichen PC und Modem oder ISDN-Karte möglich.[258]

Kinderpornografie steht folglich heutzutage im engen Zusammenhang mit dem Internet. Die Kommunikations- und Verbreitungsformen pädophiler Täter erfolgen über Chat-Rooms, E-Mails und Newsgroups, die im Folgenden näher dargestellt werden.

2.3.5.1 Newsgroups

Eine Newsgroup ist eine Diskussionsgruppe im Usenet.[259] Newsgroups werden wie schwarze Bretter genutzt. Dort kann jeder Benutzer einen Beitrag veröffentlichen oder andere Beiträge lesen.[260] Das Benutzen der Newsgroups ist grundsätzlich sehr effektiv, um schnell nützliche Informationen zu erlangen oder zu erfragen. Allerdings kommt es hier immer öfter dazu, dass die Pädophilen so genannte Postings anhängen und somit das System der Newsgroups für deren illegale Handelungen ausgenutzt wird. Postings sind Dateien, die Bilder oder Videos enthalten, die sich dann jeder Internetnutzer auf seinen heimischen Rechner laden kann.

2.3.5.2 Chat-Rooms und IRC

Zusätzlich bieten viele Internetdienstleister die Möglichkeit, eigene Chat-Rooms[261] zu eröffnen. Diese müssen nur noch unzweideutige Namen erhalten, und schon tauchen innerhalb weniger Minuten die ersten Pädophilen in diesem Raum auf und tauschen Bilder in Bruchteilen von Sekunden per E-Mail. Aber nicht immer haben Chat-Rooms so eindeutige Namen. Es gab Tauschhandel von kinderpornographischem Material in Chat-Rooms mit Namen wie

---

[258] Graf 1999, S. 281 ff.

[259] Das Usenet (urspr. Unix User Network) ist ein weltweites elektronisches Netzwerk, das aus Diskussionsforen besteht und an dem jeder, der über das Internet Zugang zu einem Newsserver hat, teilnehmen kann.

[260] Newsgroups werden auch als Discussion Groups, Bulletin Board oder Area bezeichnet. Benutzer können in bestehenden Newsgroups Nachrichten veröffentlichen (posten) und die Postings anderer lesen, auf vorherige Beiträge antworten oder auch neue Newsgroups einrichten. Newsgroups sind hierarchisch nach Themen gegliedert, wobei die ersten (drei oder vier) Buchstaben eines Newsgroup-Namens die Kategorie des Haupthemas angeben. Unterkategorien werden mit dem Namen des jeweiligen Unterthemas aufgeführt. Wichtige Hauptkategorien sind news (Nachrichten), rec (recreation, dt.: Freizeit, Erholung), soc (society, dt.: Soziales), sci (science, dt.: Wissenschaft) und comp (Computer).

[261] Chat (von engl. to chat, dt.: plaudern) ist die Bezeichnung für die innerhalb des Internets weit verbreitete Art der direkten Unterhaltung zwischen zwei oder mehreren Personen in Echtzeit. Es ist eine Art Computerkonferenz, die meist allerdings ohne Bilder auskommen muss. Stattdessen gebrauchen Teilnehmer, die zusammen chatten, neben dem geschriebenen Wort auch Ersatzbilder (Avatare, Emoticons). Oft wird in themenbezogenen Chaträumen gechattet. Fast immer besteht auch die Möglichkeit, zu zweit in einen privaten Chatraum zu wechseln.

„Bauernhof“, „Mutter und Tochter“ oder „Tierlieb“. Die Pädophilen erkennen sich in diesen Chat-Rooms meist anhand von für nicht Eingeweihte bedeutungslosen Schlüsselwörtern. Werden sie genannt, erfolgt der Tausch von Fotos durch von Dateiattachments per E-Mail, ohne dass jemand etwas bemerkt oder gar Verdacht schöpft.[262]

Eine Sonderform ist der Internet Relay Chat (IRC)[263], den z.B. der nach den Taten von Zandvoorten ermittelte und inzwischen von der Polizei aufgelöste Kinderpornoring nutzte. Ein großer Unterschied ist, dass IRCs nichtkommerzieller Art sind. Der IRC wird mit speziellen Programmen bedient, die im WWW frei heruntergeladen werden können. Das IRC-System wurde Ende der 1980er-Jahre von dem Finnen Jarkko Oikarinen entwickelt und verbreitete sich im Netz sehr schnell, da es die Möglichkeit bot, sich live via Computer zu unterhalten. Man muss bei der Kommunikation im IRC dem jeweiligen Gesprächspartner nicht seinen richtigen Namen preisgeben, sondern kann ein beliebiges Pseudonym wählen. Vorgeschrieben ist aber bei der Anmeldung, die erforderlich ist, um Zugang zum IRC zu erhalten, den richtigen Namen und die E-Mail-Adresse anzugeben. Eine Überprüfung dieser Daten findet jedoch zu keinem Zeitpunkt statt. Der Teilnehmer kann dann aus einer Vielzahl von Kanälen auswählen, an dem er teilnehmen möchte, oder er kann einen eigenen Kanal eröffnen, wodurch er Operator wird und bestimmte Rechte in der Gesprächsrunde hat. Dazu zählt, dass er bestimmte Teilnehmer aus dem Channel entfernen oder deren Teilnahme von bestimmten Bedingungen abhängig machen kann. So wird z.B. in kinderpornographischen Konferenzen die Teilnahme davon abhängig gemacht, ob der Teilnahmeanwärter Kinderpornos eingebracht hat oder einbringen kann.[264] Der IRC wird teilweise nur genutzt, um Kontakte herzustellen. Der Austausch des entsprechenden Materials findet dann wieder außerhalb des Internets, also im realen Leben statt. Professionelle Anbieter von Kinderpornos schicken getarnt als Anbieter kommerzieller Sexseiten oft auch mit ihren unerwünschten Werbe-E-Mails ein Probebild zur Adresse des Empfängers, so dass der Adressat unfreiwillig in den Besitz entsprechender Bilder kommt.

[262] Wiedemann 2000, S.232 f.

[263] Heute gibt es tausende voneinander unabhängige Netze. Große Netze mit gleichzeitig mehr als 100.000 verbundenen Clients sind QuakeNet, EFnet, IRCNet oder Undernet, kleinere heißen DALnet, Freenode, Blitzed oder NewNet. Die Netze unterscheiden sich in regionalen Schwerpunkten, Sprachen, Themen und angebotenen Services. Auch die Akzeptanz oder Toleranz gegenüber Sex und Kanälen für die Verteilung von Raubkopien spielt zunehmend eine Rolle.

[264] Wiedemann 2000, S.232 f.

2.3.5.3 E-Mail

Für die Pädophilen ist das Internet interessant, weil es ihnen ermöglicht, schnell an kinderpornografisches Material zu gelangen. Genutzt werden vorwiegend die Versandwege über E-Mail und nicht über eine Homepage, weil dort die Personen zu leicht feststellbar wären, während sie im E-Mail-/ Newsgroupbereich weitgehend anonym bleiben. Der E-Mail-Dienst wird häufig für Verbreitungshandlungen genutzt. Er stellt eine Form der Individualkommunikation dar, die einem die Möglichkeiten des weltweiten Nachrichtenaustauschs gibt. Nachrichten werden an einen definierten Empfängerkreis versandt, oder es werden sog. Mailinglisten erstellt, mit denen Rundschreiben verschickt werden. Es gibt inzwischen Hunderte von Unternehmen im Internet, die den Nutzern kostenlose E-Mail-Adressen anbieten. Hierzu ist es meist nicht notwendig, seine Personalien anzugeben, bzw. bei Angabepflicht von Personalien werden diese nicht auf Richtigkeit überprüft. Das einzige, das immer angegeben werden muss, ist ein beliebiger Name (Pseudonym) und ein Passwort, um die eigenen E-Mails vor unbefugten Lesern zu schützen. Genau diese Möglichkeiten werden von Pädophilen genutzt.

Der Bereich der illegalen Pornografie, speziell im Internet, ist ein derart großer und umfangreicher Bereich, dass dessen umfassende Besprechung den Rahmen dieser Arbeit sprengen würde. Harte Pornographie existierte schon vor der Entstehung des Internets, das lediglich ein neues Medium darstellt, welches von Kriminellen als bequemer und sicherer empfunden wird. Aus diesem Grund soll auf eine weitere und ausführliche Darstellung verzichtet werden.

2.3.6 Extremistische Propaganda

Schon frühzeitig haben insbesondere rechtsextremistische Täter begonnen, ihr Gedankengut über das Internet weltweit zu publizieren, und auf diese Weise Post- und Zollkontrollen bundesdeutscher Ermittlungsbehörden umgangen. Derzeit existieren mehr als 200 Homepages deutscher sowie über 300 Homepages ausländischer Rechtsextremisten. Auch soweit es sich um deutsche Täter handelt, speichern sie regelmäßig ihre Propaganda auf ausländischen Rechnern ab, um Ermittlungen zu erschweren. Daneben benutzt diese Tätergruppe das Internet auch zum schnellen und preisgünstigen internen Informationsaustausch, da einerseits per E-Mail Nachrichten mit geringem Aufwand an einen vorbestimmten Verteiler verschickt und

andererseits die elektronische Post zum Schutz vor eventuellen Überwachungsmaßnahmen sicher verschlüsselt werden kann.[265]

2.3.7 Cyberterror

Cyberterror ist eine neue Form des Terrorismus. Zum Teil wird Cyberterrorismus auch als Informationskrieg bezeichnet. Dies mag wohl damit zusammenhängen, dass heutzutage Terror und Krieg nur noch schwer voneinander zu unterscheiden sind. Cyberterror ist eine Bezeichnung für ein Sammelsurium aus verschiedensten computertechnischen Angriffen. Es können darunter alle Computerkriminalitätsformen im engeren Sinne fallen wie Computerviren, Trojaner, logische Bomben und DDoS-Angriffe.[266] Cyberterroristen arbeiten aus großer Entfernung, anonym, und ihre Angriffe haben auch negative Auswirkungen auf die Ökonomie. Ziel der Cyberterroristen ist es, zu stören, zu manipulieren, Betriebe und staatliche Einrichtungen auszuspionieren. Ziele dieser Terroristen sind unter anderem Kommunikations- und Steuerungszentren, das Verkehrswesen und die IT-Infrastruktur. Um dem Cyberterrorismus zu begegnen und mit denselben Mitteln agieren zu können, forscht die amerikanische Armee nach Cyber-Angriffstechnologien. Dabei handelt es sich um elektronische Attacken auf die digitale Kommunikation, mit denen die Täter bezwecken, gezielt Netzwerke zu stören oder zu manipulieren und so den Gegner täuschen zu können.[267] Dabei sind zivile Einrichtungen ebenfalls betroffen. Im Kosovokrieg im Jahre 1999 soll Bill Clinton die CIA ermächtigt haben, elektronisch in Banken in Russland, Zypern und Griechenland einzubrechen, um sämtliche Auslandskonten Milosevics zu leeren.[268] Genauso soll es der amerikanischen Regierung möglich sein, die Konten von Osama Bin Laden zu löschen.[269]

2.3.8 Sonstige Delikte

Erpressung, Bedrohung über E-Mail, Menschenhandel, Verabredung von Straftaten, Sprengstoffdelikte in Form von Anleitungen, Gewaltdarstellungen, Betäubungsmittelverstöße, Waffenhandel und alle anderen Delikte könnten auch zu den Computerdelikten im weiteren Sinne zählen, sind jedoch heutzutage noch nicht derart stark vom Computer beeinflusst, dass dies erforderlich wäre.

---

[265] Graf 1999, S.281 ff.
[266] Medosch/ Röttgers 2001, S. 163.
[267] Medosch/ Röttgers 2001, S. 166.
[268] Weitere Cyberattacken der Kriegsparteien findet man bei Power 2001 S. 227 ff.
[269] Medosch/ Röttgers 2001, S. 170.

2.4 Computerkriminalität im engeren Sinn

2.4.1 Manipulations- und Sabotagehandlungen

Unter Computermanipulation versteht man Datenveränderungen im EDV-Bereich, die der Täter mit dem Ziel vornimmt, das ordnungsgemäße Arbeitsergebnis einer Datenverarbeitungsanlage zu verändern.[270] Sabotagedelikte stellen hierbei die stärkste Form der Manipulation dar, weil damit die Vernichtung der Computerdaten verbunden ist.[271] Dabei kann aus technischer Sicht zwischen diesen beiden Handlungen nicht unterschieden werden, da hier ein fließender Übergang herrscht. Werden alle Daten komplett gelöscht, handelt es sich eindeutig um Sabotage. Wird die Datenverarbeitung verändert, ohne dass Daten gelöscht werden, handelt es sich eindeutig um Manipulation. In den meisten Fällen wird aber eine Datenverarbeitung dadurch manipuliert, dass Teile der ursprünglichen Software umgeschrieben und damit Teilbereiche für immer gelöscht werden. Erst hierdurch ändert sich der Vorgang der Datenverarbeitung in dem vom Täter gewünschten Teilbereich. Der übrige Vorgang bleibt aufgrund des unberührten Teils der Software gleich und verschleiert die eigentliche Tat. Aufgrund dieser häufigen Überschneidungen von Sabotage und Manipulation wird im Folgenden nicht zwischen diesen Handlungen unterschieden.

2.4.1.1 Viren und Würmer

Als die heute wohl bekanntesten und auch am meisten gefürchteten Sabotageakte gelten die Computerviren.[272] Diesbezüglich ist eine Professionalisierung auf Seiten der Urheber von Viren zu beobachten, die bei Ermittlungserfolg der Strafverfolgungsbehörden auch mit einer höheren Strafe rechnen müssen.[273] Laut Angaben eines führenden Anti-Viren-Herstellers werden ca. 30 neue Viren pro Tag entdeckt.[274]

Ein Computervirus ist eine Programmsequenz, die sich in ein Programm einpflanzt, um sich selbst zu reproduzieren, indem sie das Wirtsprogramm zur weiteren Verbreitung des virulen-

[270] Kaiser 1996, S. 878.
[271] Kaiser 1996, S. 877.
[272] Helmbrecht 2004.
[273] Gantar 2004.
[274] http://www.roli-online.de/article.php?sid=16 (zuletzt abgerufen am 15.08.2004).

ten Codes veranlasst.[275] In der Fachsprache ist ein Computervirus eine nicht selbstständige Programmroutine, die sich selbst reproduziert, indem sie sich an andere Computerprogramme oder Bereiche des Betriebssystems anhängt und, einmal gestartet, vom Anwender nicht kontrollierbare Manipulationen am Betriebssystem vornimmt.[276] Umgangssprachlich hat der Begriff Computervirus eine breitere Bedeutung: Er wird sowohl für Computerviren in der fachsprachlichen Bedeutung als auch für Computerwürmer benutzt. Computerwürmer sind den Computerviren konzeptionell sehr ähnlich. Die Abgrenzung besteht darin, dass ein Virus versucht, Dateien auf einem Computersystem zu infizieren, während ein Wurm versucht, eine Zahl von Computern in einem Netzwerk zu infizieren.[277] Zudem sind Computerwürmer im Gegensatz zu Viren eigenständige Programme und besitzen als Grundform keine Schadensroutine. Da heutzutage viele Würmer zusätzlich Viren sind, d.h. zusätzlich eine eigene Schadensroutine besitzen, verwischen die Grenzen zwischen beiden Programmtypen zunehmend und werden aus diesem Grund im Folgenden gemeinsam behandelt.

In den meisten Ländern ist das bloße Schreiben eines Virus noch nicht unter Strafe gestellt, während seine Verbreitung im strafrechtlichen Sinne oft strafbar sein kann. Die Gesetzgebung und Rechtsprechung unterscheiden sich jedoch von Staat zu Staat. In Deutschland ist das Schreiben eines Computervirus noch nicht strafbar. Das Schweizer Strafrecht stellt das Schaffen eines Virus unter Strafe, sofern damit eine Schädigungsabsicht verbunden ist. Auch Finnland hat im September 1999 ein Gesetz verabschiedet, das das Schreiben und Verfügbarmachen eines Virus unter Strafe stellt, selbst wenn niemand geschädigt wurde. Allein die Tatsache, dass eine Schädigung möglich ist, reicht für eine Verurteilung aus.[278] Die Regierung Sambias hat am 04.08.2004 einen Gesetzesentwurf vorgestellt, der für Hacker und andere Computer-Straftäter Haftstrafen von 15 bis 25 Jahren vorsieht.[279]

1988 gab es die erste Verurteilung in den USA. Robert Morris wurde zu drei Jahren auf Bewährung, 400 Stunden gemeinnütziger Arbeit und 10.000 US-Dollar Strafe verurteilt. Er hatte einen Internet-Wurm in Umlauf gebracht.[280] Ein anderer Virenautor, David Smith, schrieb den so genannten „Melissa-Virus“. Das Virus, das Smith nach einer Stripteasetänzerin benannt und im März 1999 in Umlauf gebracht hatte, infizierte mehr als eine Million Computer

[275] Voss 2004.
[276] http://de.wikipedia.org/wiki/Computervirus (zuletzt abgerufen am 15.04.2004).
[277] http://de.wikipedia.org/wiki/Computerwurm (zuletzt abgerufen am 15.04.2004).
[278] http://www.symantec.com/region/de/avcenter/rechtslage.html (zuletzt abgerufen am 15.08.2004).
[279] http://www.net-tribune.de/article/040804-07.php (zuletzt abgerufen am 22.08.2004).
[280] http://www.symantec.com/region/de/avcenter/rechtslage.html (zuletzt abgerufen am 15.08.2004).

und richtete weltweit einen Schaden von rund 1,2 Milliarden Dollar an. Nachdem ihn die Strafverfolgungsbehörden gefasst hatten, verurteilte ein Gericht in Newark im US-Bundesstaat New Jersey den 34 Jahre alten David Smith zu einer Haftstrafe von 20 Monaten und einer Geldbuße von 5000 US-Dollar. Das Gericht blieb mit seinem Urteil unter der möglichen Höchststrafe von fünf Jahren. Smith wurde nach US-Medienberichten seine umfangreiche Kooperation mit den Ermittlern angerechnet.[281] Laut der Zeitschrift Testticker vom 20. Juli 2004 wurde der 26-jährige spanische Virenprogrammierer Oscar Lopez Hinarejos zu zwei Jahren Gefängnisstrafe verurteilt.

Im September 2003 hat in den USA die Polizei im Zusammenhang mit den Blasterwurmvarianten einen Minderjährigen verhaftet. Erst Ende August 2003 hatte das FBI in Minnesota schon einen anderen 18-jährigen Teenager festgenommen. Er soll eine Variante des Blasterwurms in Umlauf gebracht haben. Nur wenige Tage später wurde auch ein 24-jähriger Student in Rumänien verhaftet. Ihm wird vorgeworfen, die Variante F des Wurms freigesetzt zu haben. Ende des Jahres 2003 konnte die Polizei einen weiteren Blasterautor ausfindig machen. Er soll in Verbindung mit der so genannten «RPCSDBOT»-Variante des Wurms stehen. Diese installiert gleichzeitig einen Trojaner auf dem Rechner des Anwenders. Laut Behörden ist der Festgenommene unter 18 Jahre alt.[282]

2.4.1.1.1 Historische Entwicklung

Es wird zunächst die geschichtliche Entwicklung der Computerviren dargestellt, um die rasante Veränderung der Übergriffe darzustellen. Da diese Arbeit die Kriminalität von Hackern darstellen möchte, deren Schwerpunkt unter anderem die Verbreitung von Computerviren und Computerwürmern ist, erscheint es für den Überblick und das allgemeine Verständnis wichtig darzustellen, in welche Richtung sich die Problematik entwickelt. Dabei wird versucht, die Schäden sowie die Raffinesse aufzuzeigen, mit der die Täter Viren programmieren. Bei den Virenprogrammierern handelt es sich um Personen, die in die Gruppe der Hacker eingestuft werden können. Wer die Täter im speziellen sind, ihre Altersstruktur oder Nationalität kann meistens nicht erörtert werden, da die meisten Virenautoren nicht gefasst werden.

In Jahr 1982 wurden im Xerox Alto Research Center die ersten Computerwürmer programmiert, welche für verteilte Berechnungen genutzt werden sollten. Allerdings schlich sich ein

[281] http://www.aktienboard.com/vb/archive/index.php/t-36502.html (zuletzt abgerufen am 15.08.2004).
[282] http://www.pctipp.ch/webnews/wn/25310.asp (zuletzt abgerufen am 26.08.2004).

Programmierfehler ein, welcher bewirkte, dass sich der Wurm unkontrolliert vermehren konnte. Das System brach kurz darauf unter der enormen Last zusammen.[283] 1984 veröffentlichte der Amerikaner Fred Cohen seine Doktorarbeit mit dem Titel „Computer Viruses -Theory and Experiments“. Da er insbesondere auf die Gefahren einging, die Computerviren für Rechner darstellen können, erregte seine Untersuchung auch internationales Aufsehen. Im Rahmen seiner Arbeit stellte er ein kleines selbstgeschriebenes Programm vor – den ersten lauffähigen Computervirus.[284] Mit diesem Programm realisierte er, was bis dahin nur als theoretische Möglichkeit galt, nämlich dass sich ein Computerprogramm tatsächlich selbst reproduzieren kann. Cohen ist auch die ürsprüngliche Definition des Begriffs Computer-Virus zu verdanken: „A ‘computer virus’ is a program that can ‘infect’ other programs by modifying them to include a possibly evolved version of itself.“[285]

Im Jahr 1986 tauchte dann der erste MS-DOS-Virus auf. Zwei pakistanische Software-Händler kamen auf die Idee, verseuchte Programme zu verkaufen, um ihre Kundschaft durch die kurz darauf fällig werdende Reparaturleistung an sich zu binden. Da sie dummerweise im Virencode ihre vollen Namen nannten, kam man ihnen schnell auf die Schliche. Kurioserweise verbreitete sich der „Pakistan-Virus (auch „Brain“ genannt) dennoch bis in die USA.[286] Mit dem Pakistan-Virus kamen unzählige weitere Viren in Umlauf. Es wurden unter anderem die Viren Vienna, Cascade, Stoned und Pingpong gefunden. Diese Viren waren recht einfach gebaut und konnten anhand fester Zeichenfolgen entdeckt werden, die im Programmcode zu finden waren. Häufig handelte es sich dabei um Viren, die zu irgendeinem bestimmten Zeitpunkt eine Meldung ausgeben sollten. Man brauchte also nur nach solchen Meldungstexten zu suchen, um den Virus zu entdecken.

Es dauerte nicht lange, bis die ersten Viren auftauchten, die den Viruscode verschlüsselten. Das hatte zur Folge, dass nach Textausgaben von Viren nicht mehr einfach gesucht werden konnte, da diese Texte jedes Mal anders verschlüsselt abgelegt wurden.

Im Jahr 1987 sorgten zwei neue Viren für Aufsehen: Der im Dezember an der Hebräischen Universität in Israel entdeckte „Jerusalem“-Virus gilt als erster Virus, der sich im Arbeitsspei-

[283] http://www.vhm.haitec.de/konferenz/1997/history.htm (zuletzt abgerufen am 30.03.2004).
[284] http://www.computerviren-info.de/Geschichte.htm (zuletzt abgerufen am 30.03.2004); http://www.etymologie.info/~e/_n/in-plan18.html (zuletzt abgerufen am 30.03.2004).
[285] http://sun.soci.niu.edu/~rslade/cohen.htm (zuletzt abgerufen am 30.03.2004).
[286] http://www.computerviren-info.de/Geschichte.html (zuletzt abgerufen am 30.03.2004); http://www.tariftip.de/rubrik/8738/1/Geschichte+der+Viren.htm (zuletzt abgerufen am 30.03.2004).

cher des Computers festsetzen konnte.[287] Er war einer der ersten wirklich bösartigen Viren. Begnügten sich Viren bisher damit, für ihre Verbreitung zu sorgen, Rechnerkapazität zu stehlen oder bestenfalls Meldungen auszugeben, wurde „Jerusalem“ programmiert, um Programme und Daten zu zerstören.[288] Er drang in Computer in den USA, Europa und im Mittleren Osten ein. Der Urheber kann für sich in Anspruch nehmen, den wohl ersten Computervirus entwickelt zu haben, dem in der Presse weltweit Aufmerksamkeit geschenkt wurde.[289] Im selben Monat entwickelten Studenten an der University of Wellington in Neuseeland den berühmten „Stoned“-Virus, der erste MBR-Virus (Master Boot Record), der auch Disketten befallen konnte.

Im Lauf der Zeit haben Virenprogrammierer immer wieder Techniken entwickelt, die Viren vor Entdeckung und Bekämpfung schützen. So gibt es Viren, die ihre Anwesenheit durch Manipulation von Verzeichniseinträgen tarnen (Stealth-Viren). Diese Viren nutzten spezielle Eigenschaften des Betriebssystems aus, indem bestimmte Systemaufrufe abgefangen und verfälscht ausgegeben wurden. So konnten diese Viren in einem infizierten System zum Beispiel die alte Programmlänge vortäuschen oder dem Benutzer statt bestimmter geänderter Sektoren der Festplatte die Originalsektoren vorspiegeln, die der Virus an eine andere Stelle verschoben hatte.

Im November 1988 legte der 22-jährige Robert Morris mit seinem selbstgeschriebenen Virus einige tausend Computersysteme in den USA lahm, darunter Rechner der NASA. Der angerichtete Schaden wurde auf annähernd 100 Mio US-$ geschätzt.[290] Der Virus befiel damals ca. 6.000 Computer, das waren 10 Prozent aller damaligen Computer im Internet.[291] In diesem Jahr wurde auch die erste Antiviren-Software und der erste Virusbaukasten (Virus Construction Kit) für den Atari ST veröffentlicht. Mit Hilfe dieses Werkzeugs konnten auch Anfänger einfach Viren mit vom Benutzer bestimmten Eigenschaften „zusammenbauen“.[292]

---

[287] http://www.symantec.com/region/de/avcenter/regeln_de.html (zuletzt abgerufen am 30.03.2004).
[288] Er wurde auch unter dem Namen Freitag-der-13.-Virus bekannt, da er an einen solchen Tag alle COM- und EXE-Dateien löschte. An allen anderen Tagen verringerte er nach etwa 30 Minuten die Rechnergeschwindigkeit. Heute gibt es etwa 500 Varianten dieses Virus.
[289] http://www.computerviren-info.de/Geschichte.html (zuletzt abgerufen am 30.03.2004).
[290] http://online.wdr.de/online/computer/computerviren/chronologie.phtml (zuletzt abgerufen am 30.03.2004); http://www.computerviren-info.de/Geschichte.html (zuletzt abgerufen am 30.03.2004).
[291] http://www.tariftip.de/rubrik/8738/1/Geschichte+der+Viren.htm (zuletzt abgerufen am 30.03.2004).
[292] http://online.wdr.de/online/computer/computerviren/chronologie.phtml (zuletzt abgerufen am 30.03.2004); http://www.vhm.haitec.de/konferenz/1997/history.htm (zuletzt abgerufen am 30.03.2004).

Besonders schwierig wurde es, als 1990 die ersten so genannten polymorphen Computerviren auftauchten.[293] So bezeichnet man Programme, die ihren Quellcode fortlaufend ändern können und daher schwierig zu identifizieren sind. Es wurde von dem Virenprogrammierer mit dem Synonym „Dark Avenger" eine erste Mutation Engine veröffentlicht. Dieses komplexe Werk kann als Grundbaustein eines polymorphen Virus dienen. Die Verschlüsselungsroutine ändert sich dabei genau so wie die Instruktionen, um den Virus zu entschlüsseln; die Länge ist ebenfalls sehr variabel.[294] Um einen derartigen Virus zu entdecken, genügt es nicht mehr, nur nach bestimmten Zeichenfolgen zu suchen. Nur ein algorithmisches Verfahren, das nach bestimmten Eigenschaften des Virus sucht, führt dann noch zum Erfolg.

Im Jahr 1991 wurde der Virus „Michelangelo"[295] entdeckt und sorgte für die weltweite Hysterie um die Sicherheit von Personalcomputern. Der Virus nistete sich in den Bootsektor von Disketten und dem Startsektor der Festplatte ein und löschte am 6. März die Festplatte. Weltweit vorausgesagte Schäden blieben jedoch aus.[296] In den folgenden Jahren fanden zum ersten Mal Wettbewerbe und Veranstaltungen zum Programmieren von Viren statt, und viele Zeitschriften wurden speziell für Virenprogrammierer gegründet.[297] Im Jahr 1992 wurde der erste Windows-Virus mit dem Namen „WinVir 1.4" entdeckt. Es folgten die ersten Viren, die SYS-Dateien infizierten.[298]

1993 infizierte der Virus „SatanBug" Computersysteme in Washington DC. Die Behörden konnten die Spur zum Autor „Little Loc" nach San Diego zurückverfolgen. Da er jedoch noch minderjährig war, wurde von Strafmaßnahmen abgesehen.[299] 1994 tauchte eine neue Virusart auf, die wesentliche Unterschiede zu ihren Vorgängern hat: So verteilt sich die variable Entschlüsselungsroutine über das gesamte infizierte Programm. Dieser Virus, der One_Half oder auch Free_Love bezeichnet wird, kann sich sowohl in Dateien als auch ein Bootsektoren und Master-Boot-Records einnisten. Solche Viren werden auch multipartite Viren genannt. Zusätzlich verschlüsselt der Virus zwei Sektoren der Festplatte mit einem variablen Schlüssel.

[293] 1990 schrieb Marc Washburn "1260", den ersten polymorphen Virus.
[294] http://www.vhm.haitec.de/konferenz/1997/history.htm (zuletzt abgerufen am 30.03.2004).
[295] Er wurde aufgrund des Datums 6. März, dem Geburtstag des italienischen Malers und Bildhauers Michelangelo, nach ihm benannt.
[296] http://www.tariftip.de/rubrik/8738/1/Geschichte+der+Viren.htm (zuletzt abgerufen am 30.03.2004).
[297] http://www.vhm.haitec.de/konferenz/1997/history.htm (zuletzt abgerufen am 30.03.2004).
[298] http://www.symantec.com/region/de/avcenter/regeln_de.html (zuletzt abgerufen am 30.03.2004).
[299] http://www.familie-im-web.de/familie/freizeit/themen/sicherheit/geschichte_der_computerviren.html (zuletzt abgerufen am 30.03.2004)

Dieser speicherresidente Virus verfügt auch über Stealth-Techniken, die das Erkennen zusätzlich erschweren.[300]

Mit dem Virus „CONCEPT“ wurde 1995 die Ära der Makroviren eingeläutet. Es wurden nur Dokumente, die mit „Microsoft Word“ erstellt wurden, infiziert. Wenige Monate später gab es auch einen „Excel-Virus“ mit Namen „LAROUX“.[301] Makroviren infizieren keine ausführbaren Programmdateien, sondern Dokumente des Textverarbeitungsprogramms WinWord oder Excel von Microsoft. Da dieses Programm z.B. auch auf dem Macintosh eingesetzt wird und die Virenmakros dort auch laufen, war der erste plattformübergreifende Virus geboren. Außerdem ist für die Programmierung eines solchen Makros nur wenig Fachwissen nötig. Ein Virus wurde bis dahin hauptsächlich in Assembler programmiert, was gewisse Systemkenntnisse voraussetzte. Solche Makros können allerdings fast von jedem Anwender programmiert werden, der mit einer solchen Textverarbeitung arbeitet.[302] 1996 wurde der erste polymorphe Windows-Virus entdeckt, was unter Windows bislang ein gewisses Problem darstellte. Im 3. Quartal des Jahres 1996 wurde die Anzahl der Viren bei PCs auf mittlerweile über 10.000 verschiedene Varianten geschätzt.[303]

1997 verbreiteten sich zum ersten Mal Computerviren auch über Chatforen des Internet (IRC). Die Virusprogrammierer schrieben mIRC-Scripte, die sich automatisch unter den Benutzern des Internet Relay Chats verbreiteten.[304]

Das Jahr 1998 war eines der interessantesten Jahre in der Geschichte der Computerviren. Der erste Virus, der PC-Hardware außer Funktion setzte, der „cih“-Virus (alias „Tschernobyl“) wurde in Taiwan entdeckt. Er überschreibt den BIOS-Chip, was oft einen Austausch der Hardware erfordert. Er taucht auch heute noch gelegentlich auf.
Die Hacker- Gruppe „Cult of the Dead Cow“ brachte mit „Back Orifice“ einen der ersten modernen Trojaner heraus, ein getarntes Fernsteuerungsprogramm, das die Ausführung von Programmen sowie die Überwachung eines Computers ermöglicht. Zudem verbreiteten sich die ersten VB-Script-Viren, von denen sich einige sogar in HTML-Dokumenten verstecken konn-

[300] http://www.vhm.haitec.de/konferenz/1997/history.htm (zuletzt abgerufen am 30.03.2004).
[301] http://collabor.f4.fhtw-berlin.de:8080/antville/Mcfabe/topics/Semesterarbeit (zuletzt abgerufen am 30.03.2004).
[302] http://www.vhm.haitec.de/konferenz/1997/history.htm (zuletzt abgerufen am 30.03.2004).
[303] Ebd.
[304] http://www.symantec.com/region/de/avcenter/regeln_de.html (zuletzt abgerufen am 30.03.2004).

ten.[305] Die ersten Viren für Microsoft Access nebst Varianten sowie für Microsoft PowerPoint wurden entdeckt. Weitere Viren folgten, die sämtliche Office-97-Anwendungen infizierten.[306]

1999 machte die Computergemeinde mit „W97.Melissa“ Bekanntschaft mit einem sich besonders rasant verbreitenden Computervirus. Der Virus verbreitete sich selbstständig über das Outlook-Adressbuch in der ganzen Welt. Mailserver in aller Welt mussten abgeschaltet werden.[307] Im April desselben Jahres wurde „W95.CIH“ aktiv, der in Asien erhebliche Schäden verursachte. Chen Ing-Hau, ein Student, wurde als Autor des Virus identifiziert. Gleichzeitig verbreitete sich „ExploreZip“ im ganzen Netz und zerstörte Dateien mit den Endungen DOC, XLS, PPT, C, CPP und ASM. Im November 1999 erschien der erste Virus, der nur durch Lesen der E-Mail aktiv wurde. Dieser Virus nutzt einen Fehler in einer Microsoft-Programmbibliothek, durch den das Abspeichern und Starten der E-Mail-Anlage unnötig wird. Einfaches Anklicken der E-Mail bei einem aktiven Vorschaumodus startet den Virus.[308]

Im Jahr 2000 tauchte der Virus „I LOVE YOU“ auf. Experten sprachen von dem sich am schnellsten verbreitenden Virus der Computergeschichte. Wiederum brachen weltweit tausende Mailserver zusammen. Mittlerweile sind unzählige Klone entstanden, die mit abweichenden Namen und Endungen versuchen, sich weiter zu verbreiten.[309] Daneben tauchte im September der erste Virus für Personal Digital Assistants (PDA) auf. „Palm.Liberty.A“ verbreitet sich nicht von selbst, sondern gelangt beim Synchronisationsprozess in den Kleincomputer und löscht Aktualisierungen. Herkunftsland ist Schweden. Entwickelt wurde er versehentlich von einem Beschäftigten der Universität von Gavle namens Aaron Ardiri.[310]

Im Jahr 2001 stieg durch zunehmende Zahl der Internetnutzer auch die Anzahl der Computerviren. „Code Red“ befiel binnen weniger Stunden 250.000 Rechner und verursachte einen Schaden von 2 Mrd. US-$. Er nutzte eine Sicherheitslücke in der Web-Software „Internet Information Server“ von Microsoft aus, die unter Windows NT oder 2000 läuft. Sein Ableger „Code Red II“ attackiert nicht – wie das Original – die Webseiten des Weißen Hauses, son-

[305] http://www.computerviren-info.de/Geschichte.html (zuletzt abgerufen am 30.03.2004).
[306] http://www.familie-im-web.de/familie/freizeit/themen/sicherheit/geschichte_der_computerviren.html (zuletzt abgerufen am 30.03.2004).
[307] http://www.tariftip.de/rubrik/8738/1/Geschichte+der+Viren.htm (zuletzt abgerufen am 31.03.2004).
[308] http://www.familie-im-web.de/familie/freizeit/themen/sicherheit/geschichte_der_computerviren.html (zuletzt abgerufen am 31.03.2004).
[309] Ihm folgten bis heute viele ähnliche Schädlinge: „Kournikova“, „Naked Wife“, „Nimda“, „SirCam“, „Badtrans“, „Blaster“ – und ein Ende ist nicht in Sicht.
[310] http://www.familie-im-web.de/familie/freizeit/themen/sicherheit/geschichte_der_computerviren.html (zuletzt abgerufen am 31.03.2004).

dern installiert eine Hintertür in das System, durch das Hacker den Rechner kontrollieren können.[311] Im September 1999 tauchte zudem der Computerwurm „Nimda“ im World Wide Web auf. Die Innovation bestand darin, dass für seine Verbreitung keine Benutzerinterventionen mehr erforderlich sind. Stattdessen nutzt er bekannte Software-Schwachstellen und unterschiedliche Formen der Infektion. Er verbreitet sich über E-Mail und kann sich zudem über das Internet auf fremden Rechnern einnisten. Die rasante Verbreitung des Wurms belastet den Internetverkehr, führt zum Zusammenbruch der betroffenen Webseiten und kompromittiert die Sicherheit des Filesystems, indem er die lokalen Laufwerke im Netzwerk freigibt.[312] Zwei Monate darauf nutzte der Computervirus „W32.Badtrans.B@mm“ ein bekanntes Sicherheitsloch in den E-Mail-Applikationen (MS Outlook/MS Outlook Express). Nach der Infektion registriert sich der Wurm als Systemservice und beantwortet eingehende E-Mails, spioniert Passwörter aus und installiert einen Key-Logger.[313]

Im Jahr 2002 breitete sich der Virus mit dem Namen „Warhol“ aus, der in der Lage ist, selbstständig IP-Adressen zu scannen, bekannte Sicherheitslücken auszukundschaften, um sich dann auf dem Server einzunisten. In noch nie dagewesener Geschwindigkeit sollte sich diese neue Generation von Viren durch das Internet verbreiten können. Nach Aussage der Spezialisten könnte sich der Wurm innerhalb von 15 Minuten auf neun Millionen Webservern vermehren – genug für eine weltweite Verbreitung.[314] Im September machte sich der erste Wurm auf den Weg ins Netz, der seine eigene SMTP-Engine, also einen eigenen Mailserver und somit unabhängigen Verbreitungsmechanismus mitbrachte. Der 50.886 Bytes große Schädling trug den Namen „Bugbear“ und verbreitete sich sehr schnell. Neu an diesem Wurm war auch, dass er in der Lage ist, Virenschutzprogramme und Firewalls auszuhebeln, wenn sie nicht aktuell sind. Einmal auf den Rechner gelangt, öffnet Bugbear durch eine trojanische Komponente einen bestimmten „Port“ des Rechners (also eine Eintrittstür) und erhält so Zugang zum Zielrechner. Ein ärgerlicher Nebeneffekt ist zudem, dass Bugbear sich an alle freigegebenen Netzwerkdrucker verschickt und selbstständig Druckaufträge druckt.[315]

---

[311] Ebd.
[312] http://www.symantec.com/region/de/avcenter/regeln_de.html (zuletzt abgerufen am 31.03.2004).
[313] http://www.trojaner-info.de/archiv/w32_badrans_b.html (zuletzt abgerufen am 31.03.2004); http://securityresponse1.symantec.com/sarc/sarc-intl.nsf/html/de-w32.badtrans.b@mm.html (zuletzt abgerufen am 31.03.2004).
[314] http://za-internet.de/NL/2002-11-infobrief-fastest-virus.pdf (zuletzt abgerufen am 31.03.2004).
[315] http://www.familie-im-web.de/familie/freizeit/themen/sicherheit/geschichte_der_computerviren.html (zuletzt abgerufen am 31.03.2004).

Im Januar 2003 beeinträchtigte der Computerwurm „Sapphire“ alias „Slammer“ alias „SQ hell“ mit einem Denial-of-Service-Angriff auf zehntausenden Internet- und E-Mail-Server in Nordamerika, Asien und Europa den globalen Datenverkehr massiv. Der Wurm nutzte für die DDoS-Attacke eine seit einem halben Jahr bekannte Sicherheitslücke in der weit verbreiteten Datenbanksoftware SQL Server 2000 von Microsoft. In Nordamerika wurde deutlich, dass der Internet-Angriff auch Auswirkungen in Bereichen des alltäglichen Lebens hatte, die bislang als weitgehend sicher galten: So funktionierten in Seattle an einem Samstag für mehrere Stunden nicht die Notrufnummern von etlichen Polizei- und Feuerwehrbezirken. Die Geldautomaten der Bank of America, einer der größten US-Banken, waren außer Betrieb, ebenso wie 14.000 Postämter in Italien. Im August 2003 hielten gleich zwei Würmer die IT-Welt in Atem: Der Computerwurm „Blaster“ (alias „Lovsan“) verbreitete sich direkt über die bloße Anbindung an das Internet, indem er eine Sicherheitslücke im Betriebssystem Windows ausnutzte – ähnlich wie der Slammer. Danach sorgte der Computerwurm „Sobig.F“ für Wirbel und breitete sich – so schnell wie noch kein Wurm zuvor – über aktivierte E-Mail-Anhänge aus; dabei fälschte er den E-Mail-Absender, was zu einer weiteren Flut von automatisierten Warnungen durch Virenschutzprogramme an die vermeintlichen Absender führte.[316]

Im Januar 2004 geisterten gleich drei Viren, „Dumaru“, „MiMail.Q“ und „MyDoom“ durch das Internet. Anders als die Viren und Würmer der letzten Monate öffneten sie Hintertüren, über die z.B. Passwörter und Kreditkartennummern ausgespäht werden konnten. Allein „MyDoom“ richtete Schäden in Milliardenhöhe an, blockierte weltweit E-Mail-Postfächer und setzte sogar für kurze Zeit die Internetseiten der Softwarefirma SCO Group mit einem DoS-Angriff außer Gefecht.[317]

Anfang Mai 2004 verbreitete sich ein Computerwurm namens Sasser auf Computern mit den Microsoft Betriebssystemen Windows 2000 sowie Windows XP. Unter den betroffenen Systemen waren Computer bei Banken, Reiseunternehmen und öffentlichen Einrichtungen. Besonders betroffen waren die Computer der deutschen Postbank, einer großen finnischen Bank und der Europäischen Kommission.[318]

[316] http://www.familie-im-web.de/familie/freizeit/themen/sicherheit/geschichte_der_computerviren.html (zuletzt abgerufen am 31.03.2004); http://www.bsi-fuer-buerger.de/viren/04_06.htm (zuletzt abgerufen am 31.03.2004).
[317] http://www.bsi-fuer-buerger.de/viren/04_06.htm (zuletzt abgerufen am 31.03.2004).
[318] http://de.wikipedia.org/wiki/Sasser (zuletzt abgerufen am 05.07.2004).

2.4.1.1.2 Strategie und Aufbau eines Virus

Ein Computervirus ist ein aus dem Bereich der Biologie entlehnter Begriff. Hier wird der Begriff verwendet für nichtselbstständige Programmroutinen, die sich selbst reproduzieren und Manipulationen z. B. an der Betriebssystemsoftware oder anderen Programmen vornehmen können.[319] Ein Computervirus ist kein eigenständiges Programm, sondern eine Abfolge aneinander gereihter Zeichen. Diese Abfolge ist für sich genommen nicht ausführbar. Im Gegensatz zu Würmern und Trojanern, die „echte" Programme (z.B.: exe-Dateien) sind, kann ein Virus im Dateimanager nicht aufgespürt werden. Der Quellcode eines Virus kann nur eine Zeile lang sein oder viele Seiten füllen. Es liegt ganz in der Fantasie und im Können der Virenprogrammierer, welche Schadensroutinen sie dem Quellcode der Viren hinzufügen.[320] Der klassische Virus ist ein Schadprogramm, das sich von Datei zu Datei auf einem Computer ausbreitet. Der Virus repliziert sich selbst, zum Beispiel wenn der Benutzer ein bestimmtes Programm ausführt oder den Computer hochfährt. Damit der Virus sich auf dem PC ausbreiten kann, muss er aktiviert werden. Dazu ist menschliche Hilfe nötig, so dass er mit dem Öffnen einer Datei oder dem Starten des Computers seinen Rechner infiziert.[321]

Die Gesamtzahl der bekannten Viren liegt derzeit bei über 50.000. Da es keine einheitliche Konvention für die Kategorisierung und Benennung von Computerviren gibt, differieren die Angaben teilweise erheblich.[322] Sophos, einer der größten Entwickler von Antivirensoftware, nennt eine hohe Steigerungsrate neu geschriebener Viren. Insgesamt hat Sophos in den ersten sechs Monaten des Jahres 2004 über 4.000 neue Viren entdeckt und entsprechende Gegenmaßnahmen entwickelt. Im Vergleich zum Vorjahreszeitraum ergab sich damit ein Zuwachs von 21 Prozent.[323] Ob diese hohe Anzahl an neuen Viren allein von jugendlichen Hackern geschrieben werden, ist fraglich. In Frage kommen unter anderem auch Antiviren-Hersteller, die ein großes Interesse daran haben, dass ihre Produkte weiterhin genutzt werden. Unternehmen, die Konkurrenten Schaden zufügen wollen, können als Tätergruppe ausgeschlossen werden. Viren lassen sich nicht speziell auf ein Netzwerk oder einen Rechner programmieren, so dass Schäden auch an den eigenen Rechnern entstehen würden, zumindest durch Varianten des selbst programmierten Virus. Durchschnittlich dauert es nur noch 20 Minuten, bevor ein

[319] Anonymus 2003, S. 381.
[320] http://www.computerviren-info.de/Definition.html (zuletzt abgerufen am 01.04.2004).
[321] http://www4.informatik.uni-erlangen.de/Lehre/SS02/PS_KVBK/talks/ausarbeitung-trojaner.pdf. (zuletzt abgerufen am 13.04.2004).
[322] http://www.symantec.com/region/de/avcenter/wissenswertes.html (zuletzt abgerufen am 13.08.2004).
[323] http://www.sophos.de/pressoffice/pressrel/20040728topten.html (zuletzt abgerufen am 13.08.2004).

ungesicherter Windows-Rechner mit Viren oder anderen Schädlingen infiziert ist. Vor einem Jahr lag die Zeit bis zum ersten Angriff noch bei durchschnittlich 40 Minuten, so eine am 17.08.2004 in Bethesda, Maryland, veröffentlichte Statistik, die das Internet Storm Center veröffentlicht hat, das zum SANS Institute gehört.[324]

Die Absicht der Urheber von Viren ist es, so viele Dateien wie möglich innerhalb eines Computers zu infizieren oder vitale Funktionen zu blockieren. Es gibt verschiedene Verbreitungswege, über die sich Computer mir Viren infizieren können. Dabei kommt es immer auf den derzeitigen Stand der Technik an. War die Diskette früher der häufigste „Überträger", so gewannen später die CD-ROM und andere externe Datenträger ein größeres Gewicht. Heute wird noch eine erhebliche Zahl von Viren über diese Wege weitergegeben. Mittlerweile sind alle möglichen Formen von Netzwerken (z.B. Unternehmens- oder Behördennetzwerke) weiter auf dem Vormarsch. Das Internet und die Virenverbreitung mittels E-Mail stehen mit Abstand an Nummer eins. Zur Verbreitung bedient sich der Virus eines Wirtprogramms oder einer Wirtdatei. Dazu setzt er eine winzige Sprunganweisung (einen „Zeiger") an den Beginn des Wirts (4 Byte reichen dazu) und platziert sich dann am Ende des Wirtsprogramms. Die vom Originalprogramm abgetrennten Bytes werden hinter den Virencode geschrieben und die internen Adressen angepasst, so dass das Programm komplett bleibt und weiterhin ausgeführt werden kann. Gleichzeitig wird innerhalb des Zeigers ein Hinweis platziert, der das Programm als infiziert markiert. Einfacher erstellte Viren überschreiben auch Teile des Wirtsprogramms. Bei neueren Viren sollte das nicht mehr vorkommen, denn die Gefahr der vorzeitigen Entdeckung wäre dabei zu hoch. Sobald das infizierte Programm gestartet wird, sorgt der Zeiger dafür, dass zunächst der Virus und dann erst das Programm aktiv wird. Nun durchsucht der Virus die Festplatte nach Programmen oder Dateien, die noch nicht befallen sind, an deren Beginn also die entsprechende Markierung fehlt, und platziert dann Reproduktionen von sich selbst in ihnen – einschließlich der eigentlichen Schadensroutine (der „Payload").[325]

Die heutigen Viren bestehen meist aus einem Infektionsbereich, einem Aktivierungsbereich und einem Manipulationsmodul. Der Infektionsteil befällt meist den Bootsektor einer Festplatte oder Diskette, auf dem der Rechner nach dem Einschalten das Ladeprogramm für das Betriebssystem sucht. Sobald eine Diskette eingelegt wird, durchsucht der Virus auch den dort enthaltenen Bootsektor und nistet sich in ihm ein. Bei gut programmierten Viren ist der

[324] http://de.internet.com/index.php?id=2030378&section=Marketing-Statistics (zuletzt abgerufen am 20.08.2004).
[325] http://www.computerviren-info.de/Definition.html (zuletzt abgerufen am 01.04.2004).

Infektionsteil sogar in der Lage zu erkennen, ob ein neuer Datenträger oder eine Datei bereits befallen ist und kann so eine Doppelinfektion vermeiden.[326] Der Aktivierungsteil eines Virus bestimmt, wann dieser das erste Mal aktiv werden soll. Beliebte Auslöser sind Zählermechanismen, die beispielsweise hundert Rechnerstarts abwarten, oder zeitabhängige Ereignisse, wie das Erreichen eines bestimmten Datums.[327] Bezüglich des Manipulationsmoduls unterscheidet man zwischen gutartigen und bösartigen Viren. Gutartige Viren stören lediglich den Programmablauf mit unerwünschten Meldungen und richten keine weiteren Schäden an. Die bösartigen Varianten richten teilweise enorme Schäden an. Sie überschreiben Speicherinhalte, zerstören Festplatteninhalte oder stellen einfach nur Zahlenwerte in Dateien um.[328]

Einige Virenarten besitzen neben den genannten Komponenten auch noch einen Tarnungsbereich und einen Erkennungsbereich. Der Tarnungsbereich dient dazu, dass ein Virus in einem System nicht so leicht entdeckt werden kann. Im Erkennungsbereich wird geprüft, ob das Programm bereits durch den Virus infiziert wurde. Ist dies der Fall, so muss dieses Programm nicht ein zweites Mal infiziert werden, somit kann sich der Virus schneller ausbreiten.[329]

2.4.1.1.3 Virenarten

In der Umgangssprache wird meistens nur das Wort Virus genannt, wenn man an Programme mit schädlichen Wirkungen denkt. Hiermit sind Viren im eigentlichen Sinne, Trojanische Pferde, logische Bomben, Internetwürmer oder auch Hoaxe gemeint. Der Fachmann nennt derartige Programme/Dateien „Malicious-Software“ (böswillige Software), kurz wird jedoch meist von „Malware“ gesprochen. Um eine Einteilung der Virenarten vorzunehmen und den Sprachgebrauch zu erläutern, wird im Folgenden eine Klassifizierung vorgenommen. Bei der Klassifizierung von Viren gibt es dabei ebenso wenig Einigkeit wie bei der Einordnung der Softwarebedrohungen insgesamt. Das liegt nicht nur an den vorhandenen verschiedenen Bezeichnungen für dieselben Viren, sondern auch daran, dass es Mischformen gibt, die mehreren Kategorien zugeordnet werden können. Daher kann die folgende Aufzählung lediglich der

[326] Zimmermann 2002, S. 60; http://www.michael-berndt.de/ie/sou/viren1.htm#28 (zuletzt abgerufen am 01.04.2004).
[327] Zimmermann 2002, S. 60; http://www.mrco.at/kurs/grund_03_datensicherheit.htm (zuletzt abgerufen am 01.04.2004).
[328] Zimmermann 2002, S. 60¸ http://www.rotary-arnsberg.de/vortrag/virenwarnung.html (zuletzt abgerufen am 01.04.2004).
[329] http://www-ra.informatik.uni-tuebingen.de/lehre/ws02/pro_sicherheit_ausarbeitung/Guschelbauer_Gefahren.pdf (zuletzt abgerufen am 06.04.2004).

Versuch einer Begriffsklärung sein. So lassen sich Viren z.B. danach unterscheiden, wo sie sich einnisten. Dementsprechend gibt es System- und Programmviren, die zum Teil auch Dateiviren genannt werden. Orientiert man sich an weiteren Eigenschaften, kann man Systemviren, Programm- bzw. Dateiviren, Makroviren, Residenteviren, Stealth- bzw. Tarnkappenviren und polymorphe Viren unterscheiden.

Ich möchte zunächst eine Klassifizierung vornehmen, die sich an den Angriffsobjekten von Computerviren orientiert. Alle weiteren Virentypen sind entweder Mischformen oder Untergruppen, die im Anschluss dargestellt werden und anhand ihrer Techniken klassifiziert werden können. Gerade die Verknüpfung mehrerer Eigenschaften machen Computerviren so gefährlich. Diese Mischformen sollen nachfolgend näher beschrieben werden.

2.4.1.1.3.1 Bootviren, Dateiviren, Makroviren

Eine mögliche Klassifizierung kann in folgender Weise erfolgen: Bootviren, Dateiviren, Makroviren.

Bootsektor- und Partitionsviren[330] verankern sich zumeist im ersten physikalischem Sektor, dem Boot-Record (DBR), einer Diskette oder im Master Boot Record (MBR), welcher manchmal auch als Partitionssektor bezeichnet wird, einer Festplatte. Ist eine Festplatte partitioniert, so ist der erste Sektor jeder Partition der Boot-Record, in welchem ein Programm die Boot-Fähigkeit des Datenträgers überprüft und bei Erfolg die Kontrolle an das Betriebssystem übergibt.[331] Der Virus überschreibt entweder einen Teilbereich, ersetzt den gesamten Code oder lagert weitere Codeteile in andere Bereiche der Festplatte aus. Bootviren haben eine ähnliche Funktionsweise wie ein Betriebssystem. Wenn der Rechner gestartet wird, führt das BIOS eine kleine Startroutine von der Festplatte oder von einer Bootdiskette aus. Die Startroutine ist auf dem MBR am Anfang des Datenträgers gespeichert. Sie ruft den Startcode des Betriebssystems im Bootsektor der aktiven Partition auf.[332] Bei einem infizierten Bootvorgang wird zuerst der Virus aktiviert und anschließend wird der Bootsektor ausgeführt, der dann das Betriebssystem lädt. Bei jedem weiteren Systemstart wird nun der Virus automatisch ausgeführt. Dies führt zur Infizierung weiterer Bootsektoren. Der Virus verbleibt nach dem boo-

[330] Im Folgenden als Bootviren bezeichnet.
[331] Anonymus 2003, S. 393.
[332] Anonymus 2003, S.395.

ten[333] durchgehend im Arbeitsspeicher und hat damit Zugriff auf alle an das System angeschlossenen Laufwerke, d.h. auf weitere Festplatten und auf das Diskettenlaufwerk. Er kann jetzt jeden Bootsektor von nicht schreibgeschützten Disketten manipulieren und sich dadurch auf weitere (ungeschützte) Computer übertragen. Da auch eine scheinbar leere Diskette einen Bootsektorvirus enthalten kann, müssen sich nicht einmal Programme oder Daten auf der Diskette befinden.[334]

Dateiviren befallen im Gegensatz zu den Bootsektorviren ausführbare Programme. Zu den ausführbaren Programmen zählen unter anderem alle Dateien mit den Endungen: com-, exe-, ovl-, obj-, sys-, bat-, drv-, vbs-, dll-Dateien. Unter den auch als Programm- bzw. Fileviren bezeichneten Dateiviren gibt es solche, die sich lediglich an ein Programm anhängen. Andere überschreiben die zu infizierende Datei, soweit sie deren Platz benötigen (sog. überschreibender Virus). Ist das Wirtsprogramm kleiner, wird es komplett überschrieben und zusätzlich benötigter Platz hinten angehängt.[335] Der Virus kopiert sich in der Regel selbst oder eine Sprunganweisung auf sich an den Anfang der Datei und wird immer dann ausgeführt, wenn die Datei aufgerufen wird.[336]

Während sich die bereits genannten Viren anstelle des Programmcodes einnisten, benutzen Makroviren[337] Steuersequenzen in Datendateien.[338] Moderne Programme erlauben es, häufig benötigte Steuerinformationen mittels einfach erlernbarer Programmiersprachen zu erstellen (sog. Makros).[339] Diese bieten die Möglichkeit, Arbeitsabläufe zu automatisieren. Dies geschieht durch kleine Programme, sog. Scripte, die zur Laufzeit der jeweiligen Anwendung interpretiert und ausgeführt werden. Meistens sind die Scripte als reiner, lesbarer Text geschrieben, was das Erzeugen und damit allerdings auch den Missbrauch in Form von Viren

[333] Als Booten oder Hochfahren bezeichnet man das Laden eines Computer-Betriebssystems. Zuerst wird der Prozessor sowie das BIOS gestartet. Zudem werden u. a. Programme ausgeführt, die zwar eigenständig sind, sich aber in sonst nicht zugänglichen und im Inhaltsverzeichnis der Disketten und Festplatten nicht sichtbaren Sektoren, auch Bootsektoren genannt, befinden. Diese Programme heißen Boot-Loader.
[334] http://www-ra.informatik.uni-tuebingen.de/lehre/ws02/pro_sicherheit_ausarbeitung/Guschelbauer_Gefahren.pdf (zuletzt abgerufen am 06.04.2004).
[335] http://www.jurpc.de/aufsatz/20010205.htm#C17 (zuletzt abgerufen am 06.04.2004); http://www-rnks.informatik.tu-cottbus.de/de/materials/ss2001psSicherheit/file5_2.pdf (zuletzt abgerufen am 06.04.2004).
[336] http://www.ifi.unizh.ch/ikm/Vorlesungen/Sem_Sich01/Estermann.pdf (zuletzt abgerufen am 06.04.2004).
[337] Der Begriff Makrovirus ist ungenau und suggeriert eine eher künstliche Unterscheidung zwischen Makro- und Scriptviren, dies gilt insbesondere für VBS.
[338] Anonymus 2003, S. 396.
[339] Ein Makro ist ein kleines Programm, mit dem zum Beispiel in Microsoft Word Abläufe automatisiert werden. Die an Basic angelehnte Makrosprache ist eine recht einfach erlernbare Programmiersprache. Dies hat letztlich zur Folge, dass Makroviren weitaus öfter anzutreffen sind als andere Virenarten.

erheblich vereinfacht.[340] Einige bekannte Script-Sprachen sind Visual Basic Script, mIRC, Visual Basic for Applications (VBA), JavaScript etc. Makros werden hauptsächlich bei Officepaketen verwendet. Um eine gewisse Abfolge von Arbeitsschritten nicht ständig wiederholen zu müssen, wird ein so genanntes Makro erstellt, um diese Abfolge quasi auf Knopfdruck erledigen zu können. Mit den Befehlen einer mächtigen Scriptsprache kann ein Makro beispielsweise Dateien und andere Officedokumente manipulieren oder Applikationen fernsteuern.[341] Der Großteil dieser Viren ist allerdings einer einzigen Scriptsprache zuzuordnen: Visual Basic Script. Diese Scriptsprachen sind teilweise so umfassend, dass damit fast alle Funktionen eines Betriebssystems aufgerufen und ausgeführt werden können.

Die Funktionsweise von Makroviren gleicht der von Dateiviren. Allerdings werden nur Dokumente infiziert und keine Programme. Wird ein Dokument geöffnet, das Makros enthält, startet das Programm automatisch die Makros. Ist eines davon ein Virus, so kopiert es sich ab sofort in jeden Text hinein, den der Benutzer abspeichert. Unter anderem befallen Makro-Viren Word-Dokumente, Excel-Tabellen und PowerPoint-Präsentationen. Besonders gefährlich sind Makroviren, da sie sich sehr schnell und bevorzugt über das Internet als Anhang von E-Mails verbreiten. Daneben lassen sich damit auch Bildschirmmeldungen aufrufen, Applikationen steuern, E-Mails versenden, Programme ausführen, Festplatten formatieren, externe Viren starten, das komplette System von außen fernsteuern und vieles mehr. Dieses große Funktionsspektrum öffnet trotz Sicherheitsvorkehrungen der Hersteller den Viren Tür und Tor zum lokalen Computersystem.

2.4.1.1.3.2 Mischformen und Untergruppen

Neben den drei Grundtypen (Bootviren, Dateiviren, Makroviren) existieren unzählige Mischformen, die zusätzlich zu den Grundeigenschaften mit Zusatzfunktionen ausgestattet sind. Die Vermengung von einzelnen Grundtypen mit verschiedenen Zusatzfunktionen machen Viren einzigartig und im Speziellen erst gefährlich. Ein Virus kann mit einer oder mehreren Zusatzfunktionen versehen werden, so dass die folgende Aufzählung keine eigenen Virustypen an sich darstellt, sondern vielmehr der Begriffsklärung dient. Jedoch werden gerade diese Mischformen von Hackern dazu benutzt, um Trojaner oder andere Programme auf fremden Syste-

[340] http://www.antivir.de/infos/scriptvir.htm (zuletzt abgerufen am 07.04.2004); http://www.trojaner-info.de/viren/virentypen.shtml (zuletzt abgerufen am 07.04.2004); http://www.irongate.ch/security/demo.htm (zuletzt abgerufen am 08.04.2004).
[341] http://www.ifi.unizh.ch/ikm/Vorlesungen/Sem_Sich01/Estermann.pdf. (zuletzt abgerufen am 06.04.2004).

men zu installieren und dadurch Computer fernzusteuern oder Passwörter herauszufinden. Zudem muss darauf hingewiesen werden, dass bei den folgenden Zusatzfunktionen nur die bislang bekannten Viren einbezogen werden können und die Liste im Lauf der kommenden Jahre erweitert werden muss.

Polymorphe Viren zählen zu den derzeit modernsten und gefährlichsten Varianten der Dateiviren. Bevor der erste polymorphe Virus erschien, war es für Virenscanner relativ einfach, Viren aufzuspüren. Anhand einer Vergleichsliste, die laufend aktualisiert werden musste, konnten Viren erkannt werden. Um der Entdeckung anhand dieser Suchmethode zu entgehen, kamen polymorphe Viren zum Einsatz. In diese Klasse teilt man Viren ein, die bei jeder neuen Infektion ihr Erscheinungsbild ändern. Gewöhnlich wird dies erreicht, indem sie den Viruscode mit einem wechselnden Schlüssel bei jeder Infektion neu verschlüsseln, so dass Virenscanner Viren anhand einer definierten Bytefolge nicht mehr erkennen können.[342] Zur Aktivierungszeit wird über eine Entschlüsselungsroutine der Viruscode entschlüsselt und gelangt zur Ausführung. Da die Entschlüsselungsroutine sehr klein gehalten wird, ist eine Entdeckung des Virus mit einem Scanner kaum möglich oder wird von häufigen Fehlalarmen begleitet.[343] Viele Virenprogrammierer bedienen sich zur Verschlüsselung ihrer Codes sog. Codegeneratoren (Mutation Engines)[344], welche diesen Teil der Programmierarbeit übernehmen.[345] Es handelt sich dabei um ein Programm, das jeder Virenprogrammierer in seinen Virus einbinden kann. Es sorgt nicht nur dafür, dass der Virus ständig neu codiert wird, sondern beinhaltet auch eine Veränderung der Instruktionen innerhalb des Entschlüsselungsprogramms. Jeder neue Virus gleicht damit in fast keinem Byte mehr seinem Vorgänger.[346] Eine Entdeckung des Virus ist nur mittels algorithmischer Suche oder heuristischer Analysen möglich.[347]

Speicherresidente Viren installieren sich zunächst resident im Hauptspeicher, von wo aus sie dann versuchen, die Systemdateien zu befallen, um eine möglichst schnelle Ausbreitung zu sichern. [348] Bei Aufruf eines infizierten Programms wird der Virus zunächst aktiv. Der Code des Virus ist so angelegt, dass er sich speicherresident[349] beendet. Der Virus kontrolliert ab

[342] http://www.thesitehf.de/aktuell/aktuell2a.htm (zuletzt abgerufen am 06.04.2004).
[343] http://www.borg-perg.eduhi.at/informatik/viren1/einteil.html (zuletzt abgerufen am 06.04.2004).
[344] Die erste Mutationsengine wurde von dem Bulgaren Dark-Avenger im Jahr 1992 veröffentlicht.
[345] http://www.jurpc.de/aufsatz/20010205.htm#C17b (zuletzt abgerufen am 06.04.2004).
[346] http://www.borg-perg.eduhi.at/informatik/viren1/einteil.html (zuletzt abgerufen am 06.04.2004).
[347] http://www.jurpc.de/aufsatz/20010205.htm#C17b (zuletzt abgerufen am 06.04.2004).
[348] http://www.interest.de/cgi-bin/lexika/Virus.html?pos=T15734491&ID=177492885602 (zuletzt abgerufen am 07.04.2004).
[349] Als speicherresident werden alle Programme bezeichnet, die im Arbeitsspeicher des PCs verbleiben, nachdem das Programm gestartet wurde. Andere Bezeichnungen hierfür sind TSR oder VxD.

sofort einen oder mehrere Interrupts.[350] Ruft der Nutzer nun ein Programm oder einen Befehl auf, das einen Interrupt benutzt, so wird der Virus zunächst wieder aktiviert. Die Verbreitungsstrategie dieser Viren ist sehr effizient; da der Virus im Speicher sitzt, ist er zur weiteren Verbreitung nicht darauf angewiesen, dass ein infiziertes Programm aufgerufen wird. Jeder Programmaufruf kann nun dazu führen, dass eine Infektion erfolgt.[351] Im Gegensatz dazu werden nichtresidente Viren nur aktiv, wenn das infizierte Programm gestartet wird. Sie können von sich aus Prozessaufrufe abfangen, externe Speichermedien manipulieren und erhebliche Schäden im System verursachen, ohne dass vom Benutzer irgendeine Aktion ausgelöst wurde. Die meisten dieser Viren können nicht durch einen Warmstart (d. h. CTRL + ALT + DEL) aus dem Arbeitsspeicher entfernt werden, da sie diese Tastenkombination abfangen und einen Warmstart nur vortäuschen. Nur das Drücken des Reset-Knopfes entfernt einen solchen Virus aus dem Hauptspeicher.[352] Der Bootsektorvirus ist das klassische Beispiel für einen speicherresidenten Virus. Aber beinahe alle andere Virenarten können ebenfalls diese Eigenschaft besitzen.

Stealth-Viren benutzen mehrere Techniken, um die Tatsache zu verbergen, dass das Laufwerk infiziert wurde. Die erste Tarnvariante ist, über die Programmeigenschaften zu täuschen. Fordert das Betriebssystem oder ein Virusscanner bestimmte Informationen an, stellt der Stealth-Virus diese Informationen in der Form zur Verfügung, in der sie vor der Infizierung waren. Bei Erstinfizierungen speichert der Virus die vorhandenen Informationen, um später das Betriebssystem und den Virenscanner zu täuschen.[353] Dazu überwachen sie die Zugriffe auf Programmdateien und das Inhaltsverzeichnis. Stealth-Viren geben somit dem Antivirusprogramm falsche Parameter weiter, um dem Virenscanner vorzumachen, dass das befallene Programm gar nicht verändert sei. Eine zweite Tarnfunktion liegt in der Selbstlöschung. Wird eine Programmdatei nicht ausgeführt, sondern nur gelesen, entfernt der Virus aus der zu le-

[350] In der Informatik versteht man unter Interrupt (lat. interruptus: Unterbrechung) die kurzfristige Unterbrechung eines laufenden Programmes oder, genauer gesagt, einer von der CPU abzuarbeitenden Befehlssequenz, um einen anderen Prozess, die Interrupt-Routine, auszuführen. Anschließend wird die Ausführung des Programmes an der Unterbrechungsstelle fortgesetzt. Sinn eines Interrupts ist z.B. die Möglichkeit einer schnellen Reaktion auf Signale von Ein/Ausgabe-Bausteinen oder Zeitgebern (Timern). Ausgelöst werden Interrupts meist durch Elektronikkomponenten mittels einer so genannten „Unterbrechungs-Anfrage“ (engl. Interrupt Request - IRQ). Mittels eines Interrupts wird dem Prozessor zum Beispiel eine Tastatureingabe übermittelt. Auch Multitasking wäre ohne Interrupts nicht möglich.

[351] http://www.unibw-muenchen.de/campus/RZ/RZN/SZPC/9213/viren.html#Speicherresidente_Viren (zuletzt abgerufen am 07.04.2004).

[352] http://www.uni-tuebingen.de/abot/GP00/sicher.html#Computerviren (zuletzt abgerufen am 07.04.2004).

[353] http://www.irongate.ch/security/viren.htm (zuletzt abgerufen am 06.04.2004).

senden Datei den Viruscode, so dass der Virenscanner den Virus nicht in der Programmdatei finden kann. Ist der Vorgang abgeschlossen, wird der Code wieder eingefügt.[354]

Cross-Infektor-Viren sind eine gefährliche Form der Makroviren. Sie besitzen die Fähigkeit, Dokumente verschiedener Programme, zumeist aus der Microsoft-Office-Produkt-Palette, zu befallen und sich von einem Programm auf ein anderes auszubreiten.[355] Sie springen beispielsweise von Word-Dokumenten auf Excel-Tabellen oder Access-Datenbanken über und verändern dort die Daten. Besonders gefährlich sind solche Varianten, die sich nicht nur applikations-, sondern auch betriebssystemübergreifend ausbreiten können.[356]

HTML-Viren galten lange Zeit als nicht existent. HTML selbst enthält keinerlei Befehle, die einen Zugriff auf Dateien ermöglichen, d.h. die Befehle des HTML reichen zur Programmierung von Computerviren grundsätzlich nicht aus.[357] Trotzdem tauchte der erste HTML-Virus im Oktober 1998 auf. HTML-Viren verstecken sich in Form eines VB-Scripts in einer HTML-Datei und können auch andere Dateien infizieren, indem sie sich ebenfalls als Script in der Datei verstecken. Diese Viren arbeiten vom Prinzip her wie Scriptviren. Abhängig vom jeweiligen Virus können nicht nur HTML-Dateien, sondern auch VBS- und DOC-Dateien infiziert und unter die Kategorie Makroviren eingestuft werden. Zusätzlich benutzen einige HTML-Viren auch ActiveX-Controls[358] und erweitern dadurch ihre Funktionsweise. [359]

Retroviren sind darauf aus, Antivirenprogramme anzugreifen. Programmierer dieser Virensorte untersuchen die Antivirenprogramme genau nach Schwachstellen. Retroviren können z.B. einen Virenscanner dahingehend verändern, dass dieses Programm zwar noch einen Scannvorgang vollzieht, jedoch an sich nicht mehr nach Viren sucht. Das würde bedeuten: Das System könnte mit Viren verseucht sein, der Scanner meldet jedoch, dass alles in Ordnung ist. Gerade Scanner, die so genannte Prüfsummen anlegen, werden von Retroviren bevorzugt, da diese Prüfsummen einfach manipuliert werden können.[360]

---

[354] http://www.borg-perg.eduhi.at/informatik/viren1/einteil.html (zuletzt abgerufen am 06.04.2004).
[355] http://focus.msn.de/D/DC/DCD/DCD54/DCD54E/DCD54ED/DCD54ED03/dcd54ed03.htm#27 (zuletzt abgerufen am 07.04.2004).
[356] http://www.ifi.unizh.ch/ikm/Vorlesungen/Sem_Sich01/Estermann.pdf. (zuletzt abgerufen am 07.04.2004).
[357] Ebd.
[358] ActiveX-Controls sind alle Microsoft-Technologien, die es Entwicklern ermöglichen, interaktive Anwendungen für das Web zu programmieren. Dazu gehört ein Satz von sprachunabhängigen Technologien, die es erlauben, in verschiedenen Sprachen geschriebene Komponenten in einer Netzwerkumgebung zusammen auszuführen.
[359] http://www.ifi.unizh.ch/ikm/Vorlesungen/Sem_Sich01/Estermann.pdf. (zuletzt abgerufen am 07.04.2004).
[360] http://www.trojaner-info.de/viren/virentypen.shtml (zuletzt abgerufen am 07.04.2004).

Als CMOS bezeichnet man den externen Speicher eines Rechners, der mit Strom über eine Batterie versorgt wird.[361] Hier werden wichtige Informationen wie Uhrzeit, Datum, Größe des DOS-RAM, Festplattenwerte etc. gespeichert.[362] Ein Virus, auch als Batteriepuffer-Virus bekannt, kann sich in diesem Bereich nicht aktiv speichern oder starten. Jedoch gibt es Viren, die das CMOS löschen oder manipulieren, so dass es zu Systemabstürzen kommt. Es wird dadurch verhindert, dass ein infiziertes System von einer nicht infizierten Diskette gestartet werden kann.[363] Diese Art von Viren ist eine Form der Bootsektorviren und wird als sehr gefährlich eingestuft.[364]

Um dem Nachteil der langsamen Verbreitung von Boot-Viren zu begegnen, wurden sogenannte Hybrid-Viren geschaffen. Diese sind eine Kombination aus Programm-Viren und System-Viren, infizieren sich somit in zwei Varianten und müssen auch auf zwei verschiedene Arten entfernt werden.[365] Indem diese Viren in der Lage sind, die Stärken der einzelnen Infektion zu kombinieren, etwa dadurch, dass sie Tarnungsmechanismen eines Boot-Virus und gleichzeitig polymorphische Techniken der Dateiviren benutzen, optimieren sie ihren Schutz vor Entdeckung. Außerdem haben sie die Möglichkeit, sich zum einen über befallene Dateien durch den Datei-Virus-Anteil und zum anderen über befallene Dateiträger durch den Boot-Virus-Anteil zu verbreiten.[366]

Tunnelnde Viren wenden eine Technik an, die es ihnen ermöglicht, viele speicherresidente Überwachungsprogramme zu umgehen. Da Überwachungsprogramme eingesetzt werden, um Virenaktivitäten festzustellen und an den Anwender zu melden, besteht hier die Gefahr, dass der Anwender sich in einer trügerischen Sicherheit fühlt, wenn er solche speicherresidente Überwachungsprogramme benutzt. Diese Art von Programmen überwacht meistens die Interrupts und wartet darauf, dass ein Interrupt von einem Programm aufgerufen wird. Dieser wird sodann überprüft. Ein tunnelnder Virus schaltet sich davor, so dass das Überwachungsprogramm keinen Interrupt registriert und der Virenschutz hierdurch umgangen wird.[367]

---

[361] Wird auch als batteriegepufferter Hauptspeicher bezeichnet.
[362] http://www.gulli.com/security/viren/virenarten.html#arten (zuletzt abgerufen am 07.04.2004).
[363] http://www.viren-wuermer-trojaner.de/hoaxes_1mythen.html (zuletzt abgerufen am 07.04.2004).
[364] http://www-rnks.informatik.tu-cottbus.de/de/materials/ss2001psSicherheit/file5_2.pdf. (zuletzt abgerufen am 07.04.2004).
[365] http://mitglied.lycos.de/utasauermann/lycos_home/viren.html (zuletzt abgerufen am 07.04.2004).
[366] http://agn-www.informatik.uni-hamburg.de/papers/doc/bacarb_kay_fiolka.pdf. (zuletzt abgerufen am 07.04.2004).
[367] http://www.fuhs.de/de/fachartikel/buch/4.shtml (zuletzt abgerufen am 13.04.2004).

Update-Viren sind eine moderne Virenkonstruktion und können grundsätzlich allen Virenformen zugeordnet werden. Sie sind nach Familien gegliedert und werden meist von einem einzigen Programmierer oder einer Gruppe von Programmierern entwickelt. Neben ihrer eigentlichen Funktion als Virus enthalten diese Viren nicht nur eine Versionsnummer, sondern auch eine Update-Routine, die überprüft, ob der Virus bereits in einer Version vertreten ist. Die Routine untersucht außerdem, ob die Datei bereits eine ältere Version des Virus enthält. Ist das der Fall, wird diese ersetzt. Ist eine neuere Version installiert, wird die Datei nicht noch einmal infiziert.[368]

Die bislang neueste Möglichkeit für die Verbreitung von Viren ist die so genannte WAP-Übertragung bei Handys. Mit der aktuellsten derzeit verfügbaren Übertragungstechnik General Packet Radio Services (GPRS) moderner WAP-Handys kommt auch die Version 1.2 der Wireless Markup Language (WML) zum Einsatz. Da die WAP/WML-Technik künftig auch die Übertragung von Computerprogrammen erlauben wird, können dabei theoretisch auch Viren übertragen werden. Die derzeit im Einsatz befindlichen WAP-Handys mit WML 1.1 ermöglichen nur die Darstellung von Informationen, jedoch keine Programmausführung.[369] Bislang kann davon ausgegangen werden, dass keine WAP-Viren existieren, vielmehr hängt es von den zukünftigen Möglichkeiten der Handy-Betriebssysteme und der darauf laufenden Software ab, ob eine technische Grundlage für Viren und Würmer geschaffen wird.[370]

2.4.1.1.4 Strategie und Aufbau eines Wurms

Computerwürmer sind selbstständig lauffähige Programme, die in der Lage sind, sich ohne ein Wirtsprogramm über ein Computernetz zu vervielfältigen. Für seine Verbreitung sendet ein Computerwurm z.B. eine E-Mail an sich oder andere Systeme oder meldet sich in einem anderen System an. Würmer verwenden Netzwerkverbindungen, um sich von System zu System zu verteilen. Dabei suchen sie andere Systeme, indem sie die Host-Tabellen oder ähnliche Stellen von Systemadressen ermitteln, bauen eine Verbindung zu diesen Systemen auf, kopieren sich selbst auf diese und bringen ihre Kopie zur Ausführung.[371] Würmer können ihre An-

[368] http://www.mr-virus.cc/viren/detailerkl.htm (zuletzt abgerufen am 13.04.2004).
[369] http://www.1scripts.org/content.php?page_id=45 (zuletzt abgerufen am 13.04.2004); http://www.ccwap.com/de/nl_1_2002.htm (zuletzt abgerufen am 13.04.2004).
[370] http://www.tu-berlin.de/www/software/hoax/handy.shtml (zuletzt abgerufen am 13.04.2004).
[371] Computerwürmer bestehen grundsätzlich aus zwei Programmen, dem Bootstrap und dem eigentlichen Wurmprogramm. Der Bootstrap ist ein kleines Programm, das auf dem angegriffenen System kompiliert und ausgeführt wird. Es stellt eine Verbindung zu dem Rechner her, von dem es kam und lädt das eigentliche Wurm-

wesenheit verschleiern, indem sie sich den Namen eines Systemprozesses oder einen vom Systemoperator nicht erkennbaren Namen geben. Da die meisten modernen Computerwürmer nicht nur für ihre Verbreitung sorgen, sondern auch zusätzlich weitere Schadensroutinen besitzen, können sie dieselben Schäden an Computern verursachen wie Computerviren.[372] Die viel genutzten E-Mail-Programme „Outlook“ und „Outlook Express“ von Microsoft sind durch ihre weite Verbreitung, durch viele Sicherheitslücken und ihre tiefe Verankerung im System ideale Einfallstore für Computer-Würmer.[373] Entsprechend ihrem unterschiedlichen Maß an Eigenständigkeit möchte ich Computerwürmer in drei Gruppen unterteilen:

Als Hoax[374] bezeichnet man Meldungen über Viren, die es gar nicht gibt, also falsche Warnungsmeldungen von Virenbefall, die vergleichbar mit Zeitungsenten sind.[375] Derartige Informationen werden in der Regel per E-Mail übermittelt. Die Warnungen deuten häufig auf bestimmte Programme, die mit einem Virus oder Trojaner infiziert sein sollen.[376] Dabei wird empfohlen, irgendwelche Dateien oder E-Mails nicht zu öffnen, sondern sofort zu löschen und die Meldung an möglichst viele Nutzer weiterzuleiten. Dabei löschen unerfahrene PC-Benutzer vermeintlich infizierte Dateien und Programme, die eigentlich notwendig sind, um einen reibungsloses Funktionieren des Rechners zu gewährleisten.

Skriptwürmer bestehen aus einer normalen E-Mail mit einem Dateianhang, in der sich ein Skript befindet, durch welches ein Mailclient ferngesteuert und veranlasst wird, die Mail mit einem Attachment an alle im Adressbuch eingetragenen Personen zu verschicken.[377] Oftmals wird noch eine Schadensfunktion oder eine Funktion implementiert, um die weitere Verbreitung des Wurms zu sichern.[378]

Im Gegensatz zu den obigen, textbasierten Systemen nutzen echte Würmer die implementierten Netzwerkdienste eigenständig und können sich deshalb auch selbstständig verbreiten.[379] Ein berühmtes Beispiel ist der Wurm „Happy99“ alias „Win32/Ska“.

---

programm herunter, das dann startet. Mit Hilfe der Routingtabelle kann der Wurm herausfinden, mit welchen anderen Computern der infizierte Host verbunden ist und sich so mit Hilfe des Bootstraps verbreiten.

[372] http://www.computerviren-info.de/Andere.html (zuletzt abgerufen am 15.04.2004).

[373] Ebd.

[374] lateinisch hocus/engl. hoax: Scherz, Schabernack, Falschmeldung.

[375] Unter http://www.tu-berlin.de/www/software/hoaxlist.shtml kann eine Liste der bislang bekannten Hoaxes herunter geladen werden.

[376] http://www.trojaner-info.de/hoax.shtml (zuletzt abgerufen am 13.04.2004).

[377] Szallies/ Längsfeld 2001, S. 4.

[378] http://home.t-online.de/home/winni.w/virinfo_scriptwuermer.htm (zuletzt abgerufen am 15.04.2004).

[379] Szallies/ Längsfeld 2001, S. 4.

2.4.1.1.5 Schäden durch Computerviren/-würmer und ihre Entstehungsgründe

2.4.1.1.5.1 Schäden durch Computerviren/-würmer

Es gibt ein breites Spektrum an Schadensroutinen und ihren Auswirkungen auf Computersysteme und Computernutzer. Das Ausmaß der Schäden durch Viren reicht von der Zerstörung von Programmen und Dateien auf Disketten und Festplatten bis zur Beeinflussung der eingesetzten Hardware. Die Beeinflussung der Computersysteme durch Computerviren kann fatale Folgen für alle Lebensbereiche haben, die vom Computer und Netzwerksystemen abhängig sind. Um ein reines Aufzählen zu vermeiden, werden die möglichen Schadensarten in drei Bereiche klassifiziert: temporäre, unmittelbare und mittelbare Schädigungsformen.

Temporäre Schädigung (Behinderung der Arbeitstätigkeit)

- erhöhte Laufzeiten durch größere Dateien
- Blockierung von Festplattenspeicherplatz
- Blockierung von Ressourcen
- Erzeugung von Deadlock-Situationen[380]
- Erzeugung und Meldung von vermeintlichen Fehlern
- Setzen falscher Datumsangaben
- Umbenennen von Dateien
- Bildschirm-, Ton-, Geräuscheffekte
- Veränderung von Tastatureingaben.

unmittelbare Schädigungen (Vernichtung von Daten, Programmen, Systembereichen, Hardware)

- Crasher-Viren[381]
- Überschreiben von Daten-, Programm-, Systembereichen
- Zerstörung/Verwürfelung der FAT [382]

[380] Ein Deadlock (auch Verklemmung genannt) ist in der Informatik ein Zustand von Prozessen, bei dem mindestens zwei Prozesse untereinander auf Betriebsmittel warten, die dem jeweils anderen Prozess zugeteilt sind. Z.B. kann einem Prozess A der Bildschirm zugeteilt worden sein. Gleichzeitig benötigt A allerdings den Drucker. Auf der Gegenseite ist der Drucker dem Prozess B zugeteilt, der wiederum den Bildschirm fordert.
[381] Diese Viren verursachen einen Systemcrash. Der Rechner stürzt ab und es sind keine Zugriffe von außen mehr möglich.

- physisches Löschen bzw. Überformatieren von Dateien und Programmen
- Zerstörung von Hardware[383]
- Verstecken von Dateien/Verzeichnissen
- Manipulation von Datenträgerzugriffen

mittelbare Schädigungen (Virensuche, Datenrekonstruktion, Virenschutz)

- Rechnerausfallzeiten für Virensuche, Virenbeseitigung, Rekonstruktion der Daten und Neuinstallation
- Überprüfung aller Datenträger, Backups
- Kosten für Virenbeseitigung
- Kosten für Virenschutz-Programme
- Vertrauensverlust

2.4.1.1.5.2 Computerviren/-würmerentstehung

Neue Virenformen mit neuartigen Funktionen werden meist von Spezialisten programmiert. Der Programmierer muss über eine allgemein hohe Sachkenntnis verfügen, die Betriebssysteme (z.B. UNIX, Windows, MacOS, Linux, DOS) genau kennen und in verschiedenen Programmiersprachen (z.B. C, LISP, Perl, Java, VBS, HTML) programmieren können. Daher wird es nur wenige dieser Spezialisten geben, die aus eigener Kraft ein solches Programm entwickeln können.[384] Bei den Spezialisten kann es sich unter anderem auch um jugendliche Hacker handeln, die zum Teil über sehr gute Programmierfähigkeiten verfügen.
Viele Viren sind lediglich abgeänderte Viren, die einen anderen Namen tragen, die geänderte Botschaften senden, veränderte Aktionen ausführen, so dass auch mittelklassige Programmierer solch veränderte Viren in den Umlauf bringen können. Ebenso sind Makroviren recht einfach zu programmieren. Makroviren werden in leicht verständlichen Hochsprachen programmiert, so dass es für alle, die sich ein wenig mit der Makroprogrammierung beschäftigen, ein leichtes ist, Makroviren zu erstellen.

---

[382] FAT steht für engl. File Allocation Table (auf Deutsch: Dateizuordnungstabelle) und wurde als Dateisystem für Betriebssysteme wie MS-DOS entwickelt. Zu der Familie der FAT-Dateisysteme gehören FAT 12, FAT 16, VFAT, FAT 32. Die FAT ist eine verkettete Liste in einem Speicherbereich einer Partition (Festplatte), in dem Informationen zu jedem Cluster der Partition stehen.
[383] Dies ist nur indirekt möglich, indem die Software von Hardwareelementen gelöscht wird.
[384] http://www.gulli.com/security/viren/#herkunft (zuletzt abgerufen am 13.04.2004).

Dazu kommen die zahlreichen Viren, die mit Hilfe so genannter Virengeneratoren erstellt werden, so dass jeder Nutzer, der den Internet-Explorer bedienen kann, heute in der Lage ist, Viren anzufertigen.[385] Auf zahlreichen einschlägigen Internetseiten[386] werden Virengeneratoren angeboten, die genauso einfach zu bedienen sind wie eine Textverarbeitung unter Windows. Der Benutzer braucht lediglich dem Virenkonstruktionsprogramm mitzuteilen, welchen Zerstörungsgrad der Virus haben soll, wann er aktiviert werden muss, ob er den Hauptspeicher belegen darf oder sich in Programmen verstecken soll, welche Dateien infiziert werden müssen und welche Meldungen dem Opfer angezeigt werden sollen. Das Konstruktionsprogramm setzt den gewünschten Virus dann nach einem Baukastensystem zusammen.[387] Diese Art der Virenverbreitung wird zu einem großen Teil so genannten Script-Kiddies zugeschrieben.

2.4.1.2 DoS- oder DDoS-Attacken

2.4.1.2.1 Definition

„Denial-of-Service-Attacken“ (DoS-Attacken) sind sich auf Rechner auswirkende schädigende Angriffe. Die Angriffe bezwecken, die Verfügbarkeit einzelner Server und deren Dienste einzuschränken oder gänzlich zu verhindern. Ein Rechner kann auf unterschiedlichen Wegen unerreichbar gemacht werden. Man bombardiert ihn mit Softwarepaketen, die seine Ressourcen völlig ausschöpfen und ihn sogar zum Absturz bringen können.[388] Die Ressourcen eines Rechners sind die Prozessorleistung, Arbeitsspeicher oder die Bandbreite der Netzwerkanbindung. Bei einem solchen Angriff ist der Rechner so stark ausgelastet, dass es ihm nicht mehr möglich ist, den übrigen Aufgaben nachzugehen.[389]
„Distributed Denial of-Service-Attacken“ (DDoS-Attacken) sind DoS-Attacken, die von mehreren Standorten gleichzeitig ausgehen. Im Gegensatz zu einer einfachen Denial-of-Service-Attacke werden Distributed-Denial-of-Service-Attacken nicht nur über einen Angriffsrechner durchgeführt, sondern gleichzeitig im Verbund mit mehreren Rechnern. Dies hat zur Folge, dass es für die Betroffenen sehr aufwendig ist festzustellen, von welchen Standorten die An-

[385] Zimmermann 2002, S. 61.
[386] http://www.bioniciberica.com/dir.viren.htm ; http://www.nevertheless.ch/hacking/download-ff.htm ; http://www.washere.de/data_config.html ; http://www.blockversuche.de/enter-xxl.html ; http://www.thetackleshop.ws/hacker/cracker.cfm.htm ; http://www.ehandel.ws/frameset_zugang.htm ; http://www.trolliges.de/mdb_deutsch.html; http://www.portlist.de/highspeed-l.html ; http://www.warez-crackz-serialz.de/ ; http://www.jcw.cc/hackerseiten.html ; http://www.colors-band.ch/hacking/knacken.script.htm.
[387] Zimmermann 2002, S. 61.
[388] Der Systemabsturz wird in der Computerszene generell als Nuken bezeichnet.
[389] http://info.pcwebshop.ch/glossar/D.htm (zuletzt abgerufen am 21.04.2004).

griffe kommen. Für eine DDoS-Attacke platziert ein Angreifer einen so genannten Agenten auf unterschiedlichen Rechnern im Internet, vornehmlich auf Rechnern, die per Standleitung und Breitbandanschluss angebunden sind. [390] Diese Platzierung kann auch schon Monate vor den eigentlichen Angriffen erfolgen. Wird nun ein Angriff auf ein bestimmtes Opfer gestartet, erfolgen gleichzeitige Angriffe über die Rechner, auf denen die Agenten installiert sind. Diese erzeugen in der Gesamtheit ein enormes Angriffsvolumen, um das Ziel für alle anderen Anwendungen unerreichbar zu machen. Von DDoS spricht man ab ungefähr 50 beteiligten Angriffsrechnern. [391]

Die CSI/FBI-Untersuchung im Jahr 2004 bezifferte die Höhe der Schäden, die durch DoS-Angriffe verursacht wurden, auf über 26 Millionen US-Dollar.[392] Dabei handelte es sich zum Beispiel um Angriffe auf die New York Times[393], auf Computerfirmen wie Solaris[394] oder sogar auf deutsche Ministerien. Danach wurden durch einen Hacker-Angriff in Nordrhein-Westfalen Ministerien, Landtag und Landesbehörden vom Internet abgeschnitten.[395] Selbst Firmen, die sich auf Computersicherheit spezialisiert hatten, konnten sich vor DoS-Angriffen nicht schützen. Ein bekanntes Beispiel ist hierfür die Homepage des US-Zentrums für Computersicherheit CERT, die im Jahr 2001 von Hackern mit Denial-of-Service-Attacken angegriffen wurde.[396]

Über die Täter gibt es bislang nur wenige Informationen. Das liegt unter anderem daran, dass ein Aufspüren der Hacker ein sehr hohes Verständnis von Computer- und Netzwerktechnologie sowie gute Programmierkenntnisse erfordert. Um dies zu verdeutlichen, sollen im Folgenden kurz zwei Fälle aufgezeigt werden, die durch Hacker begangen wurden.

Im Jahr 2001 wurde der 17-jährige kanadische Hacker mit dem Szenenamen „Mafiaboy“ zu acht Monaten Haft in einer Jugendstrafvollzugsanstalt verurteilt. Dem Teenager wurde zur Last gelegt, im Februar des Jahres 2000 zahlreiche Cyber-Angriffe auf namhafte Unternehmen wie Yahoo, Amazon, Ebay und CNN gestartet zu haben. Dabei wurden deren Websites durch Denial-of-Service-Attacken für mehrere Stunden außer Betrieb gesetzt. Insgesamt

[390] Kubica 2001, S. 77.
[391] http://elge.iteam-cms.de/index.asp?cmsseiteid=166 (zuletzt abgerufen am 21.04.2004).
[392] Siehe unter Gliederungspunkt 1.4.3
[393] http://www.zdnet.de/news/tkomm/0,39023151,2098409,00.htm (zuletzt abgerufen am 21.08.2004).
[394] http://www.computerwoche.de/index.cfm?pageid=254&artid=31458&type=detail&kw=Hacker%20greifen%20Solaris%20an (zuletzt abgerufen am 21.08.2004).
[395] http://home.t-online.de/home/boa-archiv1/k0307260.htm (zuletzt abgerufen am 21.08.2004).
[396] http://www.computerwoche.de/index.cfm?pageid=254&artid=30401&type=detail&kw=Hacker%20gehen%20auf%20Sicherheitsexperten%20los (zuletzt abgerufen am 21.08.2004).

musste sich der Hacker in 58 Fällen verantworten. Den entstandenen Schaden bezifferte das Gericht auf rund 1,7 Milliarden Dollar. Richter Gilles Ouellet erklärte in seinem Urteil, dass der Angeklagte ein hohes Maß an Vorbereitung und Vorsatz an den Tag gelegt hätte. Er hätte in krimineller Absicht gehandelt. Die kanadische Rechtsprechung sieht in solchen Fällen für Jugendliche eine Höchststrafe von zwei Jahren Haft vor. Ein erwachsener Hacker könnte mit bis zu zehn Jahren Gefängnis bestraft werden. Nachdem Mafiaboy die acht Monate in der Jugendstrafanstalt verbüßt hatte, stand er ein Jahr unter Bewährung. Zudem verurteilte der Richter den 17-Jährigen zu einer Geldstrafe von 160 Dollar.[397]

Im Jahr 2003 verhafteten das FBI und der US-Geheimdienst Secret Service den Programmierer des Lovesan/W32.Blaster-Wurms Jeffrey Lee Parson. Lovesan/W32.Blaster verbreitete sich über das Internet und war darauf programmiert, den Windows-Updateserver von Microsoft mit einer konzertierten DOS-Attacke lahm zu legen. Der Wurm befiel über 48.000 Rechner und verursachte einen Schaden in Millionenhöhe. Der 18-jährige US-Amerikaner mit dem Beinamen „Teenkid“ wurde im August 2003 von den Beamten überführt und zu einer achtzehn monatigen Haftsrafe verurteilt.[398]

Moderne DoS-Attacken kombinieren mehrere Funktionen und werden von Hackern über Viren, Würmer oder Trojaner in fremde Systeme eingebracht. Dabei werden fremde Rechner für DDoS-Attacken derart missbraucht, dass die jeweiligen User keine Kenntnis davon haben, dass von ihrem PC aus DDoS-Attacken ausgehen. In diesem Zusammenhang ist ein Urteil zu erwähnen, dass in Großbritannien gegen einen mutmaßlichen Computerhacker erging. Dem jungen Mann wurde im Jahr 2003 vorgeworfen, eine DDoS-Attacke gegen das System des Hafens von Houston/Texas initiiert und den Rechner der Industrieanlage zum Absturz gebracht zu haben. Obwohl der Computer des Teenagers als Ausgangspunkt der Attacke zweifelsfrei ermittelt wurde, sprach die Jury den Angeklagten frei. Der junge Mann konnte vor Gericht glaubhaft machen, dass auf seinem Rechner ein Trojaner installiert und der PC ferngesteuert gewesen sei. Nach Ansicht des Staatsanwalts wollte der Angeklagte nicht den Hafen von Houston treffen, sondern den Rechner einer Chatraum-Bekanntschaft.[399]

[397] http://www.tecchannel.de/news/allgemein/6537/ (zuletzt abgerufen am 21.08.2004).
[398] http://www.html-world.de/news.php?show=527 (zuletzt abgerufen am 23.02.2006).
[399] http://www.news.av-software.at/modules.php?name=News&file=article&sid=1492 (zuletzt abgerufen am 21.08.2004).

Der hohe jährliche Schaden veranlasst US-Firmen zudem zu außergerichtlichen Aktionen. Im Januar 2004 verbreitete sich zusätzlich zum ersten MyDoom-Wurm auch die abgewandelte Form MyDoom.B im Internet. Im Unterschied zum ersten MyDoom-Wurm führt der Nachfolger nicht nur eine DoS-Attacke gegen SCO[400], sondern auch gegen Microsoft und andere Firmen aus. SCO und Microsoft honorierten daraufhin Hinweise zur Ergreifung und Verurteilung des bislang unbekannten Urhebers von MyDoom.B mit jeweils bis zu 250.000 US-Dollar.

Eine Liste mit über 300 der bekanntesten DoS-Attacken ist auf der Webseite http://www.attrition.org/security/denial/ zu finden. Dabei handelt es sich um Informationen über ältere und neuere DoS-Attacken, die nach Betriebssystem, Software und Hardware sortiert sind.

2.4.1.2.2 DoS-/DDoS-Arten

Es existiert eine Vielzahl von verschiedenen Möglichkeiten, ein System auszuschalten. Die bekanntesten und meist genutzten sollen hier in acht Gruppen unterteilt und erläutert werden.

2.4.1.2.2.1 Mail Bombing

Einer der ältesten Denial-of-Service-Attacken ist das inzwischen „klassische“ Mail Bombing. Beim Mail Bombing handelt es sich um einen Angriff, bei dem sehr viele oder sehr umfangreiche elektronische Nachrichten an einen Empfänger geschickt werden. Die Masse der Mails, die zum Teil mit datenintensiven Bildern angereichert sein können, führt zum Ausfall des Mailservers, auf dem der Empfänger sein elektronisches Postfach unterhält. In minder schweren Fällen fällt der Mailserver zwar nicht gänzlich aus, ist jedoch stark belastet, oder der Empfänger der Mails wird mit diesen derart überflutet, dass es für ihn unmöglich wird, die richtige Post herauszusuchen.[401] Es handelt sich hierbei nicht um ein Bagatelldelikt, sondern um ernst zu nehmende Belästigungen, vergleichbar einem Telefonterror. Manche erfahrene Nutzer sehen solche Kampfmaßnahmen in bestimmten Fällen als legitimes Mittel an, ebenfalls mit Mail Bombing zurückzuschlagen, wenn zum Beispiel der Betroffene selbst durch massenhaftes Versenden unverlangter Werbe-Mails unangenehm aufgefallen ist. Um anonym Mail

[400] SCO ist eine auf IT-Dienstleistungen spezialisierte Firma und bieten weltweit Partnern und Kunden lokale Support- und Serviceleistungen an.
[401] Anonymus 2003 S. 358 ff.

Bombing zu verschicken, gibt es auf verschiedensten Webseiten Anleitungen und Tools. [402] Dabei wird nicht bedacht, dass immer Unbeteiligte in Mitleidenschaft gezogen werden.[403] Schon allein die zunehmende Netzbelastung ist ein Ärgernis für alle, und die anderen Nutzer des betroffenen Servers müssen mit Störungen rechnen.[404] Die Gefahr des E-Mail-Bombing scheint allerdings im Alltag bislang nicht allzu groß zu sein, haben doch von den 500 im Auftrag der PC-Welt befragten Unternehmen gerade mal drei Prozent Erfahrungen mit E-Mail-Bombing gemacht. Diese allerdings gaben an, nicht nur einmal, sondern bereits mehrmals unter derartigen Sabotageakten gelitten zu haben. Hat die Belästigung durch E-Mails erst einmal begonnen, ist die Wahrscheinlichkeit offenbar hoch, dass sich dies wiederholt.[405]

Eine Mailbombe besteht im Prinzip aus einer einzigen E-Mail, die an einen SMTP-Mailserver zur Ausführung geschickt wird. Diese E-Mail hat jedoch die Besonderheit, dass sie die E-Mail-Adresse des Opfers gleich mehrmals als BCC-Empfänger enthält. Der ausführende Mailserver hat bei entsprechend hoher Angabe von BCC-Empfängern ebenfalls viele E-Mails zu generieren und zu versenden. Moderne Mailserver unterbinden diese Art von Mail Bombing. Da immer die gleiche E-Mail verschickt wird, lässt sie sich leicht als Angriff identifizieren. Schwer zu erkennen sind Angriffe, welche die E-Mail-Inhalte zufällig erzeugen und die Absenderadressen abwechselnd aus einer Liste entnehmen. Der Nachteil für den Angreifer ist, dass er jede E-Mail einzeln versenden muss. Eine weitere sehr unangenehme Variante des Mail Bombings ist die Anmeldung eines Opfers auf Unmengen von Mailinglisten. Das Opfer muss sich nämlich nach einer Attacke mühsam aus allen angemeldeten Listen manuell wieder austragen.[406]

2.4.1.2.2.2 Broadcast Storms

Broadcast Storms gehören ebenfalls schon zur älteren Generation von Denial-of-Service-Attacken. Sie richten besonders hohe Schäden in lokalen Netzwerken an, in denen jeder Rechner als Gateway[407] fungiert. An jedem Rechner wird bei einer Broadcast-Storm-Attacke

---

[402] http://www.hacker-archiv.de/page/literatur/allgemeine_literatur/mailbombing.html
[403] http://www.webwunder.de/ASP/abc.asp?abfrage=e-mail-bombing (Zuletzt abgerufen am203.04.2004).
[404] Heute ist E-Mail-Bombing schon auf vielen Mail-Servern nicht mehr möglich, da die Systemadministratoren hinreichende Abwehrmaßnahmen eingerichtet haben.
[405] http://www.glossar.de/glossar/1frame.htm?http%3A//www.glossar.de/glossar/z_email.htm (zuletzt abgerufen am 20.04.2004).
[406] Anonymus 2003, S.368.
[407] Heißt soviel wie „Übergang“, „Zugang“ oder „Schnittstelle“. Gateways sind Rechner, die die Verbindung bzw. den Datentransfer zwischen unterschiedlichen Netzen ermöglichen (zum Beispiel die Verbindung von einem Online-Dienst oder einem Firmen-Intranet mit dem Internet).

eine Flut von IP-Paketen[408] verschickt, die allesamt an nicht existierende Ziele adressiert sind. Wird dieser Datenstrom für mehrere Rechner innerhalb dieses Netzwerks aufrechterhalten, ist das gesamte Netzwerk sehr schnell überlastet, da die Rechner die falsch adressierten Pakete über die Gateways immer wieder in andere Subnetze verschieben.[409]
Um die Problematik von Broadcast Storms zu vermeiden, ist eine sorgfältige Planung des Netzwerks notwendig, um das „Hängenbleiben" von umherirrenden IP-Paketen von vornherein zu verhindern bzw. in kürzester Zeit zu eliminieren. Heutzutage erleben Broadcast Storms leider wieder eine Renaissance, da immer mehr lokale Netzwerke an das Internet angebunden werden und dabei immer weniger auf Sicherheit geachtet wird.

2.4.1.2.2.3 Smurf/Fraggle

Bei einem Smurf-Angriff sendet der Angreifer sehr viele Internet-Control-Message-Protocol-Pakete (ICMP-Pakete)[410], z.B. Ping-Anfragen, an die Broadcast-Adresse eines Netzwerks, so dass dieses Paket von jedem Rechner innerhalb des Netzwerks empfangen wird.[411] Der Angreifer tarnt sich jedoch nicht mit einer beliebigen oder einer nicht-existierenden Adresse, sondern mit der Adresse des eigentlichen Opfers. Die ICMP-Anfragen werden nun um die Anzahl der Rechner im Netzwerk vervielfacht; das Netzwerk dient quasi als Sprungbrett. Ist das Netz korrekt konfiguriert, werden die ICMP-Antworten am Router des Netzwerks abgeblockt und gelangen nicht bis zum Rechner des Opfers. Erlaubt das Netz jedoch solche ICMP-Broadcasts nach außen, werden die multiplizierten ICMP-Antworten an das Opfer weitergeleitet. Dadurch können Angreifer mit geringer Leitungskapazität (Modem, ISDN) die Opfer mit breitbandigen Anschlüssen mit ICMP-Paketen überfluten. Die ICMP-Antworten belegen die gesamte Leitungskapazität, und die reguläre Datenkommunikation wird unterbunden. Sehr häufig brechen auch die Server unter diesem Ansturm zusammen und müssen vorübergehend vom Netz getrennt werden. Die Angreifer selbst sind nur sehr schwer zu identifizieren, da sie

[408] „Internet Protocol", zusammen mit dem „Transmission Control Protocol" ist es das Herzstück der Internet-Technologie. Es wird fast immer in der Kombination TCP/IP genannt. Das Netzwerk-Protokoll IP verwaltet den Transport der Informationseinheiten im Netz. Es prüft nicht, ob Daten unterwegs verloren gehen. Für die Zustellung am Zielort sorgt dann TCP.
[409] http://www.id.unibe.ch/~asiegen/ena/Skripte/ena-secnet/ENA_04_Risiken%20von%20Protokollen.pdf (zuletzt abgerufen am 20.04.2004).
[410] Beim Internet Control Message Protokoll handelt es sich um ein Internet-Protokoll, bei dem zwischen Internet-Modulen Testdaten ausgetauscht werden, um Fehlern bei TCP/IP-Verbindungen auf die Spur zu kommen. Es wird dabei davon gesprochen, dass ein Rechner „angepingt" wird. PING ist ein Programm, das durch Versenden von Testdaten im Internet sucht, um festzustellen, ob eine Zieladresse existiert bzw. betriebsbereit ist.
[411] http://www.wolthusen.com/books/Netzwerksicherheit/slides/05_Attacks.pdf (zuletzt abgerufen am 20.04.2004); http://www.pentics.net/denial-of-service/white-papers/smurf.cgi (zuletzt abgerufen am 20.04.2004).

sich als das Opfer tarnen (IP-Spoofing)[412]. Die einzige sichere Abwehr ist, die Administratoren der als Sprungbrett dienenden Netzwerke über ihr Sicherheitsloch zu informieren und zu überzeugen, ihre Netze korrekt zu konfigurieren, um das Nach-Außen-Leiten von Broadcastpings (ICMP) zu unterbinden.
Ein Fraggle funktioniert genau wie ein Smurf, außer dass er UDP-Pakete (User Datagram Protocol) anstatt ICMP-Pakete versendet. UDP ist eines der Protokolle, auf denen das Internet beruht. Im Gegensatz zu TCP, das kontrolliert, ob bei der Datenübertragung die Pakete richtig sortiert bei einem ganz bestimmten Zielrechner ankommen, bietet UDP keine Fehlerkorrekturen. Es findet oft beim so genannten Broadcasting[413] Verwendung.[414]

2.4.1.2.2.4 TCP Syn Flooding (Land Attacks)

Diese Attacke nutzt den Handshake-Mechanismus beim Aufbau einer TCP-Verbindung aus. Bevor eine Verbindung zwischen zwei Rechnern aufgebaut wird, schickt der Absender ein spezielles TCP-Paket an den Empfänger, um eine Verbindung anzukündigen (SYN-Pakete, SYN = Synchronize). Der Empfänger sendet dann ein Antwortpaket (SYN/ACK-Paket, ACK = Acknowledgement = Empfangsbestätigung) zurück an den Absender. Das SYN/ACK-Paket muss vom Initianten mit einem ACK-Paket bestätigt werden, damit der Verbindungsaufbau komplett ist. Wenn der Absender eine falsche IP-Adresse benutzt, wird das SYN-ACK-Paket ins Nirgendwo geschickt und das Opfer sendet nach einem bestimmten Intervall die Quittung erneut, da er vom Verlust der Daten ausgeht. Nach einer bestimmten Zeit wird der Verbindungsaufbau abgebrochen. Während dieser Zeit wird Speicherplatz und Rechenleistung benötigt.[415] Führt nun ein Absender eine TCP-Syn-Flooding-Attacke aus, sendet er nicht, wie vom Empfänger erwartet, ein ACK-Paket aus, sondern sendet dem Empfänger weiterhin unzählige SYN-Pakete. Der Empfänger quittiert alle diese SYN-Pakete. Hier tritt nun der Fehler auf, da der Empfänger bei einem weiteren SYN-Paket nicht nur für das gerade empfangene SYN-Paket ein SYN/ACK-Paket verschickt, sondern auch für alle bisher empfangenen. Wenn die gefälschte IP-Adresse des Angreifers dazu nicht existiert, sendet der Router ein ICMP-Unreachable-Paket (Host/Netzwerk unerreichbar) zurück. Auf diese Weise wird auf dem

[412] Eine Methode, um unerwünscht in fremde Systeme einzudringen. Bei dieser Methode wird der Ziel-Host mittels eines modifizierten Verbindungsprotokolls hereingelegt, so dass er glaubt, der Eindringling sei jemand Berechtigtes.
[413] Englisch für „Sendung“. Gemeint ist damit das Versenden von Nachrichten in einem Netzwerk an alle Teilnehmer.
[414] Huegen 2000.
[415] Gühne 2002, S. 14 ff.

Empfängernetzwerk schnell ein hoher unerwünschter Datenverkehr erzeugt, wodurch das Opfer nicht mehr zu erreichen ist.[416]

2.4.1.2.2.5 Ping Flooding

Das Ping Flooding gehört zu den Denial-of-Service-Attacken, die keine Sicherheitslöcher ausnutzen. Pings werden benutzt, um die Erreichbarkeit von anderen Hosts im Netz zu prüfen. Ein angepingter Host quittiert hierzu einen Ping mit einer Echoantwort, einem so genannten Pong. Beim Ping Flooding wird ein Host jedoch mit unzähligen Pinganfragen bombardiert, die der Host alle bearbeitet, falls keine entsprechenden Mechanismen die Abarbeitung von sich rasch wiederholenden Ping-Anfragen verhindert. Entsprechend sind das eigene System und die Netzverbindung ausgelastet.[417] Ping Flooding ist eine Denial-of-Service-Attacke, die beim Opfer teuer werden kann. Wird eine Netzverbindung eines Hosts nämlich nach dem erzeugten Datenaufkommen abgerechnet, können hohe Summen entstehen.

2.4.1.2.2.6 Ping-AT-Attacks

Ende der 1970er-Jahre wurde eine einheitliche zeilenorientierte und öffentliche Befehlssprache für Modems entwickelt, die mittels AT-Befehlen angesprochen werden. Heutzutage wird diese Sprache in allen Modems verwendet, so dass die Modems von den Betriebssystemen und der Software einheitlich angesprochen werden können. Sobald sich ein Modem im Offlinemodus befindet, kann es über AT-Befehle angesprochen werden. Findet ein Wechsel in den Onlinemodus statt, kann das Modem nicht mehr mittels der AT-Befehle angesprochen werden, da es sich im Übertragungsmodus befindet. Dies kann verhindert werden, indem man dem Modem die Zeichenkette des dreimaligen Drückens des Escape-Zeichens sendet, das als „+++“ gekennzeichnet wird. Dabei wird in den Kommandomodus gewechselt. Aus Sicherheitsgründen muss zwischen diesem Umschaltkommando in den Kommandomodus und dem ersten AT-Befehl mindestens eine Pause von einer Sekunde vorhanden sein. Einige Modemhersteller verzichten aus patentrechtlichen Gründen auf eine solche Pause, so dass bei jenen Modellen der Umschaltbefehl in den Kommandomodus und ein kompletter AT-Befehl direkt hintereinander eingegeben werden können. Diese Voraussetzung eignet sich für einen Angriff. Man schickt an einen Empfänger über das Internet ein Ping-Paket, welches zum Beispiel

[416] http://www.id.unibe.ch/~asiegen/ena/Skripte/ena-secnet/ENA_04_Risiken%20von%20Protokollen.pdf (zuletzt abgerufen am 20.04.2004).
[417] http://www.netplanet.org/sicherheit/ (zuletzt abgerufen am 20.04.2004).

die Sequenz „+++ATHO“ enthält, was das Umschalten in den Kommandomodus und das Beenden der Verbindung bedeutet. Laut Ping-Protokoll antwortet der Rechner des Empfängers auf die Ping-Anfrage mit der Spiegelung des Pakets. Kennt das Modem nun die oben genannte Pause zwischen dem Umschalten und dem darauffolgenden AT-Paket nicht, wird es den Paketinhalt des Antwort-Pings als abzuarbeitende Sequenz interpretieren und die Verbindung trennen.[418]

2.4.1.2.2.7 Large Packet-Attacken (Ping of Death)/ IP-Fragment-Angriff (Teardrop)

Eine besonders schwerwiegende Denial-of-Service-Attacke sind die Large-Packet-Attacken, auch bekannt unter „Ping of Death“. Die Wirkungsweise von Large-Packet-Attacken ist zugleich einfach und fatal. Das IP-Protokoll verpackt alle Daten beim Absender in 64 KB große Datenpakete. Diese werden jedoch protokollintern vor der Übertragung in kleinere Päckchen zerlegt, um sie einfacher übertragen zu können. Beim Empfängerrechner werden diese einzelnen Päckchen wieder zusammengefügt; allerdings erst, wenn alle Einzelteile vorliegen. TCP/IP kann jedoch maximal 64 Kilobyte große Pakete verarbeiten. Ist das ankommende Paket am Ende größer als 64 KB, läuft ein interner Speicherpuffer über und bringt im ungünstigsten Fall den Rechner zum Absturz. Es handelt sich hierbei also um eine Denial-of-Service-Attacke, bei der ein TCP/IP-Netzwerk mit einem Datenpaket einer nicht zulässigen Größe lahm gelegt wird.[419]

Ein IP-Fragment-Angriff, auch Teardrop genannt, ist ähnlich wie der Ping of Death aufgebaut. Anders als beim Ping of Death sind hier die Pakete nicht zu lang, sondern überlappen sich. Das bedeutet, dass dort wo das eine IP-Fragment endet, ein zweites schon angefangen hat. Dies verursacht beim Zusammensetzen zu einem IP-Datenpaket einen Systemabsturz.[420]

2.4.1.2.3 DDoS-Tools

Für die Ausführung von DDoS-Attacken muss der Angreifer über einen qualifizierten Wissensstand verfügen. Um ihm die Angriffe zu erleichtern, wurden mittlerweile DDoS-Tools geschaffen, die dem Angreifer viele Arbeitsschritte abnehmen.[421] Man könnte diese Pro-

[418] Gühne 2002, S. 14 ff.
[419] http://home.t-online.de/home/TschiTschi/ping.htm (zuletzt abgerufen am 20.04.2004).
[420] Gühne 2002, S. 14 ff.
[421] http://www.computec.ch/dokumente/denial_of_service/ddos-angriffe_und_schutz/ddos-angriffe_und_schutz.html (zuletzt abgerufen am 20.04.2004).

gramme mit den Virengeneratoren vergleichen, die den Angreifern das eigene Programmieren abnehmen. Mittlerweile existieren sechs Haupttools[422]: Trinoo, Trible Flood Network (TFN), TFN2K, Stacheldraht, Shaft, Mstream. Sie unterscheiden sich durch größere Änderungen in ihren Angriffsarten, in ihrer Kommunikation oder anderen zusätzlichen Funktionen. Darüber hinaus gibt es eine Vielzahl weiterer Tools, die nur einige kleine Änderungen erhalten haben und im Wesentlichen einem dieser Basistools entsprechen.[423]

2.4.1.3 Weitere Sabotageakte

2.4.1.3.1 Guestbookbombing

Viele Webseiten bieten Gästebücher an, in denen die Besucher der Seite ihren Namen und einen Kommentar zurücklassen können. Eine Form der Sabotage besteht darin, als Kommentar übergroße Dateien im Bereich von einigen hunderttausend Zeichen in das Gästebuch einzutragen. Dadurch wird das Gästebuch für andere Benutzer unbrauchbar, unter Umständen wird auch das ganze System, auf dem der Webserver läuft, unbrauchbar, beziehungsweise stürzt ab.

2.4.1.3.2 Crackz

Ein Cracker[424] ist eine Person, die sich damit auseinandersetzt, den Kopierschutz oder den Registrierungszwang limitierter Programme zu entfernen. Beim Knacken von Anwendungen benutzen Cracker verschiedene Verfahren, um die Programmabläufe des Originals nach Schwachstellen zu untersuchen. Sind Lücken erst einmal entdeckt, werden Crackz programmiert, um anderen Personen die Umgehung bestimmter Schutzmechnismen zu erleichtern. Mit Crackz sind kleine Programme oder Registry-Dateien gemeint, die es gestatten, die Zeitbeschränkungen oder sonstigen Limitierungen einer Software aufzuheben oder zu übergehen. Die Verfahrensweise zur Anwendung eines Crackz ist unterschiedlich. Zumeist wird der Crack in das Stammverzeichnis des noch nicht freigeschalteten Programms kopiert und dort gestartet.[425] Die häufigste Form ist dabei das Herausfinden der Seriennummer (serial), die bei

[422] http://www.intersecu.org/texte/security/angriffe.txt (zuletzt abgerufen am 20.04.2004).
[423] Es besteht zudem die Möglichkeit, dass weitere neuartige Tools existieren, aber bisher noch nicht gefunden worden sind. Wie viele Systeme es im Internet gibt und wie viele schon verwendet wurden, lässt sich nur vermuten.
[424] to crack (engl.) = knacken.
[425] http://www.gulli.com/lexikon/crackz.html (zuletzt abgerufen am 26.04.2004).

der Installation jeder kommerziellen Software gebraucht wird und beim Kauf einer solchen vom Hersteller mitgeliefert wird. Crackz und Serials sind überall im Internet, zumeist in archivierter Form, zu finden.[426]

Daneben werden Personen, die mit der Absicht der Computersabotage in fremde Rechner eindringen, ebenfalls als Cracker bezeichnet. [427] In der Computerszene wird dabei zwischen Hackern und Crackern unterschieden. Hacker dringen in Computersysteme ein, um ihr Wissen zu erweitern, wogegen Cracker zusätzlich Sabotageakte begehen.[428] Diese Unterscheidung und deren unterschiedliche kriminelle Motivationen werden im dritten Teil der Arbeit genauer betrachtet.

2.4.2 Spionagehandlungen

2.4.2.1 Trojaner

Trojaner[429] sind Programme, die sich als nützliche Anwendungen tarnen, im Hintergrund aber ohne das Wissen des Anwenders andere Programmcodes ausführen können. Der geschriebene Computercode wird meistens mit Anwendungsprogrammen, Dienstprogrammen oder Spielen eingefügt.[430] Trojaner können sich im Gegensatz zu Viren und Würmern nicht replizieren, werden aber teilweise durch andere Programme mitinstalliert oder durch Würmer heruntergeladen.[431] Nach dem Start des Tarnprogramms wird auch die schädliche Ladung auf dem Rechner aktiviert. Strategie des Trojaners ist es, sensible Daten auszuspionieren und den Rechner zu kontrollieren. Die Absicht vieler Trojaner ist, unbemerkt so viele sensible Benutzerdaten wie möglich auszuspähen. Wenn der Internetbenutzer persönliche Daten wie zum Beispiel Passwörter für das Onlinebanking[432] oder für Mailaccounts, Kreditkartennummern

---

[426] Zum Beispiel unter: http://www.crackz.ws (zuletzt abgerufen am 26.04.2004), http://www.crackz-serialz.com/ (zuletzt abgerufen am 26.04.2004).
[427] http://www.net-lexikon.de/Cracker.html (zuletzt abgerufen am 26.04.2004).
[428] Im Folgenden werden Cracker, wenn nicht anders gekennzeichnet, ausschließlich im letzteren Sinn gebraucht.
[429] Der Trojaner (oder das Trojanische Pferd) hat seinen Namen aufgrund seiner ähnelnden Funktionsweise in Bezug auf den nach Homers Erzählungen stattfindenden Krieg zwischen Griechenland und Troja erhalten. Genauso wie das Trojanische Pferd (samt den darin befindlichen Soldaten) als Geschenk getarnt war, schleusen sich Computer-Trojaner als angeblich nützliche Programme unbemerkt in Systeme ein und bringen unerwünschte Funktionen mit sich.
[430] Anonymus 2003 S. 415.
[431] http://www.borg-perg.eduhi.at/informatik/viren1/verwandt.html (zuletzt abgerufen am 16.04.2004).
[432] Laut einer Schlagzeile der silicon.de haben Hacker einen Trojaner ausgesetzt, der die Tastenschläge dokumentiert und eingegebene Passwörter an die Hacker weiterleitet. Hauptsächlicher Zweck dieser Trojaner ist es, Passwörter von Online-Banking-Kunden auszuspionieren. Zu finden unter http://www.silicon.de/cpo/news-itsecurity/detail.php?nr=15278 (zuletzt abgerufen am 16.07.2004).

und Ähnliches übermittelt, schreibt der Trojaner diese mit. Die leistungsfähigsten Trojaner sind in der Lage, die wirklich interessanten Informationen herauszufiltern, und übermitteln sie dann per E-Mail an den Empfänger, sprich den Absender der Trojaner-Attacke. Meist handelt es sich dabei um einen Hacker, der sensible Daten benötigt, um unbemerkt diese für sich zu nutzen. Viele Trojaner installieren sich auf dem System, damit dieses bei jedem Systemstart ebenfalls mitgestartet wird, somit läuft dieses Programm ständig im Hintergrund mit. Andere Trojaner starten erst, wenn ein bestimmter Vorgang (Start eines anderen Programmes) auf dem System stattfindet.[433]

Im August 2004 ist der erste Trojaner für Pocket-PCs aufgetaucht. Der Trojaner breitete sich auf den PDA-Betriebssystemen Windows Mobile und Windows CE aus. Die Hauptfunktion des Programms besteht darin, dem Autor die maximale Kontrolle über das infizierte Gerät zu verschaffen. Nach dem Start erstellt WinCE.Brador.a eine Verknüpfung mit dem Namen svchost.exe im Autostartordner von Windows und erhält so beim Starten des PDAs die Kontrolle über das System. Danach übermittelt der Trojaner die IP-Adresse des infizierten Gerätes per E-Mail an den Virenautor. Dieser öffnet Port 2989 und wartet auf weitere Befehle. Die Ausbreitung der PDA-Viren wird den gleichen Verlauf wie die der PC-Viren nehmen.[434]

Zu bedenken ist weiterhin, dass Trojaner auch für die Polizei und Geheimdienste interessant sind, um Nutzer zu ermitteln, die sich auf illegalen Seiten bewegen. Laut der Zürcher Zeitung NZZ Online gehen Schweizer Polizeifahnder mit Hackermethoden gegen Kriminelle vor. Bei der Überwachung von möglichen Straftätern an ihren Computern setzt die Schweizer Polizei Trojaner ein und versucht auf diese Weise, an Passwörter, E-Mails und Dateiinhalte von Verdächtigen zu gelangen. Obwohl die „Verwanzung“ von Computern in der Schweiz rechtlich sehr umstritten ist, nutzen Computerspezialisten diese Methode schon seit zwei Jahren.[435] Auch das FBI arbeitet angeblich an einem Trojaner, der Verschlüsselungstechniken umgehen kann.[436]

Die kanadische Polizei nahm im Mai 2004 den Entwickler des Trojaners „Randex“ fest. Die Royal Canadian Mounted Police (RCMP) teilte mit, dass es sich hierbei um einen 16-jährigen Hacker handelt. Ihm wird unter anderem der Straftatbestand Computersabotage gemäß dem

[433] Anonymus 2003, S. 415 ff.
[434] http://www.pressetext.at/pte.mc?pte=040806015 (zuletzt abgerufen am 26.08.2004).
[435] http://www.nzz.ch/2003/09/07/il/page-article92AK5.html (zuletzt abgerufen am 26.08.2004).
[436] http://www.chip.de/news/c_news_8826831.html (zuletzt abgerufen am 26.08.2004).

kanadischen Youth Criminal Justice Act for Computer-Related Offences zur Last gelegt. Die Polizeiaktion fand im Rahmen einer koordinierten Ermittlung in mehreren Ländern statt. Der Kanadier ist nach zwei US-Amerikanern und einem Briten der vierte Randex-Entwickler, der ermittelt und dingfest gemacht werden konnte. Der Trojaner Randex ist ein so genannter IRC-Bot, der, sobald er einen Computer infiziert hat, über das Chat-Protokoll IRC Kontakt zu seinen Urheber aufnimmt. Er empfängt Befehle, wie etwa nach CD-Keys von Spielen zu suchen, SYN-Flood-Attacken vom infizierten System aus zu starten oder unbemerkt weitere Software nachzuladen. So installierte der Trojaner beispielsweise auch einen SOCKS-Proxyserver, der zur Weiterleitung von Spam über die befallenen PCs genutzt werden kann.[437]

Im Juli 2004 wurde zudem der spanische Trojanerautor Óscar López Hinarejos von einem Gericht in Valencia zu zwei Jahren Haft verurteilt. Außerdem soll er den durch seinen Trojaner „Cabronator" geschädigten Computernutzern eine Entschädigung zahlen. Der 26-jährige Hinarejos war im April 2003 festgenommen worden und ist nun der erste Trojanerautor, der in Spanien ins Gefängnis gehen muss. Cabronator hat über 100.000 Systeme befallen. Der Trojaner hat die infizierten Computer nach persönlichen Daten ausspioniert und konnte zudem über das Chat-Protokoll IRC ferngesteuert werden. Derart zweckentfremdete Rechner werden von Hackern zum Versand von Spam oder für Denial-of-Service-Attacken genutzt.[438]

Der Begriff Trojaner umfasst verschiedenste Funktionen, man kann Trojaner jedoch in fünf Hauptgruppen unterteilen: logische Bomben, ANSI-Bomben, Dropper, Keylogger und RAT-Trojaner.

2.4.2.1.1 Logische Bomben

Zu den Trojanern gehören im weitesten Sinn auch so genannte logische Bomben[439], die bei Erreichen einer bestimmten Bedingung einen anderen als den vorgesehenen Programmcode ausführen.[440] Logische Bomben sind Codefragmente in Betriebssystemen oder Anwendungssoftware, die beim Eintreten bestimmter Umstände (Erreichen eines Datums, Löschen eines

[437] http://www.heise.de/newsticker/result.xhtml?url=/newsticker/meldung/47755&words=Trojaner%20verhaftet (zuletzt abgerufen am 26.08.2004).
[438] http://www.heise.de/newsticker/result.xhtml?url=/newsticker/meldung/48889&words=Trojaner%20Gericht (zuletzt abgerufen am 26.08.2004).
[439] Logische Bomben werden oftmals auch als Viren bezeichnet, da ihre Schadensroutinen manchmal denen der Viren gleichen. Jedoch können sich logische Bomben nicht selbstständig reproduzieren und müssen deswegen eher zu den Trojanischen Pferden gezählt werden.
[440] http://www.interest.de/cgi-bin/lexika/Logische_Bomben.html?pos=T8442679&ID=433531453175 (zuletzt abgerufen am 16.04.2004).

speziellen Datensatzes einer Datenbank, Erzeugen einer Datei mit einem speziellen Namen, das Drücken spezieller Tastenkombinationen, einer speziellen Systemaktivität) Schaden anrichten können.[441] Dabei können alle erdenklichen Schadensroutinen eintreten. Jedoch sind logische Bomben im Gegensatz zu Viren auf das System beschränkt, in dem sie sich befinden und können sich nicht selbst reproduzieren.[442] Ein friedliches Beispiel ist die Angewohnheit mancher Entwickler, durch bestimmte Tastenkombinationen einen grafischen Gruß vom Entwickler-Team ablaufen zu lassen. Eine unfreiwillige logische Bombe war die Nachlässigkeit der Software-Entwickler bei der Berücksichtigung des Jahres 2000.[443]

2.4.2.1.2 ANSI- und Makrobomben

Ein Spezialfall einer logischen Bombe ist die so genannte ANSI-Bombe.[444] Eine ANSI-Bombe ist eine Trojanerart, die in einfachen ASCI-Texten vorkommen kann. Bedingung für das Funktionieren einer ANSI-Bombe ist das Vorhandensein des ANSI.SYS-Treibers im Speicher des Rechners. Der ANSI.SYS-Treiber wird mit DOS mitgeliefert und von den meisten Anwendern in die CONFIG.SYS Datei eingebunden. Damit wird der ANSI.SYS-Treiber mit jedem Booten des Rechners in den Arbeitsspeicher geladen.[445] Einige wenige Programme benötigen den ANSI.SYS Treiber, um Bildschirmfarben einzustellen oder um den Tasten auf der Tastatur eine neue Funktion zu geben. Dies geschieht mit so genannten ANSI-Sequenzen. Diese ANSI-Sequenzen werden vom ANSI.SYS-Treiber abgefangen und als Befehle interpretiert, sobald man versucht, den Text, in dem sie vorhanden sind, auf dem Bildschirm auszugeben (z.B. mit dem TYPE-Befehl). Wurde von der ausgeführten ANSI-Sequenz z.B. eine Taste der Tastatur belegt, wird dieser Befehl ausgeführt, sobald die entsprechende Taste gedrückt wird. Betätigt nun der Anwender z.B. die Taste „g“, erscheint „z“ auf dem Bildschirm. Jedoch kann auch eine Taste mit „Format C:“ + „Return“ auf einer Taste gesetzt werden.[446] Auch Labels von Disketten können eine ANSI-Bombe enthalten.

Makrobomben sind Nachkommen der ANSI-Bomben. In Dateien von Microsoft Word, Wordperfect oder Staroffice können neben dem eigenen Text auch Befehle für das Programm

---

[441] http://www.digitalcraft.org/index.php?artikel_id=282 (zuletzt abgerufen am 16.04.2004).
[442] http://www-is.informatik.uni-oldenburg.de/~schoenb/Sicherheit/Malware/LogischeBomben.htm (zuletzt abgerufen am 16.04.2004); http://www.interest.de/cgi-bin/lexika/Logische_Bomben.html?pos=T8442679&ID=433531453175 (zuletzt abgerufen am 16.04.2004).
[443] http://www.belwue.de/spots/spots-98/9Viren.html (zuletzt abgerufen am 16.04.2004).
[444] http://home.t-online.de/home/m_both/Virenarten.htm (zuletzt abgerufen am 16.04.2004).
[445] Anonymus 2003, S.430.
[446] http://www.gulli.com/security/viren/virenarten.html#arten (zuletzt abgerufen am 16.04.2004).

eingebettet werden. Diese Befehle werden als Makros bezeichnet. Sie werden auf dem Computer des Benutzers ausgeführt und können dort wie trojanische Pferde oder sogar Viren agieren. Sie manipulieren Daten und vervielfältigen sich. Da sich die Gewohnheit einbürgert, Dateien für Microsoft Word per E-Mail zu versenden und viele Mailprogramme inzwischen beim Eintreffen einer solchen Datei automatisch Microsoft Word starten, um die Datei anzuzeigen, wird auf diesem Weg auch automatisch die Makrobombe ausgeführt.[447]

2.4.2.1.3 Dropper

Bei dieser Form der Malware handelt es sich ebenfalls um eine spezielle Art von Trojanern. Ihre Aufgabe ist es, einen anderen Trojaner, Virus oder Wurm in das System zu bringen, wobei die Dropper selber nicht mit diesem infiziert sind, sondern ihn lediglich installieren. Bei Ausführung des Programms findet die Infizierung des Systems statt. Der Dropper kann ein anderer Dateityp sein als der Virus, Wurm oder Trojaner, der sie eingeführt hat. Um ein System von einem durch einen Dropper infizierten Virus, Wurm oder Trojaner zu bereinigen, genügt es also nicht, selbigen zu entfernen, sondern der Dropper muss auch identifiziert und entfernt werden. [448]

2.4.2.1.4 Keylogger und Sniffer

Eine andere Art der Trojaner betätigt sich auf dem Wirtsrechner als Keylogger und Sniffer. Keylogger speichern lokal alle Tastaturanschläge, die auch in den Output-Files gespeichert werden, aber solange keine Tastenschläge über das Netz versandt werden, geht auch keine Gefahr von den Keyloggern aus. Diese zeichnen die Tastaturfolgen auf, die den Hacker interessieren. Dazu können Eingaben von Passwörtern für Online-Dienste, Mail-Accounts, Webseiten, FTP, Kreditkarten-Nummern, Konten usw. gehören.[449] In einigen Fällen werden sogar Home-Banking-Programme überwacht und die Daten verschickt. [450]
Sniffer fangen Netzwerkpakete ab. Ihr einziger Zweck besteht darin, den Netzwerkverkehr zu analysieren. So können sie Gefahrenbereiche aufspüren, und der Administrator hat es leichter,

[447] http://md.hudora.de/jura/rechtstatsachen/node42.html#macrobomben (zuletzt abgerufen am 22.04.2004).
[448] Anonymus 2003, S. 428.
[449] Als Brute Force-Attack (= engl.: Angriff mit brutaler Gewalt) wird dagegen der Versuch der Beseitigung von Zugangssperren (wie Passwortabfragen) mittels eines einfachen aber sehr zeitaufwendigen Probierens aller möglichen Kombinationen bezeichnet. Um sich vor solchen Attacken zu schützen, ist es sinnvoll, sein Passwort so zu wählen, dass möglichst viele Kombinationen erforderlich sind, um es zu ermitteln.
[450] http://www.trojaner-info.de/beschreibung.shtml (zuletzt abgerufen am 16.04.2004).

sich im Netzwerk zurechtzufinden und Problemlösungen zu konzipieren.[451] Sniffer lassen sich an einzelnen Computern im WWW, LAN oder WAN installieren. Sie protokollieren den Datenstrom und speichern die analysierten Daten in einer Datei zur Einsicht für den Nutzer, der den Sniffer installiert hat.[452] Die Verteilung der Daten arbeitet dergestalt, dass Jeder an das jeweils angeschlossene Netz die Daten in kleinen Paketen, so genannten Frames, an den Verteiler sendet und dieser die erhaltenen, aber nicht weiter verarbeiteten Daten an jeden Rechner weiterleitet. Auch wenn nur ein Rechner die Daten annimmt und verarbeitet, kommen sie überall an. Wird nun ein Datenpaket von einem Rechner verschickt, können alle anderen Rechner dieses Paket auch „hören", wenn es an ihnen vorbei zu der Zieladresse geschickt wird. Die Rechner reagieren nur nicht auf ein solches Paket, wenn es nicht ausdrücklich an sie adressiert ist. Ein Rechner nimmt nur ein Paket an, das an ihn adressiert ist.[453] Es wird zwar angenommen, aber nicht weiterverarbeitet, wenn die Header-Adresse[454] nicht stimmt. Der Sniffer versetzt das Interface[455] des Rechners in den Promiscuous-Modus,[456] der nun die Verarbeitung und Annahme der Pakete durch bestimmte Applikationen erlaubt, auch wenn sie nicht für ihn bestimmt sind. Ein Abfangen der Daten kann auf diese Weise erfolgreich sein. Vom Computer-Hacker wird der Sniffer nun so eingestellt, dass er nur die relevanten Daten annimmt und analysiert und an ihn weiterleitet. Das ist dann oft nur der erste Teil des Frames, oder der Sniffer wird so konfiguriert, dass er nach bestimmten Informationen sucht, z.B. Passwörtern und Nutzernamen.

Der Sinn solcher Trojaner ist also nicht das Zerstören der Software oder einzelner Daten, sondern vielmehr das Ausspionieren wichtiger Benutzer- und Netzwerkdaten.[457] Für den Hacker hat es den Vorteil, dass er nur an die für ihn relevanten Daten gelangt und diese nicht aus einer riesigen Datenmenge herausfiltern muss. Gefundene Passwörter und andere Eingaben sowie Screenshots werden über das Internet z.B. an eine bestimmte Mailadresse versandt.

---

[451] Ein Sniffer kann die verschiedensten Protokolle auswerten. Ob nun TCP/IP (Ethernet/WWW), IPX, AppleTalk, Banyan VINES oder LCC.

[452] Das so genannte Output-File.

[453] Anonymus 2003, S. 335 ff.

[454] Mit dem Begriff Header werden die Kopfzeilen einer E-Mail bezeichnet in denen Absender, Empfänger, Betreff und Datum eingetragen sind.

[455] Ein Interface ist eine Schnittstelle des Systems, welche dem Informationsaustausch mit anderen Systemen dient.

[456] Der Promiscuous Mode bezeichnet einen bestimmten Empfangsmodus für netzwerktechnische Geräte. In diesem Modus liest das Gerät den gesamten ankommenden Datenverkehr an die in diesen Modus geschaltete Netzwerkschnittstelle mit und gibt die Daten zur Verarbeitung an das Betriebssystem weiter.

[457] Zum Teil werden jedoch auch Passwörter heimlich geändert, so dass für den eigentlichen Benutzer sein Account gesperrt ist. Je nach Anwendungssoftware und dem Dienstleistungsanbieter ist es dann oft zeitaufwendig oder zum Teil unmöglich, den Account wieder zu entsperren.

Diese Arbeitsweise der Trojaner ist als sehr gefährlich einzustufen, da diese die Eigenschaften besitzen können, an sämtliche Daten eines Anwenders zu gelangen.[458]

2.4.2.1.5 RAT-Trojaner oder Backdoors

Des Weiteren gibt es noch eine fünfte Untergruppe von Trojanern, die RAT-Trojaner (Remote Access Tools), auch Backdoors genannt. RAT-Trojaner ermöglichen einem Angreifer die volle Kontrolle über den PC und bestehen meist aus drei Teilen: 1. dem Server – der Teil, der auf dem Rechner des Opfers platziert wird und dann die Kontrolle über den Computer übernimmt. Das Serverprogramm öffnet in dem System verschiedene Ports, damit der Zugriff auf das System durch den Hacker möglich wird. 2. dem Client – einem kleinen Programm, mit Hilfe dessen sich der Angreifer mit dem Server auf dem Computer verbinden kann, um ihn zu kontrollieren. 3. dem Editor – einem Hilfsprogramm, mit dem Einstellungen und Verhaltensweisen des Servers vor der Platzierung festgelegt werden können.[459]

Der Server wird auf dem Rechner des Opfers installiert und bietet nach außen hin Dienste an, auf die man über den Client zugreifen kann. Dadurch ist es einer zweiten Person möglich, den Rechner des Opfers auszuspähen, Screenshots zu machen, diesen komplett fernzusteuern, Dateien zu kopieren oder zu löschen, den Rechner für DoS-Attacken gegen dritte Rechner zu missbrauchen, Passwörter auszulesen, Tastaturfolgen zu speichern, Dateien herunter- oder heraufzuladen und alle sonstigen Funktionen ferngesteuert zu leiten.[460] Diese Art der Trojaner sind zur Zeit als besonders gefährlich einzustufen.[461]

2.4.2.1.6 Netzwerktrojaner

Netzwerktrojaner agieren, wie der Name schon vermuten lässt, nicht in einem bestimmten System, sondern im Netzwerk. Dabei können sie eine Vielzahl von Aktivitäten ausführen, die sich dem Hacker als nützlich erweisen können. Netzwerktrojaner registrieren Zugriffsdaten-banken, erstellen Netzwerkfreigaben, um dadurch in andere Netze und auf deren Rechner zu gelangen. Außerdem scannen sie nach offenen Ports und ermitteln Rechner, die ungenügend geschützt sind, um diese für fremde Zwecke nutzen zu können.[462]

---

[458] http://www.trojaner-info.de/beschreibung.shtml (zuletzt abgerufen am 16.04.2004).
[459] http://www.emsisoft.de/de/malware/?Backdoor.Voodoo.6.dropper (zuletzt abgerufen am 16.04.2004).
[460] http://www.trojaner-info.de/beschreibung.shtml (zuletzt abgerufen am 16.04.2004).
[461] Ebd.
[462] Anonymus 2003, S. 425 f.

2.4.2.2 Kleine Trojaner

Eine große Gefahr für die Spionage geht auch von den Werbeunternehmen aus. Dank unterschiedlicher Programme ist es Unternehmen relativ problemlos möglich, Bewegungsbilder der Surfgewohnheiten zu erstellen. Die Werbeindustrie nutzt verschiedene Möglichkeiten, um an Daten von Internetsurfern zu gelangen. Dabei ähneln die Programme im Wesentlichen den klassischen Trojanern, sind jedoch auf spezielle kommerzielle Informationen ausgerichtet und werden im Folgenden deshalb als kleine Trojaner bezeichnet. [463] Es werden dabei die meistverbreiteten Formen aufgezeigt.

2.4.2.2.1 Cookies

Cookies (engl. für Kekse) sind kleine Textdateien, die beim Besuch einer Webseite auf dem Computer abgelegt werden und beim zweiten Besuch vom Bereitsteller der Homepage gelesen werden können. Die Informationen in einem Cookie mit einer maximalen Länge von 4.000 Zeichen stammen entweder vom Server der besuchten Webseite oder aus Angaben, die der Surfer macht. Wie lange ein Cookie auf dem Rechner bleibt, hängt vom Einzelfall ab. Normalerweise wird der Cookie gelöscht, sobald der Browser nach der Internetsitzung geschlossen wird. Allerdings ist es auch möglich, Cookies dauerhaft auf dem Rechner zu speichern.[464] Ursprünglich waren Cookies dafür vorgesehen, das Einkaufen im Internet bequemer zu machen. Man musste beim zweiten Besuch einer Seite nicht erneut alle Daten angeben. Heute wird die Cookietechnologie vielfach missbraucht. Mit Hilfe bestimmter Techniken können die gespeicherten Daten nicht nur von der ursprünglich besuchten Seite, sondern auch von Dritten gelesen und gespeichert werden. Die Folge ist, dass Daten weltweit und unkontrolliert gespeichert und verwertet werden und zu einem gewissen Maße mit Cookies Bewegungs- und Benutzungsprofile von Nutzern erstellt werden können.[465]

[463] Die Strafbarkeit solcher Vorgehensweisen ist teilweise ungeklärt. Festzuhalten bleibt jedoch, dass auch solche Programme Eingriffe in die informationelle Selbstbestimmung darstellen.
[464] http://www.net-lexikon.de/Cookie.html (zuletzt abgerufen am 27.04.2004).
[465] Ebd.

2.4.2.2.2 Spyware

Als Spyware (engl. Spionage-Programme) wird üblicherweise Software bezeichnet, die persönliche Daten des Benutzers ohne dessen Wissen oder gar Zustimmung an den Hersteller der Software oder an Dritte sendet.[466] Oft wird Spyware verwendet, um Produkte scheinbar kostenlos anzubieten. Manche Hersteller nutzen Spyware für die Überprüfung, ob der Nutzer das Programm auch ordnungsgemäß registriert und bezahlt hat.[467] Wenn dies nicht der Fall ist, kann der Hersteller das Programm z.B. online sperren. Vor allem aber für Werbezwecke und Datenspionage wird Spyware genutzt. Spywareprogramme analysieren das Surfverhalten des Nutzers im Internet, um gezielt Werbebanner oder Popups einzublenden, die auf die Interessen des Benutzers ausgerichtet sind. Die Unternehmen erhoffen sich daraus eine Steigerung in der Wirksamkeit dieser Werbemethoden.[468] Daneben geben viele Hersteller ihre Software als Free- oder Shareware heraus. Aus finanziellen Interessen schließen sie Verträge mit Unternehmen ab, die sich auf die Sammlung von Nutzerdaten spezialisiert haben. Die Datensammlung funktioniert eben über die in den Programmen eingebaute Spyware.[469] Das besonders Heimtückische an Spyware ist, dass sie sehr hartnäckig ist. Selbst wenn man verseuchte Programme vom Rechner löscht, verbleiben doch gewisse Dateien (meist DLL-Dateien) und Registry-Einträge weiter auf dem Computer, die uneingeschränkt Informationen über die Surfgewohnheiten an die entsprechenden Firmen übermitteln.

2.4.2.2.3 Clear-Gifs

Eine besonders perfide Art der heimlichen Datengewinnung sind Clear-Gifs, auch Web-Bugs genannt. Sie ähneln den Cookies. Clear-Gifs sind Grafiken auf Webseiten oder in E-Mails, die typischerweise so klein sind, dass sie für den Nutzer unsichtbar sind. Das dahinter stehende System ist raffiniert: Wenn man eine spezielle Webseite, die ein Clear-Gif enthält, aufruft, stellt der Computer fest, dass hier eine Grafik vorliegt, und möchte diese vom Server dieser Webseite herunterladen. Der Server stellt wiederum fest, dass diese Grafik auf einem anderen Server liegt und gibt diese Informationen an den Computer weiter. Dieser versucht sodann vom zweiten Server die Grafik herunter zu laden und übermittelt hierfür notwendige Informa-

[466] Diese Art von Software kann mit den Trojanern verglichen werden.
[467] Eine spezielle Form der Spyware sind Phonehome-Programmen. Dabei handelt es sich um Software, die nach dem Spyware-Prinzip unbemerkt über das Internet Kontakt zu seinem Hersteller aufnimmt, Seriennummern weitermeldet und abgleicht, oder unerwünscht nach Updates anfragt.
[468] http://de.wikipedia.org/wiki/Spyware (zuletzt abgerufen am 26.04.2004).
[469] Zu den bekanntesten Firmen dieser Art gehören Radiate, Doubleclick und Engage.

tionen. Dergestalt gelangen alle Computerdaten an den zweiten Server, angefangen von der IP-Adresse über die URL der von dem Rechner besuchten Seiten bis hin zum Inhalt der Cookies, die auf dem Rechner gespeichert sind. Der Nutzer erfährt von diesen Abläufen nichts, da der gesamte Datentransfer im Hintergrund stattfindet.[470]

2.4.2.2.4 Banner-Ads

Banner-Ads funktionieren prinzipiell ähnlich wie die oben beschriebenen Clear-Gifs. Wenn der Nutzer eine Webseite speichern möchte, versucht der Computer, das Werbebanner einer Homepage mit herunterzuladen und wird ungewollt zu einem dritten Server umgeleitet. Dabei handelt es sich zumeist um einen zentralen Server, an den mehrere Werbeunternehmen angeschlossen sind. Besucht man später eine andere Homepage mit einem entsprechenden Banner, können die bereits gespeicherten Daten verglichen werden.[471]

Die rechtliche Behandlung von kleinen Trojanern ist umstritten. Soweit personenbezogene Daten verarbeitet werden, ist in Deutschland auf jeden Fall das Datenschutzrecht zu beachten. Personenbezogen sind Daten über bestimmbare natürliche Personen. Bestimmbar sind Personen, wenn sie mit überschaubarem Aufwand anhand der Daten ermittelt werden können. Das ist unter Umständen schon über die IP-Adresse möglich, sicher aber dann, wenn der Nutzer seinen Namen und andere Angaben hinterlässt.[472] Die rechtliche Behandlung von Cookies ist jedoch in den einzelnen Staaten sehr unterschiedlich ausgestaltet.[473] In den USA wurde zum Beispiel im Januar 2000 ein lang andauernder Rechtsstreit beendet. An den Gerichten in Brooklyn, Manhattan, Kalifornien und Louisiana waren Sammelklagen gegen den Einsatz von Cookies eingebracht worden. Die Bezirksrichterin Naomi Reice Buchwald lehnte die Sammelklage gegen DoubleClick ab, bei der der Internet-Media-Agentur vorgeworfen wurde, durch den Einsatz von Cookies die Privatsphäre von Computernutzern zu verletzen.[474]

[470] http://www.sicherheit-online.net/html/lexikon.html (zuletzt abgerufen am 27.04.2004).
[471] http://www.sicherheit-online.net/html/lexikon.html (zuletzt abgerufen am 27.04.2004); http://www.rokop-security.de/main/article.php?sid=16 (zuletzt abgerufen am 27.04.2004).
[472] http://www.cybercourt.de/download/2001-2-ipitnews.pdf (zuletzt abgerufen am 28.08.2004); Näheres unter http://www.onlinelaw.de/download.php?content=9.
[473] Näheres unter http://www.fu-berlin.de/jura/mapo/magister/oliverhermann.pdf
[474] http://derstandard.at/?url=/?channel=WEBSTANDARD%26ressort=NETZPOLITIK%26ID=532150 (zuletzt abgerufen am 26.08.2004).

2.4.2.3 Eingriffe in die Datenübertragung

2.4.2.3.1 Falsche Adressangaben und gefälschte E-Mails

Das Fälschen von Nachrichten, insbesondere das Einsetzen eines anderen Absenders und das Versenden von eigenen Nachrichten mit fremdem Absender kann verschiedene Gründe haben:[475] Zum einen kann versucht werden, durch das Verschicken von Nachrichten mit unhöflichen, obszönen oder schlichtweg falschen Inhalten den vermeintlichen Autor zu diskreditieren. Zum anderen können unberechtigte Handlungen vorgenommen werden, wenn die Authentifizierung nur anhand der E-Mail-Adresse vorgenommen wird und der Empfänger gefälschte relevante Daten übermittelt. Jede E-Mail, die nach dem Internetstandard aufgebaut ist, enthält im so genannten From-Eintrag den Absender. Dieser setzt sich in der Regel aus dem Realnamen und der eigentlichen E-Mail-Adresse zusammen. Nun bestehen bei diskreditierenden Texten verschiedene Möglichkeiten der Fälschung: a) Fälschen der Unterschrift: Die E-Mail-Adresse im From-Feld bleibt zwar erhalten, es wird jedoch mit einem falschen Namen unterschrieben. b) Der Fälscher gibt den Realnamen des Opfers an: Hierbei wird nur der Namensanteil verändert, die E-Mail-Adresse des Täters bleibt unverändert. c) Der Fälscher gibt die E-Mail-Adresse des Opfers an: Hier gibt der Fälscher den eigenen Namen an, trägt aber eine fremde E-Mail-Adresse ein. Dies führt dazu, dass das Opfer gefälschte Antworten und Beschwerden bezüglich einer Mail erhält, die gar nicht von ihm stammt. d) Fälschen des gesamten Adressfeldes: Hierbei wird das From-Feld komplett dem Original nachgebildet. Eine solche Fälschung ist in der Regel durch Experten anhand von Unstimmigkeiten in anderen Feldern der Nachricht feststellbar, allerdings kann mit technischem Wissen auch dies vermieden werden. e) Fälschen von elektronischen Signaturen (Zertifikatfälschung): Eine Nachricht kann elektronisch signiert werden, um obige Manipulationen auszuschließen. Sowohl im Bereich der Verschlüsselung als auch der digitalen Signatur ist es notwendig, Sicherheit über die Identität des Kommunikationspartners zu haben. Eine digitale Signatur dient als Unterschrift unter einer E-Mail. Durch die Signatur lässt sich sicherstellen, dass ein Dokument tatsächlich von dem angegebenen Absender stammt (Identifizierung) und es auf seinem Weg durch das Internet nicht verändert wurde (Authentifizierung).[476] Wie alle modernen Kryptographie- und Signatursysteme ist auch dieses asymmetrisch, arbeitet also mit einem

[475] Als „faken“ (engl. schwindeln, vortäuschen) wird im Allgemeinen bezeichnet, sich in der Computer-Kommunikation anderen Teilnehmern gegenüber als jemand anderen auszugeben, unabhängig vom jeweils benutzten Medium.

[476] Die Deutsche Telekom hat ein System für eine digitale Signatur entwickelt, die auf einer Chip-Karte (SmartCard) gespeichert ist.

öffentlichen und einem geheimen Schlüssel. Eine Zertifizierungsstelle, das so genannte Trust Center, erstellt und verwaltet die elektronischen Schlüssel. [477] Somit muss nicht mehr die Identität des Kommunikationspartners überprüft werden, sondern bei allen von einem bestimmten Trust Center unterschriebenen Schlüsseln kann davon ausgegangen werden, dass der Schlüsselinhaber mit der Person übereinstimmt, für die sie sich ausgibt. Diese Signatur lässt sich nicht fälschen, doch kann eine Signatur erstellt werden, die dem Original ähnlich ist und bei mangelnder Überprüfung mit dem Original verwechselt wird.[478] Dies ist zumindest in einem Fall in großem Umfang geschehen. Die von der Zeitschrift c't betriebene CA wurde angegriffen, indem Schlüssel in Umlauf gebracht wurden, die laut Bezeichnung von ,,ct magazine CERTIFICATE pgpCA@ct.heise.de“ unterzeichnet waren, aber nie den Zertifizierungsprozess der c't durchlaufen hatten.[479] Grundsätzlich kann jedoch davon ausgegangen werden, dass einmal zertifizierte Personen authentisch sind.[480]

2.4.2.3.2 DNS- oder Server-Spoofing

Um im Internet mit einem anderen Rechner kommunizieren zu können, benötigt man dessen IP-Adresse. Diese Adresse setzt sich aus vier Zahlen zwischen 0 und 255 zusammen, also zum Beispiel 194.95.176.226. Da solche Nummern nicht sehr einprägsam sind, wird einer solchen IP-Adresse fast immer ein Name zugeordnet. Das Verfahren hierzu nennt sich Domain Name System (DNS). So kann ein WWW-Server sowohl unter seiner www-Adresse als auch unter der IP-Adresse angesprochen werden, denn der Name wird bei der Abfrage in die IP-Adresse umgewandelt. Die Datenbanken, in denen Rechnernamen den dazugehörigen IP-Adressen zugeordnet sind und den IP-Adressen entsprechende Rechnernamen, befinden sich auf so genannten Nameservern. Für die Zuordnung zwischen Namen und IP-Adressen gibt es zwei Datenbanken (sog. Routingtabellen): In der einen wird einem Namen eine IP-Adresse zugewiesen, und in der anderen einer IP-Adresse der zugehörige Name. Diese Datenbanken müssen miteinander nicht konsistent sein. [481]

---

[477] http://www.net-lexikon.de/Digitale-Signatur.html (zuletzt abgerufen am 20.04.2004).

[478] Allerdings ist es immer nur eine Frage der Zeit, bis bestimmte Schlüssellängen „geknackt“ werden können. Als viel größere Schwachstelle gilt immer der Mensch, der dazu neigt, aus Bequemlichkeit oder Unwissenheit Sicherheitscodes öffentlich zugänglich zu machen.

[479] http://md.hudora.de/jura/rechtstatsachen/node51.html#ctangriff (zuletzt abgerufen am 22.04.2004).

[480] http://www.iid.de/iukdg/gesetz/SigV161101.pdf. (zuletzt abgerufen am 22.04.2004); http://www.net-lexikon.de/Digitale-Signatur.html (zuletzt abgerufen am 22.04.2004); http://www.mediakomm.net/documents/forschung/neusignatur_a-z.pdf. (zuletzt abgerufen am 22.04.2004).

[481] Anonymus 2003, S. 175.

Von DNS-Spoofing ist die Rede, wenn es einem Angreifer gelingt, die Zuordnung zwischen einem Rechnernamen und der zugehörigen IP-Adresse zu fälschen, d.h., dass ein Name in eine falsche IP-Adresse und umgekehrt umgewandelt wird. Dadurch wird die Umleitung von Datenpaketen an eine durch den Angreifer besetzte Adresse möglich.[482] Zudem wird bei einigen Authentifizierungsmethoden auf das DNS-System zurückgegriffen. Diese Dienste erlauben eine Authentifizierung anhand des Clientnamens. Der Server kennt die IP-Adresse des Clients und fragt über DNS nach dessen Namen. Ist die IP des Angreifers einem fremden Namen zugewiesen, kann dieser sich unberechtigterweise anmelden.

2.4.2.3.3 IP-Spoofing

IP-Spoofing ist eine Angriffsmethode, bei der falsche IP-Nummern verwendet werden, um dem angegriffenen IT-System eine falsche Identität vorzuspielen und dadurch an relevante Informationen zu gelangen. Es unterscheidet sich von DNS-Spoofing dadurch, dass nicht DNS-Server manipuliert werden, sondern die eigene IP-Adresse.[483] Der Rechner gibt quasi eine falsche Identität an. Bei vielen Protokollen der TCP/IP-Familie erfolgt die Authentifizierung der kommunizierenden IT-Systeme nur über die IP-Adresse, die aber gefälscht werden kann. Der Header eines jeden IP-Pakets enthält dessen Quelladresse. Dies sollte die Adresse sein, von der das Paket gesendet wurde.[484] Indem der Header dergestalt verfälscht wird, dass er eine andere Adresse aufweist, kann ein Angreifer das Paket so aussehen lassen, als ob es von einem anderen Rechner gesendet wurde.[485] Täter können so Sicherheitsmaßnahmen wie zum Beispiel IP-adressbasierte Authentifizierungen umgehen oder die Identität ihres Rechners verbergen.

2.4.2.3.4 ARP-Spoofing

In LANs, in denen das Address Resolution Protocol (ARP) eingesetzt wird, sind ARP-Spoofing-Angriffe möglich. ARP dient dazu, zu einer IP-Adresse die zugehörige Hardware- oder Ethernet-Adresse zu finden. Wird in einer internen Tabelle des Rechners kein entspre-

---

[482] http://www.computerlexikon.com/begriff.php?id=2638&highlight=spoofing (zuletzt abgerufen am 23.04.2004).
[483] http://www.net-lexikon.de/IP-Spoofing.html (zuletzt abgerufen am 23.04.2004).
[484] Der IP Header wird normalerweise vom Kernel mit den richtigen Daten ausgefüllt. Dies kann jedoch umgangen werden. Näheres unter http://www.ibr.cs.tu-bs.de/lehre/ws0304/sec/uebung/blatt4.pdf. (zuletzt abgerufen am 23.04.2004).
[485] http://www.net-lexikon.de/IP-Spoofing.html (zuletzt abgerufen am 23.04.2004);
sehr genau dargestellt und erläutert unter http://www.computec.ch/dokumente/spoofing/ip-spoofing2/ip-spoofing2.html (zuletzt abgerufen am 23.04.2004).

chender Eintrag gefunden, wird ein ARP-Broadcast-Paket mit der unbekannten IP-Nummer ausgesandt. Der Rechner mit dieser IP-Nummer sendet dann ein ARP-Antwort-Paket mit seiner Hardware-Adresse zurück.[486] Der Angreifer (im lokalen Netz, da die ARP-Pakete dieses nicht verlassen) preist per Broadcast seine eigene MAC-Adresse für die umzulenkende IP-Adresse an. Die angeschlossenen Rechner nehmen diese Information vorsorglich in ihren Cache auf. Ein Angreifer kann nun mittels eines Sniffers den gesamten Datenverkehr betrachten, abfangen und wenn benötigt speichern. Der Angreifer hat somit die komplette Kontrolle über den Datenverkehr zwischen zwei oder mehreren Netzwerkteilnehmern und kann die Informationen nach Belieben einsehen und sogar manipulieren. Diese Art von Angriffen werden auch Man-In-The-Middle-Attack genannt.[487] Da die ARP-Antwort-Pakete auf diese Weise manipuliert werden können, reicht es häufig aus, die Kontrolle über einen der Rechner im LAN zu bekommen, um das gesamte Netz zu stören.

2.4.2.3.5 (Browser-) Highjacking

Ein weiterer Eingriff in die Datenübertragung ist das so genannte Highjacking. Highjacking wird das „Entführen" des Internetsurfers auf eine nicht gewünschte Internetseite genannt. Dabei werden über Würmer oder Viren die Browser-Einstellungen dergestalt verändert, dass der Browser nicht die vom User gewünschte Startseite, sondern eine gänzlich andere aufruft.[488] Dieses Highjacking nutzt eine Sicherheitslücke in der Virtual Machine von Microsoft aus. Daher ist auch nur der Internet Explorer von Microsoft hiervon betroffen.[489]

2.5 Zwischenfazit

Als Quintessenz des ersten und zweiten Abschnitts können folgende Kernelemente hervorgehoben werden:

---

[486] Genauestens erläutert: http://www.informatik.uni-hamburg.de/RZ/lehre/18.415/vortrag/11_Honeypots.pdf

[487] http://www.net-lexikon.de/Man-In-The-Middle-Attack.html (zuletzt abgerufen am 23.04.2004).

[488] Zumeist handelt es hierbei um Pornoseiten. Neuere Varianten des Highjackings verändern nicht die Startadresse des Explorers, sondern den entsprechenden Eintrag in der Registry.

[489] http://www.trojaner-info.de/anleitungen/hijackthis/htlogtutorial.html (zuletzt abgerufen am 26.04.2004); zweifelhafte Berühmtheit erlangt hierbei die Suchmaschine Cool Web Search. Die hinter diesem Webangebot stehende Firma Coolwebsearch (CWS) verbreitet immer neue Varianten trojanischer Pferde, mit dem Zweck, den Surfer auf die eigene Seite umzuleiten. Die erste Form des Highjackings auf die Seiten von Coolwebsearch wurde bereits im Mai 2003 entdeckt. Seit dem ist eine Vielzahl von Varianten hinzugekommen. Eine chronologische Auflistung der bisher bekannten Varianten befindet sich auf der Seite www.merijn.org/cwschronicles.html.

Es beschäftigen sich bislang wenige Kriminologen mit dem Phänomen der Computerkriminalität. Computerkriminalität wird zumeist im Bereich der Wirtschaftkriminalität verortet. Hier wird die Tätergruppe der Hacker jedoch teilweise gänzlich ausgelassen.

Die PKS zeigt einen erheblichen Anstieg der Computerkriminalität, die auch durch den exponentiellen Anstieg der gemeldeten Zwischenfälle bei CERT bestätigt wird. Diese Entwicklung verdeutlicht die Brisanz des Themas. Der Anstieg der Computerdelikte in der PKS ist allerdings zum größten Teil auf die Steigerung der Kreditkartenmissbrauchsfälle zurückzuführen. Computersabotage und das Ausspähen von Daten haben hier nur einen geringen Anteil. Die Untersuchungen der CSI und des FBI geben hier jedoch ein ganz anderes Bild der Lage. Danach machen DoS-Attacken mit Abstand den größten Anteil bei den Übergriffen aus. DoS-Attacken fallen jedoch in den Bereich der Computersabotage, die bevorzugt von Hackern begangen werden. Dies lässt vermuten, dass die Mehrzahl der Computerdelikte nicht durch die PKS erfasst werden kann. Die Gründe hierfür können unterschiedlicher Art sein. Zum einem zeigt die CSI/FBI-Untersuchung auch, dass seit 1999 bis heute unverändert mehr als ein Drittel der Unternehmen nicht weiß, wie viele Übergriffe in ihrem Unternehmen stattfinden. Diese Unternehmen kümmern sich folglich ungenügend um die Computersicherheit und können Vorfälle auch nicht der Polizei melden. Aber auch Unternehmen, die über die Anzahl und die Art der Übergriffe in ihren Unternehmen Bescheid wissen, verweigern oftmals eine Meldung, da sie einen Imageverlust vermeiden möchten. Zudem lässt sich vermuten, dass die Mehrzahl der Privatnutzer sich nicht über das Ausmaß und die Art der Computerkriminalität im Klaren ist. Die meisten Nutzer bemerken Übergriffe oder Fremdsteuerungen der Rechner erst gar nicht. Die PKS erfasst daher nur einen ganz kleinen Teil der Computerdelikte, weshalb davon ausgegangen werden kann, dass ein sehr hohes Dunkelfeld im Bereich der Computerdelikte existiert. Generell kann festgehalten werden, dass es viele Unklarheiten im Bereich der Computerkriminalität gibt, speziell wie man Computerkriminalität misst, welche Delikte hierzu zu zählen sind, wie sie definiert wird und wie hoch die Dunkelziffer ist.

Anhand von Beispielen wurde auch aufgezeigt, dass schwerwiegende Computerdelikte von Hackern begangen werden. Dabei haben einzelne Hacker durch den zerstörerischen Einsatz ihres hohen technischen Verständnisses zum Teil Schäden in Millionenhöhe verursacht. Es wurde gezeigt, dass auch Jugendliche als Täter in Frage kommen. Auch wenn die globalen Schäden nicht konkret zu beziffern sind, kann festgestellt werden, dass es zum ersten Mal in der Geschichte der Kriminalität Jugendlichen und zum Teil Kindern möglich ist, Schäden in

solch einem hohen Ausmaß zu verursachen. Daneben ist es jugendlichen Hackern zum ersten Mal möglich, in Bereichen kriminell zu werden, zu denen sie bislang keinen Zugriff hatten. Übergriffe auf das Pentagon, auf Banken, große Unternehmen und den gesamten wirtschaftlichen Bereich sind neue kriminelle Betätigungsfelder von Jugendlichen, die erst mit dem Computer möglich wurden. Der Schwerpunkt der jugendlichen Kriminalitätsforschung muss sich somit neben den klassischen Jugenddelikten wie Gewalt- und Abziehdelikten auch zunehmend mit der Computerkriminalität beschäftigen. Dabei ist aber zu bedenken, dass nur ein Teil der Computerdelikte von jugendlichen Hackern begangen werden.

Computerdelikte haben zudem eine hohe Schadensqualität. Die Spannweite der Schäden erstreckt sich vom „Kavaliersdelikt“ bis hin zu Milliardenschäden durch Virenattacken. Neben der Intensität deckt Computerkriminalität ein weites Spektrum an Delikten ab. Sabotage, Betrug, Urheberrechtsverletzungen und Ausspähen von Daten sind nur einige von vielen möglichen Deliktsarten. Computerkriminalität erfasst alle Bereich des Lebens, die in irgendeiner Form digitalisiert sind. Es stellt sich als ein Deliktfeld dar, das sehr schnellen Veränderungen unterworfen ist. Die Schnelligkeit der Veränderung der Delikte hängt mit der Schnelligkeit der Veränderung der Computertechnik zusammen. So komplex die Erfindungen im Bereich der Software und Hardware ausgestaltet sind, so komplex gestalten sich auch die neuen Deliktformen. Dabei verschmelzen mittlerweile Tathandlungen. Zum Beispiel werden Viren generiert, die Trojaner auf fremde Rechner bringen, mit denen Hacker Zugriff erhalten und diese Rechner ferngesteuert dazu benutzen können, Spams zu verschicken.

Diese Komplexität macht es den Strafverfolgungsbehörden immer schwerer, erfolgreich zu bleiben. Viren und Würmer verbreiten sich in Minuten über die ganze Welt. Der Täter kann hierbei beliebig von jedem Ort der Welt den Virus programmieren und verschicken. Eine strafrechtliche Verfolgung erfordert eine internationale Zusammenarbeit, da Computerdelikte oftmals globale Folgen verursachen. Internationale Zusammenarbeit erfordert aber auch gleiche Ansichten über Computerkriminalität. Bislang haben die einzelnen Staaten unterschiedliche Regelungen bezüglich Computerstraftaten, so dass einzelne Handlungen, die in Deutschland strafrechtlich relevant sind, in anderen Ländern nicht verfolgt werden können. Eine erfolgreiche Strafverfolgung erfordert im Bereich der Computerdelikte zunehmend internationale Abkommen zu klaren Vorgehensweisen und Verfahren bei speziellen Computerdelikten.

Neue rechtliche Einstellungen gehen mit der Computerkriminalität einher. Das heißt, bislang strafrechtlich nichtrelevante Verhaltensweisen müssen neu untersucht und hinterfragt werden. Dafür sind unter anderem ein technisches sowie ein rechtliches Verständnis der Materie erforderlich. Als Beispiel kann das Spoofing genannt werden. Spoofingformen, bei denen nach offenen Ports gesucht wird, sind strafrechtlich noch nicht erfasst. Es stellt sich jedoch zumindest die Frage der Sittenwidrigkeit, da Spoofing oft als Vorbereitungshandlung genutzt wird, um herauszufinden, welche Rechner im Netz zum Teil ungeschützt sind, um diese im Folgenden für kriminelle Handlungen zu missbrauchen. Auch in Bezug auf das Tauschen von Musikdateien muss in Zukunft bei den Tätern eine neue rechtliche Gesinnung aufgebaut werden, damit sie nicht in eine Dauerkriminalität finden. Computertechnik und Computerkriminalität hängen somit eng miteinander zusammen und müssen von den Strafverfolgungsbehörden und Kriminologen verstanden werden, um Handlungen adäquat einstufen zu können.

3. Computerszenen

3.1 Einleitung

In diesem Kapitel sollen Tätergruppen dargestellt und erläutert werden. Dadurch, dass Computerkriminalität in allen Bereichen zu finden sein kann (Computerkriminalität i.e.S. und i.w.S.), gehören auch alle Bevölkerungsschichten und -gruppen zu den möglichen Tätern. In den Medien wird jedoch fast immer der Begriff Hacker verwendet, wenn von Computerkriminalität gesprochen wird. Gemeint ist damit meist Computerkriminalität i.e.S. Der Begriff „Hacker“ ist somit zum Schlagwort für Computerkriminelle geworden und wird häufig sehr undifferenziert gebraucht. Selbst Horst W. Opaschowski, der sich auf Jugend und Medien spezialisiert hat, benutzt den Begriff des Hackers sehr undifferenziert. Zwar spricht er davon, dass Computerkriminalität durch Computerviren und Manipulationen in den nächsten Jahren sehr stark zunehmen wird, nennt dafür aber relativ unreflektiert die Hacker als Tätergruppe, ohne zu spezifizieren, um wen es sich dabei wirklich handelt.[490]

Entgegen den in Deutschland auf das Thema Pornographie im Internet konzentrierten Presseberichten stellen computerbezogene Wirtschaftsstraftaten den Kernbereich der Computerdelikte dar. Während dabei in den 1970er-Jahren der Schwerpunkt Wirtschaftsdelikte auf Manipulationen lag, hat sich mit der Verbreitung der Computernetze inzwischen das „Hacking“ als

[490] Opaschowski 1999, S. 96.

eine Art Grunddelikt zur Begehung zahlreicher Computerdelikte etabliert. Der unberechtigte Zugang zu Computerdaten und -systemen ist als Teilaspekt der Computerkriminalität von erheblicher Relevanz, da dieser einerseits oftmals die Vorstufe zu weiteren Handlungen, wie z.B. Datenmanipulation, ist und andererseits als eigene Deliktskategorie, vor allem in Form der Datenspionage, selbstständig auftritt. Angriffsformen des Hackings dienen vor allem zur Begehung der Delikte der Computerspionage, des Softwarediebstahls und der sonstigen Produktpiraterie, der Computersabotage und Computermanipulation. Der dazugehörende Täterkreis wird „Hacker“ genannt. Dabei kann es sich im Bereich der Hackerszene um Kinder mit geringem computertechnischen Wissen (Script-Kiddies), um Hacker ohne böse Absichten oder auch um Cracker mit kommerziellen und kriminellen Hintergründen handeln. Die einzelnen Techniken der Hacker sind in erster Linie abhängig von dem jeweiligen Kommunikationssystem und dem Wissensstand. Häufig kommt es zu einer Gefährdung des angegriffenen Unternehmens oder der Institutionen.

Es soll somit die Frage untersucht werden, ob mit der Hackerszene eine neue Tätergruppe entsteht, die zum ersten Mal in der Geschichte der Kriminalität in allen Bereichen des Lebens (Wirtschafts-, politische, militärische und private Kriminalität) tätig sein kann. Wer „die Hacker“ wirklich sind, wie ihre Szene strukturiert ist, ihre Machenschaften, ihre Altersstruktur und ihre Beweggründe sind hierbei die zu erläuternden Gesichtspunkte. Ebenfalls stellt sich in diesem Zusammenhang die Frage, ob durch die vermutete junge Altersstruktur eine gänzlich neue Form der Jugendkriminalität entsteht.

Im vierten Teil der Arbeit wird versucht, anhand der Self-Control Theory herauszufinden, aus welchen Gründen Hacker oder ihnen nahe stehende Gruppierungen kriminell werden und ob diese Theorie dafür geeignet ist, Computerkriminalität i.e.S. zu erklären. Über Hacker liegen bislang wenig empirische Untersuchungen vor, so dass zunächst anhand ausgewählter Literatur die Hackerszene beschrieben wird, wobei der Schwerpunkt auf die Beweggründe kriminellen Handelns gelegt wird. Anschließend werden die bislang wenigen empirischen Untersuchungen vorgestellt.

3.2 Die Verwendung des Begriffs „Szene“

Die Entwicklung von verschiedenen Szenen wird als ein viel beachtetes Phänomen der neueren Kultur- und Gesellschaftsentwicklung angesehen. In den Mittelpunkt rücken dabei zu-

nehmend auch Computerszenen. Der Begriff „Szene“ ist hierbei sehr unbestimmt. Gerhard Schulze definiert „Szene“ als eine Vernetzung von Personen, Orten und Inhalten, wobei das Publikum zeitlich und räumlich definiert ist.[491] Die Inhalte beschreibt er als gemeinsame Interessen, gleiche Werte, selbstgestaltete Verhaltensgrundsätze innerhalb der Szene und ein gleiches Weltbild.[492]

Dabei soll nicht unbeachtet bleiben, dass der Begriff Szene häufig als Zuschreibung von „außen“ statt als Sicht von „innen“ verwendet wird. Er soll die Vielfalt der Gruppierungen und Zusammenschlüsse von Seiten jener, die sich nicht innerhalb der Szene befinden, zu kategorisieren bzw. zu schematisieren versuchen. Obwohl gemeinsame Interessen, gemeinsame Einstellungen und ähnliche Lebensgefühle ein zentrales Thema der Szene darstellen, kann sich die Innenansicht der Szene für die einzelnen Gruppenmitglieder ganz anders darstellen.[493]

Als „Szene“ wird in dieser Arbeit somit die Gruppierung von Menschen verstanden, die bestimmte gemeinsame Perspektiven und Interessen verfolgen und sich dafür Aktionsfelder und Netzwerke schaffen. Der Begriff Szene wird dabei sehr weit gefasst und umfasst Gruppen, die in einem Bereich zumindest über einen gewissen Zeitraum gemeinsame Interessen und Aktivitäten verfolgen.[494]

Im Lauf der Zeit sind mit dem Computer und dem Internet neue Interessen und neue Szenen entstanden, die bevorzugt von Jugendlichen aufgegriffen wurden. Dabei bleibt zu beachten, dass die Computerszene keine homogene Einheit darstellt. Viele Szenen berühren und überschneiden sich in ihren Haupt- und Randbereichen, so dass auch die Hackerszene sich mit anderen Computerszenen kreuzt. Im Folgenden sollen deshalb zur Verdeutlichung der Entwicklung und der Vielfalt des kulturellen Milieus wichtige Computerszenen dargestellt werden.

3.3 Cyberpunk-Szene

Die Cyberpunk-Szene stellt sich als ein Lebensstil einer Fankultur dar, die sich maßgeblich um das Subgenre Science-Fiction gruppiert hat.[495] Auch wenn der Begriff Cyberpunk mitt-

[491] Schulze 1997.
[492] Mörth 2003, S.20.
[493] Mörth 2003 S.21.
[494] Mörth 2003 S.19.
[495] Dabei sind unter anderen Autoren wie William Gibson, Bruce Sterling oder Neal Stephenson zu nennen.

lerweile inflationär und unspezifisch in den Medien genannt wird, so steht dahinter dennoch eine Jugendszene, die sich um die digitale Welt des Cyberspace gebildet hat. Winter beschreibt den Cyberpunk folgendermaßen: „Ein Cyberpunk steht den neuen Kommunikations- und Informationstechnologien sehr positiv gegenüber, gleichzeitig hat er aber ein kritisch-politisches Bewusstsein in Bezug auf deren gesellschaftliche Verwendung entwickelt. Er sieht sich riesigen Korporationen gegenüber, die immer mehr an Stelle von Nationalstaaten treten. Das eigentliche Leben findet in den Computernetzen statt, in denen einerseits mit Informationen als Ware um Macht und Profit gekämpft wird, andererseits ekstatische und mystisch-visionäre Zustände gesucht und erlebt werden können."[496] Die Cyberpunks verstehen sich als Kolonisatoren des Virtuellen und Vorreiter bei der Erschließung neuer Stilisierungs- und Inszenierungsformen, aber auch als Wegbereiter des globalen Dorfes, in dem intensive Kompetenz-, Erlebnis- und Gemeinschaftserfahrungen möglich werden.[497] Ähnlichkeiten weist auch die japanischen Computer-Otaku-Szene[498] auf, deren Mitglieder verstärkt Mangas, Cartoons und anderen synthetischen Idolen nacheifern.[499]

3.4 LAN-Szene

Die LAN-Szene (local area network) stellt die größte Szene dar, die das Netzmedium für sich ergründet hat. Es handelt sich dabei um Computerspieler, die im Multiplayer-Modus in einem Computernetzwerk gemeinschaftlich spielen. Dabei handelt es sich um alle Arten der Computerspiele wie Schach, Fußball, Poker, das Ballerspiel Quake, das Kriegsspiel Command & Conquer oder das Simulationsspiel Siedler.[500] Diese Spiele finden auf untereinander (selbst-) vernetzten Computern statt oder auf Veranstaltungen, bei denen die Veranstalter solche Netzwerke zur Verfügung stellen. Von zwei bis über tausend Spielern kann dabei die Gruppengröße reichen, wobei die so genannten LAN-Partys oder LAN-Events die eigentlichen Szene-Highlights darstellen.[501] Mittlerweile haben sich große Teile dieser anfangs losen Spielergemeinschaften[502] in Teams organisiert, den so genannten „Clans", die ihre Zusammengehörigkeit, vergleichbar einem Sportverein, durch äußere Symbole wie Fahnen, Banner, Logos

[496] Winter 1997, S. 48.
[497] Vogelgesang 2003, S.4 f.
[498] Es existiert in Japan eine Vielzahl verschiedenster Otakus, z.B. Manga Otakus, Monster Otakus, Military Otakus, Cartoon Otakus oder Idol Otakus.
[499] Hebecker 2001, S. 171 ff.
[500] Besonders beliebt sind hierbei sog. Ego-Shooter, bei denen die Spieler mit anderen gegen ein Team kämpfen und diese sich gegenseitig virtuell töten. Bekanntheit erhielten Ego-Shooter im Zusammenhang mit Amokläufen. Den virtuellen Spielen wurde hierbei vorgeworfen Agrssivität zu fördern.
[501] Vogelgesang 2003, S.7 f.
[502] Interessierte finden eine ausführliche Auflistung aller Online-Clans mit Mitgliederzahlen und weiteren Clubinformationen unter www.clanlisten.de.

oder Kleidung verstärken. In den „Sessions“ der Clans wird geübt und Teamplay trainiert, man lernt spezifische Spielumgebungen („maps“) kennen und entwickelt Spielstrategien. Jedes Clan-Mitglied hat dann einen speziellen Aufgabenbereich. Diese Clans treten auf Events gegeneinander an. Auch im Internet gibt es solche Spieleplattformen als Treffpunkte, die von Clanmitgliedern sowohl zu Übungszwecken als auch anonym für Treffen mit fremden Spielern genutzt werden. Eine der größten Ligen ist zum Beispiel die Counterstrike-Liga mit internationalen Turnieren. Allein in der Electronic Sports League (ESPL) spielen 5.000 Clans um die Rangfolge der besten Counterstrike-Spieler.[503] Je beliebter LAN-Partys in der Szene wurden, umso interessanter wurden sie für Sponsoren (Spiele- und Hardwareunternehmen, IT-Branche). Mittlerweile haben sich auch kommerzielle Veranstalter etabliert. Dies führte dazu, dass die besten Spieler mit Sponsorenverträgen umworben werden, internationale Einladungen mit Reisekostenerstattung erhalten, Turnierpreise[504] ausgeschrieben werden und es in der Szene immer mehr Profi-Gamer gibt.

3.5 MUD-Szene

Neben der LAN-Szene existiert ein bestimmter Typus Spielergemeinschaft, die MUD-Szene[505] (Multi User Dungeon), die Online-Rollenspiele, ähnlich den früheren Brettspielen, durch Computernetze als virtuellen Inszenierungsraum nutzt.[506] Die Ausgestaltung dieser virtuellen Räume ist meist sehr komplex und beinhaltet vielfältige Raumforen, Einrichtungen und Institutionen. Die räumliche Umgebung basiert heute noch meistens auf Texten, die den jeweiligen Raum, die Objekte und die Umgebung beschreiben.[507] Frei wählbar sind unter anderem die Faktoren Geschlecht, ethnische Herkunft oder die soziale Klassenzugehörigkeit. Die sozialen Aktionen sind hierbei sehr vielseitig. MUDs können miteinander plaudern, diskutieren, streiten, lachen, spielen, einander berühren, schlagen, oder sexuelle Begegnungen haben. Sie können sich gegenseitig Eifersucht, Hass, Hilfsbereitschaft, Zuneigung oder sogar Liebe mitteilen.[508] Die Kommunikation im MUD ist dabei dem Chat-Modus im Internet vergleichbar. Dabei kann man zu zweit kommunizieren[509] oder auch allen Spielern Informatio-

[503] http://www.pc-erfahrung.de/Index.html?LANParty.html (zuletzt eingesehen am 10.08.04).
[504] Zum Teil werden professionelle LAN-Partys veranstaltet, bei denen Preisgelder von über 10.000 Euro für die Sieger vergeben werden.
[505] Dabei wird hier auf Differenzierungen verzichtet, in denen die Szene sich in MOO, MUCK, MUSE, DUM, usw. aufteilen.
[506] Turkle 1999, S. 219 ff.
[507] Coradi 1997, 2.2.1
[508] Coradi 1997, 2.2.2
[509] „Whisper“ genannt

nen übermitteln.[510] Für Mitteilungen, die alle betreffen, gibt es zudem einen öffentlichen Newskanal. Die Faszination dieser neuen Szene und die Möglichkeit u.a. soziologischer Forschungen wird durch die folgende Aussage von Waldemar Vogelgesang deutlich: „Weltweit verwandeln sich auf diese Weise alltäglich und allnächtlich Jugendliche – und hier vor allem Studenten – in Internetschauspieler, die mit Gesinnungsfreunden Kontakt aufnehmen und in der Anonymität ihrer Spielrolle(n) beliebige Identitätswechsel vornehmen können. Selbstinszenierung gerät im Spiel zu einer Auffächerung von Alternativen individueller Ich-Entwürfe, eine fiktive Erkundung des Möglichen, des Anders-Sein-Könnens. Die Inszenierungen in den virtuellen Kommunikationslandschaften verdeutlichen damit, dass Identität und Sozialität in einem komplexen Wechselwirkungsverhältnis stehen. Dies zu erkennen und produktiv zu nutzen, kann auch als existentielle Erfahrung für das Leben in der Postmoderne angesehen werden. Denn die für das heutige Dasein charakteristische Erfahrung, dass der Mensch in sehr verschiedenen Kontexten zu Hause ist und mit einer Vielzahl von höchst unterschiedlichen Orientierungen und Einstellungen, aber auch Situationen, Gruppierungen und Milieus konfrontiert ist, wird in den virtuellen Parallelwelten gleichsam simuliert – und damit trainiert. Sie werden zum Experimentierraum der Selbstdarstellung und Selbstfindung, verbunden mit einer sensiblen und flexiblen Haltung gegenüber der wachsenden Vielgestaltigkeit und Unübersichtlichkeit gegenwärtiger Lebensverhältnisse.“[511]

3.6 Programmierer-Szene

Die Programmierer-Szene versteht sich als Alternative und Gegenbewegung zu marktbeherrschenden Hard- und Software-Herstellern und -Anbietern. Am bekanntesten ist die sog. „Linux-Szene“, die mittlerweile eine weltumspannende Gemeinschaft bildet.[512] Linux ist ein sog. „Open-Source“-Projekt, das als Gegensatz zum Programm-Monopol von Microsoft für alle Anwendungen im Computerbereich frei zugängliche und damit von allen auch weiter entwickelbare Programme und Betriebssysteme beinhaltet.[513] Newsgroups sind die Portale der Linux-Szene. Darin werden alle denkbaren Programm- und Hardware-Fragen der Computerwelt

[510] „Shout“ genannt
[511] Vogelgesang 2003 S. 5 f.
[512] Zur Fülle der Aktivitäten und Themen der Szene siehe http://www.linux-community.de
[513] Bekannte Open-Source-Produkte sind unter anderem Mozilla (Websuite), Mozilla Firefox (Webbrowser), MySQL, PostgreSQL Apache (Webserveranwendungen), Samba (SMB-Protokoll) Linux-Kernel, GNU Compiler Collection Perl (Programmiersprachen).

beantwortet. Zudem werden lokale Stammtische und Workshops veranstaltet und private Treffen ihrer Mitglieder angeboten.[514]

Ein weiteres bekanntes Open-Source-Programm ist der Web-Server Apache, der mehr als 60 Prozent der Websites der Welt beherbergt, was verdeutlicht, dass die Programmierer-Szene zu einer Gemeinschaft wird, die auch auf wichtigen Ebenen Einfluss haben kann.[515] Im Sinn der Programmier-Szene soll Software frei zugänglich sein. Die Übergänge vom Programmierer zum Hacker und umgekehrt sind zum Teil fließend. Erst das Lernen von Programmiersprachen macht es möglich, in Systeme einzudringen. Andere, wohl eher die Jüngeren, kommen über die spielerischen Virenbaukästen zu Programmiersprachen. Insoweit können Programmierer häufig nicht von Hackern unterschieden werden.

Neben den genannten dominierenden Szenen existieren unzählige kleinerer Gruppierungen, die zumeist noch nicht als Szene definiert werden können. Darunter könnte man die Chatter und die Kontaktbörsen-Mitglieder zählen.

3.7 Hackerszene: Selbst- und Fremdbilder

3.7.1 Ursprünglicher Sinn und Jargon File

Seinen wörtlichen Ursprung findet das Wort „Hacker“ in dem englischen Wort „to hack“, was soviel bedeutet wie „zerhacken“.[516] Eine negative Interpretation liegt insoweit keineswegs fern, denn etwas zu zerhacken bedeutet, etwas unbrauchbar zu machen oder gar zu zerstören, das dann für den bestimmungsgemäßen Gebrauch wertlos ist. Jedoch ist eine solch einfache Herleitung unter Bezugnahme auf den Wortursprung (i.S.d. einfachen Übersetzung) keinesfalls realistisch.

Der Begriff „Hacker“ scheint vielmehr einer durch die Medienberichterstattung geprägten Definition unterworfen. Im öffentlichen Sprachgebrauch sind Hacker wohl meist Datendiebe, jugendliche Delinquente oder schlimmstenfalls Terroristen (Cyberterror), sicherlich jedenfalls „irgendwelche“ kriminell motivierten „Subjekte“, Computerfreaks, die für den gemeinen Nut-

[514] Mörth 2003, S.33 ff.
[515] Einen Überblick über wichtige Open-SourceProjekte findet man unter http://www.oreilly.de/german/freebooks/os_tb/os_tb_1.htm.
[516] Langenscheidts Lexikon engl.-dt. 2002.

zer bis hin zur global operierenden Wirtschaft immense Gefahren im Bereich Internet und EDV darstellen und denen es in egoistischer Weise häufig um die Verletzung von Urheberrechten im Software-, Musik-, Film-, aber auch dem Privatbereich geht.[517]

Damit ist im Allgemeinen die Definition des Begriffs Hacker negativ geprägt und impliziert delinquentes Verhalten. Dabei war der Begriff Hacker ursprünglich positiv besetzt. In den 1960er-Jahren kamen die ersten Computer an die Universitäten, die für alle Studierenden zugänglich waren. Bis dahin waren nur Großrechner verfügbar, und die Nutzung der Rechenzeit war sehr umständlich gewesen. Der Großrechner stand abgeschottet in einem eigenen Raum. Wer etwas rechnen wollte, musste seine Wünsche an der Tür abgeben und dort am nächsten Tag die Ergebnisse abholen, aus heutiger Sicht also eine sehr langwierige Prozedur. Demgegenüber standen in den kommenden Jahren zunehmend Maschinen zur Verfügung mit Tastatur und Bildschirm, an die man sich einfach setzen und programmieren konnte. Es gab bald einige Studenten, die von den Möglichkeiten des Rechners so fasziniert waren, dass sie nächtelang davor saßen und versuchten, ein Programm zu schreiben und es bis an die Grenze des Möglichen auszufeilen. Eine Hochburg dieser Szene war das Massachusetts Institute of Technology (MIT) in Boston, USA. Dort arbeiteten die ersten Programmierer, die als Hacker bezeichnet wurden bzw. die sich selber so bezeichneten. [518] In dieser Zeit entstand eine erste Definition des Begriffs Hacker:

„Hacker sind Personen, denen es Spaß macht, die Details eines programmierbaren Systems zu erforschen und dessen Möglichkeiten zu erweitern. Im Gegensatz zu den normalen Benutzern, die nur das Notwendigste lernen, um mit der Maschine zu arbeiten.“[519] Diese Definition von Hacker bezeichnete somit jemanden, der exzellente Programmierkenntnisse besaß.[520]

Damit zusammenhängend entwickelte sich in der Szene das Jargon File, das ebenfalls Hacker definiert und einer der meist zitierten Stellen im Internet ist, wenn es um eine geeignete Definition des Begriffs Hacker geht. Das Jargon File ist ein berühmtes Kompendium des Hacker-

[517] http://www.silicon.de/cpo/news-itsecurity/detail.php?nr=15419 (zuletzt eingesehen am 18.10.04); http://www.heise.de/tp/deutsch/special/info/13393/1.html (zuletzt eingesehen am 18.10.04); http://www.tomshardware.de/news/20040414_141836.html (zuletzt eingesehen am 18.10.04); http://www.heise.de/tp/deutsch/special/info/16053/1.html (zuletzt eingesehen am 18.10.04); http://www.heise.de/tp/deutsch/inhalt/konf/16412/1.html (zuletzt eingesehen am 18.10.04).
[518] Das Massachusetts Institute of Technology wurde 1861 gegründet und ist eine weltbekannte Universität in Cambridge, Massachusetts, USA. Das MIT gilt als eine weltweit führende Universität im Bereich von technologischer Forschung und Lehre.
[519] Raymond 1996.
[520] http://de.wikipedia.org/wiki/Hacker (zuletzt eingesehen am 03.09.04).

Jargons. Es enthält ein Lexikon über verschiedene Begriffe des Hackens und gibt Einblicke in unterschiedliche Bereiche der ursprünglichen Netz- und Hackerkultur.[521] In der aktuellen Version (Jargon File 4.4.7) sind fünf Definitionen enthalten: Demnach ist ein Hacker

1. jemand, der sich gerne mit programmierbaren Systemen und der Möglichkeit, deren Fähigkeiten zu steigern, auseinandersetzt – im Gegensatz zur Mehrzahl der Benutzer, die sich lediglich mit den notwendigen Schritten befassen.
2. jemand, der mit Begeisterung oder sogar zwanghaft programmiert bzw. sich lieber mit der Programmierung selbst als mit der Theorie der Programmierung befasst.
3. jemand, der den essenziellen Wert eines Hackerangriffs zu schätzen weiß.
4. jemand, der fähig ist, schnell und gut zu programmieren.
5. ein Experte im Umgang mit einem bestimmten Programm bzw. jemand, der oft mit einem Programm arbeitet oder Arbeiten über ein Programm veröffentlicht (wie beispielsweise „Unix-Hacker“).

Die Definitionen stellen das Programmieren von Computern in den Mittelpunkt. Die Fähigkeit zu programmieren ist eine notwendige Voraussetzung dafür, Hacker zu sein. Gleichwohl ist jedoch nicht jeder Programmierer ein Hacker. Es stehen daneben aber auch Motive wie Spaß, Erforschungsdrang, Begeisterung für das Programmieren, Enthusiasmus, Kreativität und neue Herausforderungen im Vordergrund.[522]

3.7.2 Netzwerkhacker

Als die Vernetzung von Computern begann, entstanden ganz neue Möglichkeiten und Faszinationspotentiale. Jetzt war es möglich, über das Telefonnetz mit anderen Computern in Kontakt zu treten und diese vom eigenen Computer aus fernzubedienen. Angefangen hat dies, wie oben bereits gezeigt, mit dem Arpanet. Damit zusammenhängend entstand auch eine neue Definition von Hackern, die sich nicht auf das reine Programmieren beschränkte. Vielmehr wurde auch die Nutzung der Netzwerke in diese Definition integriert. Danach sind Hacker Personen, „die sich aus verschiedensten Gründen unrechtmäßig Zugang zu fremden Netzwerken verschaffen, sei es aus Selbstbehauptung, der Faszination für das technisch Machbare, wirtschaftlichen Interessen oder auch, um im Auftrag von Firmen Sicherheitslücken in eige-

[521] Das Jargon File wird zur Zeit von Eric S. Raymond gewartet. Es ist ferner im Buchhandel unter dem Titel The New Hacker's Dictionary erhältlich. Es wurde aufgrund vieler Wortspiele und der Eigentümlichkeit etlicher Begriffe nicht ins Deutsche übersetzt.
[522] http://www.catb.org/~esr/jargon/html/index.html (zuletzt eingesehen am 03.09.04).

nen Netzwerken aufzudecken oder aus eigenem Engagement auf Sicherheitslücken in bestimmten Programmen hinzuweisen. Ein echter Hacker hinterlässt aber keine Schäden und bereichert sich nicht."[523] Die nichtkriminelle Intention sowie die Freiheit der Daten sind hiernach die ausschlaggebenden Faktoren. Hiermit zusammenhängend entstand eine so genannte Hacker-Ethik, die den Hacker und seine Handlungsweisen beschreibt. Nach Stephen Levy[524], Wau Holland und dem Chaos Computer Club (CCC) kann die Hacker-Ethik folgendermaßen beschrieben werden:[525]

1. Der Zugang zu Computern und allem, was einem zeigen kann, wie diese Welt funktioniert, sollte unbegrenzt und vollständig sein.
2. Alle Informationen müssen frei sein.
3. Misstraue Autoritäten – fördere Dezentralisierung.
4. Beurteile einen Hacker nach dem, was er tut und nicht nach üblichen Kriterien wie Aussehen, Alter, Rasse, Geschlecht oder gesellschaftlicher Stellung.
5. Man kann mit einem Computer Kunst und Schönheit schaffen.
6. Computer können dein Leben zum Besseren verändern.
7. Mülle nicht in den Daten anderer Leute.
8. Öffentliche Daten nützen, private Daten schützen.[526]

Diese Art von Hackern setzt sich zum Ziel, die Gesellschaft des Informationszeitalters über alle Hintergründe des Computers aufzuklären. Zwar dringt diese Gruppe für ihre Arbeit notwendigerweise in fremde Systeme ein, allerdings liegt es nicht in deren Zielsetzung, einen Schaden anzurichten, sondern Sicherheitslücken beispielsweise im Bereich des elektronischen Geldverkehrs oder bei Telefongesellschaften zu ermitteln, um diese dann davor zu warnen. Diese Gruppierung definiert sich selbst als Hacker und schließt alle anderen aus diesem Begriff aus, die gegen diese Hackerethik verstoßen. Dabei gibt es andere Hackerszenen, die von dem CCC auch als Hacker akzeptiert werden, die sich aber nicht ohne weiteres an die Hackerethik halten. Eine bekannte amerikanische Hackerszene stellt hierbei die Gemeinschaft von Hackern dar, die sich um die Webseite http://www.2600.com bilden. Hacker, die sich um die Webseite http://www.antionline.com formieren, sprechen sich gegen illegale Handlungen aus, jedoch bleibt es in jedem Fall dem Einzelnen überlassen, ob er die beschafften Informationen für oder gegen illegale Handlungen vornimmt. Daneben gibt es noch Hacker, die sich

[523] http://www.uni-kassel.de/~seidler/LEX_H.HTM#Hacker (zuletzt eingesehen am 03.09.04).
[524] Levy 1984 S. 39 ff.
[525] Gröndahl 2000, S.10 ff.
[526] http://www.ccc.de/hackerethics?language=de (zuletzt eingesehen am 03.09.04).

um die Webseiten http://www.cultdeadcow.com, http://www.phrack.org organisieren und unzählige andere Hackergruppierungen. Man muss wohl auch davon ausgehen, dass es viele kleine, zum Teil kriminelle Hackergruppierungen gibt, die aufgrund ihrer Größe und ihres technischen Knowhows nur von Insidern aufgespürt werden können.

Auffällig ist bei der Klärung des Begriffs Hacker, dass die Mitglieder des CCC sich selbst als Hacker definieren und dass Parteien, die Wirtschaft und die Medien in Deutschland quasi von „amtlichen" Hackern sprechen, die bei Problemen als Experten konsultiert werden. Dies zeigt, dass die Mitglieder des CCC als Hacker eine gewisse Rechtfertigung von außen erhalten. Das Image des deutschen CCC ist in den USA jedoch anders als das hier in Deutschland. Dort werden sie zum großen Teil als Bande „alienated, drug-addled crackers" beschimpft.[527] Einige Hackergruppen bezeichnen die Strategie des CCC, Sicherheitslücken etwa von Banken oder Telefongesellschaften zu hacken und danach zu veröffentlichen, als Cracker-Mentalität. In Deutschland genießen sie jedoch hierfür eher das Image eines „Daten-Robin-Hood", dessen Informationen der Gesellschaft und der Öffentlichkeit zur Verfügung gestellt werden. Dabei kann nie richtig festgehalten werden, welche Szene sich genau an welche Regeln halten will und ob auch wirklich alle Mitglieder sich an diese halten. Das Image der bösen Hacker wird im Folgenden genauer dargestellt.

3.7.3 Die Cracker

Der Jargon File unterscheidet zwischen Hackern und Crackern. Gemeint ist damit die negative Ausprägung des Hacker, der losgelöst von der Hacker-Ethik agiert. Der Begriff Cracker wird in der Szene im überwiegenden Maße in einem negativen, kriminell oder illegal geprägten Sinn verwendet. So werden in der Szene mit Crackern Gruppen angesprochen, die unbefugt in Computersysteme, Internetserver oder Bankrechner eindringen und dort willkürlich oder zielgerichtet Schädigungen und Änderungen an Programmen, Dateien, Webseiten u.ä. vornehmen. Die Unterscheidung der Begriffe Hacker und Cracker zeugt von einer starken Abneigung der Hackerszene gegen den Diebstahl und Vandalismus, die Cracker zu verantworten haben. Inwieweit es Überschneidungen beider Gruppen gibt und eine genaue Trennung möglich ist wird, im nächsten Kapitel der Arbeit genauer besprochen.

[527] Medosch/Röttgers 2001, S. 148 f.

Unter den Begriff Cracker fallen auch so genannte Script-Kiddies, die eine verwandte Form der Cracker sind. Es handelt sich dabei um Kinder und Jugendliche, die selber nicht programmieren, sondern vielmehr für ihre Angriffe Skripte und Programme von anderen Programmierern nutzen, um Schädigungen an fremden Rechnern zu verursachen.[528] Christian Rentrop beschreibt solche Script-Kiddies als das größte Problem, da von ihnen die meisten Gefahren ausgehen. Sie seien meist völlig unbegabt, verantwortungslos und launisch, dadurch unberechenbar und völlig frei von Ethik und Moral. Er nennt sie die „wahre Bedrohung für das Internet und jeden Computer-Nutzer".[529]

Von den hier beschriebenen Crackern sind die so genannten Software-Cracker zu unterscheiden. Dies sind Personen, die widerrechtlich Kopierschutzmechanismen kommerzieller Software durch Manipulation des Binärcodes zum Zwecke der illegalen Benutzung oder Verbreitung umgehen. Dabei sind sie zum Teil streng organisiert. Man kann sie in Anwendungssoftware- und Spiele-Cracker untergliedern. Verschiedene meist jugendliche Software-Cracker sind dabei nicht an Profit interessiert, sondern betrachten das Cracken von Spielen gegen die Zeit als Wettbewerb der Gruppen gegeneinander.[530] Was die Software-Cracker mit den hier im Folgenden gemeinten Crackern verbindet, ist allein die Tatsache, dass ihre Aktivitäten zum Teil oder vollständig illegal sind.

Der Begriff des Hackers wird in der Literatur, Politik und in den Medien sehr unterschiedlich und zum Teil unreflektiert benutzt. Die Szene selbst ist dabei ebenfalls nicht hilfreich. Die von der Hackerszene vorgenommene Unterscheidung der Gruppen verläuft hauptsächlich anhand der selbst gesetzten Ziele. Dabei zeichnet sich jedenfalls eine Zweiteilung in Hacker und Cracker ab.[531] Echte Hacker distanzieren sich in jeglicher Form von Crackern. Folgender Auszug aus der CCC Cologne verdeutlicht diese Haltung:
„Es gibt noch eine andere Gruppe, die sich lautstark als Hacker bezeichnet, diesen Namen aber in keinster Weise verdient. Es sind Menschen (meist pubertierende männliche Wesen), welche einen Spaß daran haben, in Computer einzubrechen und das Telefonnetz zu zerstören. Echte Hacker nennen diese Leute Cracker und wollen mit ihnen nichts zu tun haben. Wirkliche Hacker halten Cracker für ein faules, unverantwortliches und nicht besonders schlaues Pack, denn genauso wenig wie man durch das Knacken von Sicherheitscodes ein Hacker

[528] http://www.catb.org/~esr/jargon/html/C/cracker.html (zuletzt eingesehen am 03.09.04).
[529] Rentrop 2004.
[530] http://de.wikipedia.org/wiki/Cracker (zuletzt eingesehen am 03.09.04).
[531] Zum Teil werden noch als dritte Form die Script-Kiddies genannt.

wird, wird man durch das Kurzschließen eines Autos zu einem KFZ-Mechaniker. Unglücklicherweise sind viele Journalisten und Schreiber darauf verfallen, das Wort Hacker als Beschreibung für Cracker zu verwenden; dies verärgert echte Hacker ungemein.“[532]

Viele selbsternannte Hacker werden von anderen als Cracker bezeichnet. Was für den einen ein Kavaliersdelikt oder gar gerechtfertigt erscheint, mag sich für den anderen als Straftat darstellen. Selbst in der Szene ist die Sichtweise und Akzeptanz des Begriffs unklar. Amerikanische und deutsche Hacker beschimpfen sich gegenseitig als Cracker. Oft werden alle möglichen Eindringlinge in fremde Systeme unter den Begriff des Hackers subsumiert. Dabei ist es problematisch, ob hiermit auch Cracker und professionell Wirtschaftskriminelle zu fassen sind.[533]

Der Versuch einer Unterscheidung von guten und bösen Hackern scheint unmöglich zu sein. Damit aber Differenzierungen der Motivationslage nicht verloren gehen, stellt sich die Frage, ob man Hacker nach ihrer Motivation, nach ihrer computertechnischen Erfahrung, nach der Innen- oder Außensicht betrachtet. Erschwerend kommt hinzu, dass es scheinbar keine einheitliche Szene gibt und auch die Außenbewertung durch Medien, Wirtschaft und Politik differiert.

Trotzdem muss der Begriff des Hackers im Folgenden benutzt werden. Er orientiert sich in dieser Arbeit an allen Personen, die den Computer im Sinne der Definition der Computerkriminalität i.e.S. nutzen, unabhängig davon, ob die Handlungen selbst krimineller oder nichtkrimineller Art sind. Daneben werden an einigen Stellen die Begriffe echte Hacker, Cracker und Script-Kiddies ebenfalls gebraucht, da einige Autoren zwischen diesen Formen unterscheiden und auf eine solche Definition nicht verzichtet werden kann. Echte Hacker haben hiernach keine kriminellen Ambitionen. Dabei bleibt jedoch zu bedenken, dass trotzdem viele der Handlungen von echten Hackern krimineller Art sind, diese jedoch aus deren Sicht gerechtfertigt sind. Cracker werden im Folgenden als Hacker mit kriminellem Verhaltensmotiv beschrieben. Script-Kiddies wiederum betitelt eine Altersgruppe von Hackern, die zumeist nicht älter als 16 Jahre sind, oftmals weit darunter. Kennzeichnend ist hierbei zudem, dass sie über relativ wenig Fachwissen verfügen. Zudem handeln sie weder aus krimineller noch aus nichtkrimineller Gesinnung, vielmehr wird ihnen eine Unwissenheit bezüglich ihrer Handlun-

[532] http://koeln.ccc.de/prozesse/writing/artikel/hacker-howto-esr.html (zuletzt eingesehen am 12.09.04).
[533] Eckert u.a. 1991, S. 190 f.

gen nachgesagt, welche mit ihrem Alter und der damit zusammenhängenden Unreife zu tun habe.

3.8 Forschungsergebnisse zu Motivationslagen

Exakte empirische Studien und Befunde zu der Ausgestaltung und den Beweggründen der Hackerszene sind nur spärlich vorhanden. Im Folgenden wird deshalb versucht, anhand ausgewählter Literatur die Beweggründe von Hackern und ihre Szene darzustellen. Dabei liegt der Schwerpunkt der Recherche auf folgenden Fragen: Welche Motive verleiten Hacker, kriminell zu werden? Wie ist die Hackerszene strukturiert und welche Untergruppen gibt es? Dabei werden die gewonnenen Erkenntnisse typologisiert und die Beweggründe ihrer kriminellen Handlungen gezeigt und strukturiert.

3.8.1 Politisch motivierte Hacker

Politisch motivierte Hacker nutzen ihr technisches Wissen zur Durchsetzung politisch orientierter Aktionen. In den 1980er-Jahren sind politische Debatten über die Informationsgesellschaft aufgekommen, die teilweise Konsequenzen für die Hacker hatten und sie stärker politisch in Erscheinung haben treten lassen.[534]

Roland Eckert u.a.[535] sprechen bei einem Teil der Hackerszene von einer neuen sozialen Bewegung. Sie nennen diesen kleinen Teil der Bewegung Polit-Hacker. Diese stehen dabei zum Teil in Verbindung zu Bürgerinitiativen und beteiligen sich am Aufbau von Netzsystemen z.B. in der Ökologie- und Friedensbewegung. Dabei wird das politische Engagement in der Weitergabe und Vermittlung von Informationen und Computer-Knowhow gesehen. Im Sinn der Hackerethik sollen Informationen frei zugänglich sein und Informationstechnologie allen

[534] Gröndahl 2000, S. 18.

[535] Das Buch „Auf digitalen Pfaden“ ist eine überarbeitete Fassung des Gutachtens „Im Schatten der Computer-Mythen“, das vom Bundesministerium im Jahr 1990 in Auftrag gegeben wurde. Es ist eine ethnographische Untersuchung der Spezialkulturen von Hackern, Programmierern, Softwarecrackern und Computerspielern. Roland Eckert, der die Studie u.a. betreut hat, ist Professor an der Universität Trier. Ein Nachteil der Studie ist, dass sie aus dem Jahr 1990 stammt und somit die Hackerkultur nur in ihren Anfängen erfassen konnte. Interessant ist jedoch, dass gerade dadurch auch Unterschiede und Entwicklungen zu der heutigen Szene möglich sind. Wenn es früher nur eine Szene gab, so gibt es mittlerweile unzählige Hackerszenen in allen Länder verteilt. Seinen Reiz erfährt das Buch zudem durch die vielen Ausschnitte aus geführten Interviews, die u.a. auch die Motivationslagen und andere Hintergründe aufzeigen. Bemerkenswert erscheint ebenfalls an der Studie, dass sie schon wesentliche Aspekte der heutigen Hackerkultur zumindest andeutet. Ein Beispiel hierfür ist, dass die Autoren vermuten, dass Teile der Hackerkultur durch ihre Kriminalisierung in den Untergrund abtauchen oder aus der damals noch relativ homogenen Hackerszene sich verschiedene Formen heterogener Szenen gebildet haben.

zur Verfügung stehen. Der experimentierfreudige Umgang mit Technik wird als Ausdruck des Bemühens gesehen, mittels einer andersartigen Aneignung Technik zu demokratisieren. Ihre Arbeit wird von ihnen auch darin gesehen, die Möglichkeiten der Computertechnik politischen Gruppen und Bürgerinitiativen zur Verfügung zu stellen.[536]

Ein Großteil der deutschen politisch ambitionierten Hacker rekrutiert sich aus dem Umfeld des CCC. Zahlenmäßig machen sie vermutlich nur einen kleinen Teil der Hackerszene aus. Der CCC selbst zieht sich durch seine unkonventionell technikkritische Haltung immer wieder den Vorwurf zu, der Club sei ein Ort linksorientierter politischer Indoktrination. In den Anfängen suchte der CCC bei den Grünen und anderen linken Gruppierungen Verbündete.[537] So kann gesagt werden, dass der CCC im Umfeld der deutschen Alternativbewegung entstand, wobei er sich jedoch außerhalb dieser Strukturen bewegte.[538] Tatsächlich sind für den CCC und die Szene, die um ihn entstanden ist, mittlerweile sehr heterogene widersprüchliche Meinungen und Auffassungen typisch.[539] In ähnlicher Weise äußert sich Thomas Barth[540] zu diesem Thema und spricht ebenfalls vom freien Zugang aller Bürger zu den Datenbanken. Das gesamte Buch durchzieht ein roter Faden, der die Hackerproblematik anhand eines soziologischen und politischen Diskurses behandelt, wobei die Nähe des Autors zur Hackerszene spürbar ist.[541]

Kritischer sieht Boris Gröndahl[542] die politisch motivierten Hacker und differenziert nach ländertypischen politischen Neigungen und nach politischen Themen. Das Hacken selbst sieht er grundsätzlich nicht als einen politisch festgelegten Akt an, und Politik ist selten eine Motivation, die jemanden zum Hacken bringt. Diese Attitüden können je nach Gesellschaft unter-

[536] Eckert u.a. 1991, S. 172 ff.
[537] CCC/ Wieckmann 1988 S. 24ff.
[538] Gröndahl 2000 S. 64.
[539] Eckert u.a. 1991, S. 171 ff.
[540] Thomas Barth setzt sich in dem Buch, welches die überarbeitete Fassung seiner Diplomarbeit darstellt, mit der Frage nach der sozialen Kontrolle in der Informationsgesellschaft auseinander. Ein Anliegen seiner Arbeit kann in der Klarstellung einiger absurder Feststellungen über die Beschaffenheit von Hackern liegen. So lehnt er es ab, Hacker als psychisch krank, deformiert, sozial inkompetent und als vereinsamt darzustellen. Auch wenn vielen Ansichten gefolgt werden kann, so wird seine Nähe zur Hackerszene unter anderem durch dieselben Rechtfertigungsgründe für das Hacken deutlich, die auch von sogenannten „echten Hackern“ beschrieben werden. Die Arbeit stellt eher einen Versuch dar, die Hackerszene zu entkriminalisieren, er versäumt jedoch den Leser darauf hinzuweisen, dass es verschiedene Arten und Gruppierungen von Hackern gibt, von denen nicht alle mit guten Vorsätzen handeln.
[541] Barth S. 156 ff.
[542] Boris Gröhndahl beschreibt die Geschichte und Kultur der Hacker, stellt ihre Ziele und Techniken dar und untersucht die Verbindung dieser einflussreichen Computerspezialisten mit der Industrie. Das Thema wird leider recht knapp behandelt und teilweise auch nur oberflächlich angeschnitten. Zudem bleiben viele Fragen offen. Jedoch schneidet das Buch alle wesentlichen Aspekte an. Ein Pluspunkt ist zudem, dass es nicht, wie viele andere Bücher, aus der Sicht eines Hackers geschrieben wurde. Der Autor, der selbst kein Insider ist, versucht sich von Klischees fernzuhalten.

schiedliche politische Ausformungen annehmen. Dabei unterscheidet er beispielhaft zwischen der USA, den Niederlanden und Deutschland. In den USA, wo es eine antistaatliche Tradition auf Seiten der politischen Rechten gibt, die von den Republikanern bis zu christlichen Sekten mit eigenen Gesetzen und rechtsradikalen Bürgerwehren reicht, vertreten viele Hacker radikal-libertäre Positionen.[543] In den Niederlanden stehen dagegen starke Verbindungen der Hacker zu Autonomen und Hausbesetzern. In Deutschland sieht er die Szene ähnlich wie in den Niederlanden, wie sie auch von Eckert u.a. beschrieben wurde.[544] Den Schwerpunkt der politischen Interessen sieht er in den bürgerlichen Freiheitsrechten, dem Datenschutz, der bürgerlichen Privatssphäre und der freien Meinungsäußerung. Die charakteristischen politischen Gemeinsamkeiten von Hackern bezeichnet er als Vulgäranarchismus. Dies sei kein Anarchismus in seiner politischen Tradition, sondern im Sinn einer individualistischen rebellischen Attitüde, die den Autoritäten im Staat, in Konzernen oder in Universitäten misstraut, Gesetze und Regeln tendenziell missachtet und lieber handelt als darüber diskutiert.[545] Hier wird auch die politische Orientierung sichtbar, dass die Antwort auf gesellschaftliche Probleme in der Technik zu finden sei, so dass viele Hacker versuchten, durch ihre Programmierfähigkeiten die Gesellschaft einen Schritt voranzubringen.[546]

Das wichtigste politische Thema sieht er in der Gegenwehr der eigenen Kriminalisierung. Die politische Interessenvertretung ist hierbei vor allem die 2600-Hackerszene der USA[547] und der deutsche CCC.[548] Die Verbreitung von Kinderpornographie, nationalsozialistischer Propaganda und linksradikalen Webseiten im Internet erfordere neue Strafverfolgungsmaßnahmen. Neue Strafgesetze, wie das 2. Gesetz zur Bekämpfung der Wirtschaftskriminalität und sonstige Kriminalisierungsvorgänge seitens des Staates beschränkten auch die Handlungen der Hackerszene. Die Reaktionen sind häufig computertechnische Übergriffe, die dem Staat aufzeigen sollten, wie man mit hinreichender Kenntnis gesetzliche Regelungen umgehen kann.[549]

Die Mitglieder des CCC fühlen sich als nichtkriminelle Akteure und haben das Gefühl, dass sie mit einer Gruppe von vermeintlich kriminellen Hackern in Verbindung gebracht werden,

[543] Die Anfänge der politisch orientierten Hacker sieht er hierbei in der Hippie-Bewegung in den 1960er-Jahren, die massenhaft auf das Phone-Phreaking zurückgriff, das kostenlose Telefonieren mit Hilfe von selbst gebastelten Modem ermöglichte.
[544] Gröndahl 2000, S. 18ff.
[545] Gröndahl 2000, S. 18.
[546] Gröndahl 2000, S. 20.
[547] http://www.2600.com
[548] http://www.ccc.de
[549] Gröndahl 2000, S. 22.

der sie nicht angehören wollen. In diesem Zusammenhang lässt sich der Labeling approach als theoretische Begründung anfügen. Es kann davon ausgegangen werden, dass eine Vielzahl von abweichenden Handlungen im Bereich der Computerkriminalität existieren: vom Ausspähen und Sabotieren von Daten durch einzelne Hacker bis hin zum Gebrauch von Raubkopien durch eine Vielzahl der Bürger. Es treten somit unterschiedliche Formen von abweichendem Verhalten auf, aber nur ein geringer Prozentsatz ist tatsächlich einer Kriminalisierung ausgesetzt.[550] Die Sanktion durch die Strafverfolgungsbehörden erhält zudem das Kollektivgefühl der Gemeinschaft aufrecht.[551]

Desweiteren scheinen Datenschutz und bürgerliche Privatsphäre für politische Hacker von Interesse zu sein. Auch wenn Hacker versuchen, Daten auszuspähen, die ihnen vorenthalten werden, engagieren sie sich ausgerechnet dafür, Daten vor unbefugtem Zugriff zu schützen.[552] Dieser Widerspruch wird verständlich durch die Ausführungen des CCC: „Öffentliche Daten nützen, private Daten schützen!“ Politische Hacker sehen in der Geheimhaltung von staatlichen Informationen eine Vorenthaltung ihrer bürgerlichen Rechte, dagegen ist ihnen die eigene Privatsphäre sehr wichtig und wird mit allen Mitteln der Kunst verteidigt.[553] Boris Gröndahl sieht bei politisch orientierten Hackern die Hauptattitüde in einer antistaatlichen Grundhaltung.[554] Dies wird gestärkt durch die Cologne des CCC:

„Hacker sind von Natur aus antiautoritär veranlagt. Jeder, der dir Befehle geben kann, kann dich auch davon abhalten, das Problem zu lösen, das dich gerade fasziniert… Autoritäre Einstellungen müssen bekämpft werden, wo immer sie gefunden werden, damit sie nicht dich und andere Hacker ersticken. Autorität gedeiht auf dem Boden der Zensur und Geheimhaltung, sie misstraut freiwilliger Zusammenarbeit und freiheitlicher Aufteilung der Informationen – die einzige Zusammenarbeit, die sie gerne sehen, ist diese, die unter ihrer Kontrolle steht. Wenn du also wie ein Hacker handeln willst, musst du eine instinktive Feindschaft gegenüber Zensur, Geheimhaltung und dem Einsatz von Gewalt oder Betrug entwickeln, und du musst bereit sein, nach diesem Glauben zu handeln.“[555] Auch wenn diese Einstellungen lobenswert sind, so bleibt paradoxerweise hierbei oft von dieser Gruppierung unbeachtet, dass das Internet nur durch die militärische Forschung und die staatliche Förderung entstehen konnte.

[550] Keupp 1976, S. 79 ff.
[551] Popitz 1968, S.3.
[552] Himanen 2001, S. 126 ff.
[553] Gröndahl 2000, S. 20.
[554] Gröndahl 2000 S. 36 ff.
[555] http://koeln.ccc.de/prozesse/writing/artikel/hacker-howto-esr.html (zuletzt eingesehen am 17.09.2004).

Ryan Russel und Stace Cunningham[556] orientieren sich an der in der Szene gebräuchlichen Bezeichnung für das Hacking aus politischen Gründen: hacktivism.[557] Der Begriff scheint eine Verknüpfung aus Hacking und Aktivismus zu sein. Im Sinne dieses Aktivismus sollen Hackerfähigkeiten dafür eingesetzt werden, um politische Ziele zu fördern, auch wenn dabei gegen geltende Gesetze verstoßen wird. Dabei soll das politische Ziel die Mittel rechtfertigen.[558] Es geht hierbei also auch um destruktive Ziele. Russel/Cunningham nennen als Beispiel hierfür die am 10. April 2000 erfolgte Veränderung der Webseite des Ku-Klux-Klans[559] oder DDoS-Angriffe auf Unternehmen. Russel/Cunningham vergleichen diese Form des Hackens mit dem zivilen Ungehorsam oder Sitzblockaden oder Graffiti auf Werbetafeln.[560] Dabei erscheint der Vergleich mit Sitzblockaden und zivilem Ungehorsam nicht entsprechend, da beide Formen kein aktives Handeln beinhalten, das Hacking aber immer aktiv gestaltet werden muss, damit es zur Anwendung kommt. Mit diesen Vergleichen scheint sich schon eine Art Neutralisation der eigenen Handlungen anzudeuten.

Neben den genannten Hackern beschreibt Christian Zimmermann[561] unter der Überschrift „Die ganz legalen Hacker" eine gänzlich andere „Szene" der Hacker. Gemeint sind damit Hacker, die im Auftrag staatlicher Behörden Hackertechniken anwenden. Bei diesen Hackern kann es sich um Mitarbeiter von Strafverfolgungsbehörden oder Geheimdiensten handeln, wobei nicht ausgeschlossen werden kann, dass auch private Hacker von diesen Behörden be-

[556] Die Idee des Buches ist es, die Computerprofis aus der Welt der Hacker zu Wort kommen zu lassen und von ihnen zu lernen, wie sie vorgehen. In fünf Themenkapiteln werden zuerst die Theorien und Ideale der Computer-Hacker beschrieben. Dabei geht es um Vision und Wirklichkeit dieser Szene. Auch wenn das Buch sich zum großen Teil mit technischen Aspekten beschäftigt, sind doch insbesondere die einzelnen Beiträge verschiedener Szenen-Insider sehr interessant, um Motivationen herauszufinden. Zudem zeigt das Buch, wie schwer es ist, den Begriff des Hackers zu definieren. Unter der Überschrift „Hacker-Definitionen" erläutert er nur, dass es unzählige davon gibt, und geht dann über in die Entstehungsgeschichte der Hacker. Danach begnügt er sich mit einer Aufzählung möglicher Szenen, ohne weiter den Begriff des Hackers zu klären Dies zeigt wohl auch die Schwierigkeit, in der sich jeder befindet, der diesen Begriff klar definieren möchte.

[557] Denning 1999.

[558] Russel/Cunningham 2001, S. 35ff.

[559] Zu finden unter www.kkklan.com

[560] Russel/Cunningham 2001 S. 36.

[561] Christian Zimmermann, früher selber einmal ein Hacker und nun auf die Seite der Spezialisten für Datensicherheit übergewechselt, gibt dem Leser anhand konkreter Beispiele einen ersten Einblick in Denk- und Vorgehensweise von Hackern. Dabei zeigt er die mit bestimmten Systemen verbundenen Gefahren auf und räumt mit oftmals falschen Sicherheitsgefühlen bei den Benutzern auf. Er behandelt jedes der zahlreichen Themen knapp und verständlich und gibt an entsprechenden Stellen auch einige Empfehlungen, was man zum eigenen Schutz tun kann. Zudem erscheint es interessant, eine Beschreibung der Szene von jemand zu erhalten, der in der Vergangenheit zu der Szene gehörte, jetzt aber über sie als Außenstehender berichtet. Dies gibt evtl. die Möglichkeit, unbefangener über Motive und Handlungsweisen zu berichten. Unerfreulich ist, dass der Autor trotz seines früheren Hackerseins sich einiger Sensationsreportagen bedient, wie „Keiner ist mehr sicher" oder „Hacker sind überall", was eher störend wirkt, da man nicht genau weiß, was er damit bezweckt. Ein weiteres Manko ist, dass das Buch zwar 1996 herausgekommen ist und man somit auch eine Beschreibung der Szene in dieser Zeit erhofft. Es erscheint jedoch so, als ob der Autor die Hackerszene Anfang der 1990er-Jahre beschreibt, da er ausführlich Hackertechniken beschreibt, die in diesen Jahren benutzt wurden und heute schon zum Teil veraltet sind.

auftragt werden.[562] Dabei spricht er Spionageaktivitäten der NSA, des BND, des Verfassungsschutzes und der Polizei an. In erster Linie geht es diesen Behörden um die Sicherung der staatlichen Organisationen, so dass sich die Spionagetätigkeit weniger gegen einzelne Bürger richtet, sondern vielmehr gegen andere Staaten und deren Behörden.[563] Dabei beschränkt sich Zimmermann nicht auf rein typische Hackertechniken, die mit dem Computer und Computernetzen zu tun haben, sondern bezieht auch darüber hinausgehende Techniken in den Begriff des Hackens mit ein. So werden auch das Abhören von Telefonaten, Satellitenüberwachungsmaßnahmen und die Funküberwachung mit einbezogen. Auch wenn diese Formen der Spionage meines Erachtens nur entfernt als Hackeraktivitäten bezeichnet werden können, zeigt dies doch, wie unterschiedlich der Begriff des Hackens verwendet werden kann. Nichtsdestotrotz setzen die genannten staatlichen Einrichtungen auch Computerexperten ein, so dass zumindest diese Personen auch als Hacker qualifiziert werden müssen.[564]

Howard S. Becker spricht in diesem Zusammenhang vom abweichenden Verhalten, das durch die Gesellschaft geschaffen wird: „ Ich meine vielmehr, dass gesellschaftliche Gruppen abweichendes Verhalten dadurch schaffen, dass sie Regeln aufstellen, deren Verletzung abweichendes Verhalten konstituiert, und dass sie diese Regeln auf bestimmte Menschen anwenden, die sie zu Außenseitern abstempeln.“[565] Es wird also unterschieden, welche Akteure und Institutionen Systeme ausspähen. Ob eine Handlung abweichend ist, hängt folglich davon ab, wie andere Personen ihr begegnen.[566] Hier zeigt sich, dass die Definitionsmacht bei den staatlichen Organen liegt, die insoweit bestimmen, welche Art des Hackens einen Straftatbestand erfüllt.

Aus Sicht der westlichen Regierungen fallen unter die illegalen Hacker auch diejenigen, die als Cyberterroristen bezeichnet werden. Da diese Personen meist nicht im Auftrag einer bestimmten Regierung handeln, sind ihre Handlungen zumeist auf zerstörerische Akte gerichtet, vergleichbar den realen Terroristen. Debra Littlejohn Shinder stellt Cyberterroristen auf dieselbe Stufe wie die Hezbollah, die Hamas oder die al Qa’ida:

[562] Zimmermann 1996, S. 181ff.
[563] Zimmermann 1996, S. 184ff.
[564] Wie gefährlich eine Digitalisierung aller Systeme ist und wie verunsichert die Bevölkerung ist, zeigt auch der im Jahr 2004 stattgefundene Wahlkampf zwischen George W. Bush und John Kerry. Täglich kamen neue Spekulationen über die neue digitale Form des Wählens auf. Viele trauten der Bush-Administration zu, die Wahl durch computertechnische Beeinflussung zu manipulieren. Dies zeigt, wie wichtig eine Aufklärung ist, wie notwendig sichere Standards sind und wie unsinnig, aus meiner Sicht, es erscheint, alle Lebensbereiche zu digitalisieren.
[565] Becker 1975, S. 18.
[566] Becker 1975, S. 19 ff.

„Cyberterrorism refers to using the Internet and Computer skills to disrupt or shut down the critical infrastructure and government services of a country. Although no such large-scale attacks have thus far been implemented at this writing, security experts warn that such attacks are or will be within the capabilities of some terrorist organizations and could pose a huge threat to government and business operations."

Es kann festgehalten werden, dass Hacker aufgrund von unterschiedlichen politischen Motiven voneinander abweichende Ambitionen verfolgen, die von relativ harmlosen Veränderungen von Webseiten bis hin zu Angriffen auf staatliche Infrastrukturen reichen können.

3.8.2 Aufklärerische und kritisch-kreative Computernutzung

Die Aufklärung und die kritisch-kreative Computernutzung sind der Bereich, der von der Hackergemeinde in den Vordergrund gerückt wird und die sich selber als die „wahren Hacker" sieht. Es ist auch der Bereich, der von Autoren bevorzugt beschrieben wird, wenn es um die Hackerszene geht. Diese Gruppe stellt das normative Ideal des Jargon File dar. Ihrem Selbstverständnis nach handelt es sich hierbei um Programmierer mit sehr guten Fachkenntnissen, die dem Ideal der Informationsfreiheit verpflichtet sind und staatliche Autoritäten und Großkonzerne wie die IBM oder Microsoft ablehnen.[567] Im Folgenden sollen wesentliche Aspekte und Unterschiede der Untergruppen aufgezeigt werden.

Hacker, die die computertechnische Aufklärung in den Vordergrund stellen, müssen hier als erste Gruppe genannt werden, da sie den Schwerpunkt ihrer Tätigkeit im reinen Programmieren und Aufdecken von Sicherheitslücken sehen.
Boris Gröndahl und Anonymous[568] sehen als wesentlichsten Aspekt des Hackens das Programmieren selbst. Hacker verfügen über ein sehr gutes Wissen über Betriebssysteme und

[567] Medosch/Röttgers, 2001, S. 149.
[568] Als ehemaliger Hacker und Cracker hat sich der Autor des Hacker's Guide hinter dem Autorennamen „Anonymous" verschanzt, um aus dieser Position heraus die geheimen Techniken der Hacker zu offenbaren. Nachdem er eine längere Haftstrafe verbüßt hatte, hat er sich auf die Seite der „Good Guys" geschlagen und berät heute als Sicherheitsberater Unternehmen und ist Buchautor. Seiner Ansicht nach ist der wirkungsvollste Schutz für den Computer oder das Netzwerk das Wissen um die Denkweise der Angreifer. Erst wenn man das System aus der Perspektive der „Bad Guys" analysieren kann, ist man in der Lage, es effektiv zu verteidigen. Der Autor schreibt aus der Sicht der Angreifer und Angegriffenen über die Szene und deren Vorgehensweisen und Motive. Am Beispiel des Werdegangs des Autors zeigt sich auch, in welcher prekären Lage die Wirtschaft, Politik und der Rest der Gesellschaft eigentlich stecken. In einer Zeit, in der zunehmend alle Lebensbereiche digitalisiert werden, muss auf Personen zurückgegriffen werden, die früher die Systeme bedroht haben. Es zeigt sich hierin, dass die Hacker am Fortschritt der Computertechnik wohl maßgebend und führend sind, was sich darin äußert, dass sie auch die Systeme beherrschen und manipulieren können. Ohne diese Hacker gebe es jedoch diesen Fort-

Programmiersprachen und sind an allen Arbeitsabläufen eines Computers interessiert.[569] Dabei sind beim Programmieren vor allem Stilfragen von Bedeutung. Welchen Computer benutzt man, mit welcher Programmiersprache soll programmiert werden oder auf welchem Betriebssystem soll das Programm in Zukunft laufen. Für die ursprünglichen Hacker bedeutete Hacken, ein Programm so gut es geht zu programmieren, d.h. also ein Problem mit möglichst wenigen Instruktionen zu lösen.[570] In den Ursprüngen stand Software jedem frei zur Verfügung und jeder konnte diese auch nach seinen Bedürfnissen umprogrammieren. Aus dieser Idee entstand die Open-Source-Gemeinde.[571] Dabei schauen sich die Hacker auch kommerzielle Software an und entdecken hin und wieder Sicherheitslücken.[572] Wie mit diesen Sicherheitslücken umgegangen werden soll, ist wiederum in der Szene umstritten.

Russel/Cunningham 2001 thematisieren hierbei die sog. Grey-Hat-Hacker.[573] Die Begrifflichkeit entstand auf einer Black-Hat-Konferenz.[574] Die Black-Hat-Konferenzen sind jährliche Treffen von Computerexperten, die in Las Vegas zum Thema Computersicherheit abgehalten werden. Dabei unterscheiden die Computerexperten zwischen Black-Hat-Hackern und White-Hat-Hackern.[575] Black-Hat-Hacker sind Hacker, die ihr Wissen rein kriminell ausnutzen, und White-Hat-Hacker sind Hacker, die ihr Können dergestalt einsetzen, dass jeglicher Schaden vermieden wird. Problematisch ist hierbei, was gut und böse bedeuten, denn die Vorstellungen über richtig und falsch gehen weit auseinander, vor allem davon abhängig, von welcher Seite aus die Betrachtung erfolgt. Verbraucher sehen Aufdeckungen von Sicherheitslöchern in Softwareprodukten hierbei sicherlich anders als das Unternehmen, das diese Produkte verkauft. In diesem Zusammenhang entstand der Begriff des Grey-Hat-Hackers. Grey-Hat-Hacker sind der Meinung, dass die Veröffentlichung von Sicherheitslücken und von ausreichenden Informationen, um diese Sicherheitslücke ausnutzen zu können, der richtige Weg ist. Einige Grey-Hat-Hacker halten es für unvertretbar, eine Sicherheitslücke zu publizieren, ohne dem Hersteller die Gelegenheit zu geben, das Problem zu beheben. Andere vertreten den Standpunkt, die Hersteller nicht zu informieren, da sie dadurch gezwungen werden, vorsichtiger zu arbeiten und sich aktiv um die Qualitätssicherung des Programmcodes zu kümmern.

---

schritt in dieser Form nicht. Somit entsteht ein Paradoxon: Diejenigen, die am Fortschritt am meisten beteiligt sind (oder gar bestimmend), können der Technik gleichzeitig gefährlich werden.

[569] Anonymus 2003, S. 79.

[570] Gröndahl 2000, S. 24.

[571] Gröndahl 2000, S. 25.

[572] Anonymus 2003, S. 79.

[573] Russel/Cunningham 2001, S. 32 ff.

[574] Wobei die Begrifflichkeit eine Anspielung auf alte Westernfilme sein soll, in denen die „Bösen“ immer schwarze Hüte aufhatten.

[575] Russel/Cunningham 2001, S. 33.

Als Beispiel hierfür kann der Fall des als White Hacker bezeichneten Adrian Lamo genannt werden. Adrian Lamo ist zum Beispiel in die Netzwerke von Excite@Home, Yahoo, Microsoft, MCI-WorldCom oder SBC Ameritech eingedrungen, weil diese mangelhaft gesichert waren. Er hat danach immer die Unternehmen über die Sicherheitslücken und Wege ihrer Beseitigung informiert. Darüber hinaus informierte er regelmäßig die Presse über seine Hacks, nachdem das Unternehmen die Sicherheitslücke geschlossen hatte. Adrian Lamo wurde deswegen im Juli 2004 zu zwei Jahren auf Bewährung und zu einer Geldstrafe von 65.000 US$ verurteilt.[576]

In ähnlicher Art und Weise erläutert Roland Girtler[577] die klassischen Hacker und nennt sie in diesem Zusammenhang Rebellen. Seines Erachtens stehen die Freude am Programmieren und die kreative Nutzung der Technik im Mittelpunkt dieser speziellen Gruppierung von Hackern. Er bezeichnet sie als virtuelle „Robin Hoods", die sich selbst als edle Leute ansehen, obwohl ihnen klar ist, dass sie gegen Gesetze verstoßen.[578] Man könnte hier von befreienden Heldentaten sprechen, die für den berechtigten Ungehorsam notwendig erscheinen.

Einen philosophisch erweiterten Sinngehalt sieht eine andere Gruppierung. Zu ihnen können die Mitglieder und Anhänger des CCC, die Hackerszene rund um die Zeitschrift 2600 und die niederländischen Hacker gezählt werden.[579] Sie sind der Prototyp der aufklärerischen und kritisch-kreativen Hacker und im Sinn des Jargon File „wahre" Hacker.[580] In erster Linie lö-

[576] http://rabenhorst.blogg.de/index.php?cat=IT-Sicherheit (zuletzt eingesehen am 20.09.04).
[577] Roland Girtler arbeitet als Professor am Institut für Soziologie an der Universität in Wien. In der Einleitung seiner Publikation schreibt der Autor klarstellend, dass er diesen Aufsatz nicht als Computerspezialist, sondern eher als Laie schreibt. Roland Girtler beschäftigte sich aber in den letzten Jahren mit verschiedenen Randkulturen, so dass sein Augenmerk irgendwann auch auf die Hacker fallen musste. Trotz des fehlenden technischen Verständnisses ist der Ansatz bemerkenswert und erinnert an die Ausführungen über Hacker aus dem „Chaos Computer Buch". Er arbeitet deshalb auch mit einer nicht computertechnischen Definition des Begriffs Hacker. Er vergleicht diese mit „Freibeutern oder Rebellen auf dem offenen Meer, die mit allerlei Kniffen versuchen, neue Häfen zu erobern", wobei die Häfen fremde Computersysteme symbolisieren sollen. Interessant ist in seinen Ausführungen, dass er die Hackerethik mit einer Art „Gaunerehre" vergleicht. Das heißt, dass ein Dieb nur Reiche bestiehlt und es den Armen gibt und diese nicht beraubt. Dieser Vergleich zeigt aber, dass die Hacker, selbst wenn sie sich an die Hackerethik halten, nicht sofort zu rechtschaffenden Bürgern werden. Der Versuch, den Reichen, dem Staat und sonstigen Mächtigen zu nehmen und es allen zu geben, erinnert an revolutionäre und anarchistische Gedanken.
[578] Girtler 2003, S. 217.
[579] Medosch/Röttgers 2001, S. 149 f.
[580] Wobei hier gerade die Anhänger der 2600 Gemeinde sich nicht unbedingt mit allen Gesinnungen des CCC anfreunden können. Trotzdem möchte ich diese drei Gruppierungen in diesem Themenbereich wegen ihrer grundlegend ähnlichen Einstellungen zusammenfassen. Grundsätzlich erweist es sich als sehr schwer, Hackergruppen einzuteilen, da sie der technischen Kultur entsprechend nicht einheitlich nach außen auftreten und zudem viele Hacker in mehreren Gruppierungen vertreten sind.

sen Hacker Probleme und bauen Dinge auf. Gefordert sind hierfür Motivation und Kreativität, gegenseitige Hilfe und die Vermeidung von Anstrengungen:[581]
„Um wie ein Hacker zu handeln, musst du glauben, dass die Zeit, die einem Hacker zum Denken zur Verfügung steht, kostbar ist – so kostbar, dass es beinahe eine moralische Pflicht ist, deine Informationen zu teilen, Probleme zu lösen und die Lösung weiterzugeben, damit andere Hacker sich neuen Problemen zuwenden können, anstatt andauernd bereits gelöste wieder aufrollen zu müssen."[582]

Der 1983 als Hackervereinigung gegründete CCC war eine der ersten Organisationen, die sich auf der Ebene der Nutzer mit der Datenfernübertragung in der Bundesrepublik auseinandersetzte. Dieser Club trug wesentlich zur Popularisierung des Themas in der Öffentlichkeit bei. Der CCC versteht sich als Kontrollinstrument in der Datenwelt und engagiert sich in den Bereichen Datenschutz und -sicherheit und hat schon sehr früh die Diskussionen zu diesen Themen angestrengt. Im Sinn der Philosophie des uneingeschränkten und freien Informationsflusses ist die Demokratisierung der Netze ein besonderes Anliegen des CCC.[583] Der zum Teil philosophische Ansatz dieser Gruppe spiegelt sich unter anderem in Teilen der sog. Hackerethik wider.[584] Im Sinn der delinquenten Subkultur scheint es, als ob die Hackerszene ein gewisses Anti-Normensystem, zumindest im Bereich des freien Zugangs zu Computern und Daten, entwickelt hat.[585]

Thomas Barth beschreibt in diesem Zusammenhang den CCC als eine Vereinigung, die den Anspruch hat, Systeme zu verbessern, d.h. sicherer, informativer und funktionsfähiger zu gestalten. Dabei ist von Bedeutung, dass Störungen des Informationsflusses wie etwa Zugangsbeschränkungen zu bestimmten Datenbanken beseitigt werden, damit diese Informationen genutzt werden können, um das System zu verbessern.[586] Man erkennt deutlich den positiven Gedankenansatz und den „Willen zu Weltverbesserung" durch die Technik. Der immer wieder genannte freie Informationsfluss passt wiederum nicht mit marktwirtschaftlichen und politischen Grenzen zusammen, in denen Informationen zwangsläufig nicht immer für alle frei zugänglich sein werden.

[581] http://koeln.ccc.de/prozesse/writing/artikel/hacker-howto-esr.html (zuletzt eingesehen am 19.09.2004).
[582] Ebd.
[583] Wetzstein u.a. 1995, S. 127ff.
[584] http://www.ccc.de/hackerethics?language=de (zuletzt eingesehen am 17.09.2004).
[585] Schwind 1997, S. 132.
[586] Barth 1997 S. 167 f.

Paul A. Taylor[587] beschreibt die Motivation von Hackern folgendermaßen:
„Information freedom is the slogan of most hackers over here (including the notorious CCC, Chaos Computer Club). We already have a situation where electronic communications are unsafe, i.e. governments may legally tap data lines and make copies of electronic mail. Plus, the suspicion of 'hacking' alone (i.e. no evidence) is sufficient to get search warrants or to impound equipment. What hackers (not the kind that wilfully destroys data for the fun of it, but the real hackers) are fighting for, is something of a battle of principles. They want to keep the new electronic media as safe or even safer than regular paper mail from intrusion by government agencies."[588]

Durch den Bezug auf die Regierung und deren Handlungen in Bezug auf Daten wird deutlich, dass diese Gruppe stark verwandt ist mit den politisch orientierten Hackern.
Die Forderung nach uneingeschränktem und freiem Informationsfluss ist unter den Hackern selbst umstritten, gerade wenn es sich um geheime Daten und Informationen handelt. Einerseits werben sie zwar für den freien Fluss von Informationen und den ungehinderten Zugang zu allen Daten. Andererseits erkennen sie aber auch, dass es bei der freien Veröffentlichung von Sicherheitslücken nicht nur um die „Freiheit der Informationen" geht, sondern dass auch andere wie Spione und Wirtschaftskriminelle hieraus Vorteile ziehen können.[589]

Pekka Himanen[590] beschreibt Hacker ebenfalls als Personen, die das Individuum stets schätzen und die ihrer Grundhaltung nach antiautoritär gesinnt sind.[591] Geld und andere kapitalisti-

[587] Das Buch von Paul A. Taylor orientiert sich an einer Forschungsarbeit des „Research Centre for Social Sciences" an der Universität von Edinburgh. Der Autor vergleicht das Computerzeitalter in seinen Auswirkungen mit der industriellen Revolution und versucht, soziale, kulturelle und historische Veränderungen aufzuzeigen. Gerade die große Anzahl an geführten Interviews mit Hackern, Computerwissenschaftlern und Sicherheitsexperten geben die Spannbreite des Themas wieder.
[588] Taylor 2001, S. 61.
[589] Eckert u.a. 1991, S. 158.
[590] Trotz des Titels ist „Die Hacker-Ethik" vor allem ein philosophisches Buch, das die westliche materialistische Weltsicht dem Weltverständnis von Hackern gegenüberstellt. Das von dem finnischen Medienwissenschaftler geschriebene Werk bietet weder eine Anleitung zum Hacken noch Spezialwisssen für Computerexperten. Die Hacker-Ethik setzt sich mit Werten und Chancen des beginnenden 21. Jahrhunderts auseinander, die sich nach der Einschätzung des Autors nicht von PC und Internet trennen lassen. Vor allem ist der Autor der Meinung, dass Unternehmen mit dem Wissen Geld verdienen, das Wissenschaftler frei zur Verfügung stellen. Das führt zu einem philosophischen Dilemma. Unternehmen sind begierig darauf, der Informationen habhaft zu werden, die Hacker frei zur Verfügung stellen, und halten im gleichen Atemzug die Informationen zurück, die sie selbst gewinnen. Himanen untermauert seine Argumentation mit Ideen von Platon bis hin zum mittelalterlichen Dorfleben, dem Protestantismus, akademischer Weltanschauung, der industriellen Revolution und vielen anderen historischen Faktoren. Er schlussfolgert, dass die Informationsrevolution die Arbeit zur zentralen Instanz unseres Lebens gemacht hat und damit alle Energie verzehrt, die normalerweise für das Vergnügen und für das Verfolgen der eigenen Leidenschaften zur Verfügung stand. Der Autor geht dabei stets von einem Hackerbegriff aus, der den „echten Hacker" meint.
[591] Himanen 2001, S. 61f.

sche Motive seien ihnen grundsätzlich fremd.[592] Der Schwerpunkt seiner Darstellung bezieht sich jedoch im Bereich der aufklärerischen Hacker stark auf die Hacker-Ethik und die Netiquette.[593] Diese zeigen allgemeine Regeln auf wie Nutzer mit ihrem Computer, dem Internet und E-Mail umgehen sollen, sowie sonstige Verhaltensregeln für die Kommunikation im Netz.[594] Die Hacker-Ethik und die Netiquette spiegeln seiner Ansicht nach die Einstellungen von Hackern wider. Dabei definiert er Aktivität und soziale Verantwortung als die Hauptwerte dieser Hackergesinnung. Aktivität umfasst in diesem Zusammenhang das Recht auf freie Meinungsäußerung, den Schutz der Privatsphäre im Hinblick auf einen individuellen Lebensstil und die Ablehnung einer passiven, rezeptiven Haltung zugunsten von Eigenaktivität bei der Verwirklichung der Leidenschaften. Diese drei Elemente ermöglichen es einem Menschen, selbstständig und kreativ zu denken, einen persönlichen Lebensstil zu entwickeln, ohne überwacht zu werden, und nach eigenen Vorstellungen und Interessen zu leben.[595] Hierbei staunt der Leser über das Ziel der Hacker, die Privatsphäre zu schützen, da gerade in der öffentlichen Diskussion dargestellt wird, dass diese von den Hackern bedroht sei, indem Hacker in fremde Rechner eindringen und Informationen ausspähen. In erster Linie ist hierbei der Schutz der Privatsphäre vor Übergriffen seitens des Staates oder der Wirtschaft gemeint. Sich selber haben Hacker in diesem Zusammenhang nicht im Blick. Ihnen ist die Überwachung durch Unternehmen mittels kleiner Trojaner oder durch Geheimdienste zuwider.[596] Um die Privatsphäre zu schützen, ist die Verbindung zum Programmieren notwendig. Technische Lösungen wie Verschlüsselungen oder Methoden, um die Identität zu anonymisieren und den Schutz der Privatsphäre zu ermöglichen, stehen dabei im Vordergrund. Seiner Ansicht nach wird die Privatsphäre in Zukunft nicht nur eine ethische, sondern auch eine technische Frage sein.[597]

Soziale Verantwortung bedeutet wiederum die Sorge um andere als Selbstzweck und den Wunsch, die Netzwerk-Gesellschaft von einer reinen Nehmermentalität zu befreien. Jeder soll zur Mitarbeit im Netzwerk motiviert werden und davon profitieren können. Außerdem sollen sich alle für die langfristigen Konsequenzen der Netzwerk-Gesellschaft verantwortlich fühlen und anderen helfen.[598]

---

[592] Himanen 2001, S. 69ff.
[593] Entstand aus den Begriffen Netz und Etiquette.
[594] http://www.ping.at/guides/netmayer/netmayer.html#classic (zuletzt eingesehen am 16.09.04).
[595] Himanen 2001, S. 130.
[596] Himanen 2001, S. 122 ff..
[597] Himanen 2001, S. 128 ff.
[598] Himanen 2001, S. 159 f.

Eckert u.a. verdeutlichen die kritisch-kreative Computernutzung, indem sie die Meinungen von vier Hackern im Alter zwischen 19 und 24 Jahren wiedergeben:[599]

Jürgen, 19 Jahre, Hacker

„Es gibt verschiedene Definitionen zum Hacken. Hacken ist zum einen mal ganz sicher erlebnisorientiertes Lernen, also sich seinen Horizont anhand dessen bilden, was man an Erfahrungen macht. Zum anderen ist Hacken schöpferisch kritischer Umgang mit Technologie, d.h. halt eine gewisse Form des respektlosen Umgangs mit Technik, halt ganz klar in den Vordergrund stellen, dass der Mensch die Maschine zu beherrschen hat und nicht umgekehrt (...). Die Leute versuchen halt glaubhaft zu machen, dass man Sicherheit durch die bestehenden Gesetze erreichen kann. Und wir versuchen halt seit eh und je eine offene Form des Dialogs zu betreiben, offen über die Probleme zu reden, die es im Zusammenhang mit Computern gibt und durch das Hacken werden dann natürlich manche Sachen schon klar."

Hermann, 22 Jahre, Hacker

„Hacken ist auch eine Möglichkeit, kritisch mit dem Medium umzugehen, Missstände aufdecken zu können und so das öffentliche Bewusstsein für die Gefahren der immer größer werdenden Vernetzung der Gesellschaften zu fördern."

Hans, 21 Jahre, Hacker

„Ich bin halt für die Freiheit der Information. Viele Informationen, die wichtig sind, befinden sich hinter verschlossenen Türen, in großen Computern, von denen keiner etwas weiß (...). Ich denke da an das AIDS-Virus. Überall in der Welt arbeiten Wissenschaftler daran. Wenn alle Informationen zusammen kämen, hätte man vielleicht schon etwas dagegen gefunden. Aber niemand will Informationen an einen anderen weitergeben (...). Es gibt noch einen Grund. Die Leute, die die Systeme installieren, werden angehalten, ihre Systeme besser zu schützen. Wenn jemand reinkommt, müssen sie etwas ändern (...). Ich bin zwar für den freien Fluss der Informationen, aber es sollte z.B. keine Informationen über Waffen geben. Ich glaube nicht, dass das wichtig ist für die Existenz der Erde. Informationen sollten soweit publik gemacht werden, wie man es auch verantworten kann."

[599] Eckert u.a. 1991, S. 171.

Heiner, 24 Jahre, Hacker

„Also ich will damit auch sagen, dass ich mich als jemand fühle, der an der Gestaltung der Zukunft mitarbeitet. Ich meine, ich bin jetzt 24 Jahre und studiere seit zwei Semestern Datenkommunikation. (...) Was ich damit sagen will, ich will an den Sachen da mitgestalten. Demokratie und so was, das gibt es ja nicht einfach so, da muss man schon was dafür tun. Na ja, vielleicht ist das bei uns in Holland ja auch anders. (...) Also ich engagiere mich z.B. auch in einer Vereinigung, die sich um die Aufklärung von Fällen des Datenmissbrauchs kümmert."

Aufklärerische Hacker setzen sich im Allgemeinen zum Ziel, die Gesellschaft des Informationszeitalters über die Hackerszene, die richtige Computernutzung, damit zusammenhängende Probleme und deren Hintergründe aufzuklären und Hilfestellungen zu geben. Dabei steht überwiegend die Aufdeckung von Sicherheitsmängeln im Vordergrund. Diese Gruppe dringt notwendigerweise in fremde Systeme ein, es liegt ihnen allerdings grundsätzlich fern, Schaden anzurichten. Es zeigt sich auch, dass die Übergänge von reinen Programmierern bis zu philosophischen Hackern fließend ausgestaltet sind. Dabei können bei Hackern, die neben rein programmtechnischen Ambitionen auch noch philosophische Gründe des Hackens vermitteln wollen, diese als allgemeine soziale Herausforderung sehen.

3.8.3 Macht und Kontrolle

Die Soziologin Sherry Turkle war die erste Autorin, die sich mit dem Phänomen der Hackerszenen beschäftigte. Dabei stellt sie die perfekte Beherrschung des Computers als leitendes Motiv heraus. Ihrer Ansicht nach spielt die Beherrschung von Dingen und Fertigkeiten in der Entwicklung eines jeden Individuums eine entscheidende Rolle. Die Fähigkeit, etwas „im Griff zu haben", stelle etwas Positives dar und sei so der wichtigste Bezugspunkt der Selbstdefinition.[600] Der Computer leiste hierbei einen Beitrag zur persönlichen Entwicklung. Die Bewältigung technischer Probleme und neue Ideen könnten als Herausforderung angesehen und empfunden werden.[601] Eine besondere Motivation bildeten geschlossene Systeme. Als Beispiel nennt sie hierbei den Mount Everest, der dazu da sei, um bestiegen zu werden. Genauso seien die verborgenen Geheimnisse von geschlossenen Systemen dazu da, um aufgedeckt zu werden. Hierbei müssten zum Teil mehrere computertechnische Ebenen durchbrochen werden, die die Herausforderungen verstärken.[602]

[600] Turkle 1984, S. 255f.
[601] Turkle 1984, S. 257f.
[602] Turkle 1984, S. 287.

Eckert u.a. betrachten unter anderem die Herausforderung und den intellektuellen Wettkampf als wesentliche Motive für Hacker.[603] Computersysteme sind durch eine Anzahl von technischen Vorrichtungen gegen das unberechtigte Eindringen geschützt. Die wichtigsten Vorrichtungen sind hierbei Passwörter. Ohne die Kenntnis des Passworts ist keine Dialogaufnahme mit einem geschützten Computersystem möglich. Neben rein technischen Möglichkeiten muss in diesem Zusammenhang auch das sog. Social Engineering[604] genannt werden. Allgemein gesprochen bezeichnet Social Engineering oder auch Social Hacking eine Vorgehensweise zum nichttechnischen Ausspähen von Daten durch Kontakt zu den Informationsträgern. Dabei versuchen Hacker sicherheitsrelevante Informationen von einer unvorsichtigen Person zu erfahren, um so organisationsinterne Sicherheitsvorkehrungen zu umgehen. So werden die technischen Sicherheitsvorkehrungen nicht auf der technischen, sondern auf der sozialen Ebene umgangen.[605] Im Bereich der Passwörter erkunden Hacker dabei das Umfeld von Computerbetreibern und anderen Zugangsberechtigten. Sie versuchen die Eingabe von Daten wie Namen der Kinder, Namen der Ehefrau, Geburtsdatum oder sonstige Informationen über die Person, da in vielen Fällen bereits diese Kenntnis dieser Daten die Türen eines fremden Computers öffnet.[606]

Neben Passwortausspähungen ist es für den Hacker eine weitere Herausforderung, das System zu übernehmen: zum einen, um sich spätere Zugänge mit Hilfe von Trojanern offen zu halten und zum anderen, um möglichst tief in das jeweilige System einzudringen. Dabei müssen verschiedene Hürden überwunden werden, angefangen von Zugriffen auf einzelne Nutzer-Rechner bis hin zur gesamten Kontrolle des Computersystems des Unternehmens. „Der größte Erfolg eines Hackers ist die totale Beherrschung des Systems, d.h. er ist in der Lage, den Systemoperatoren (die normalerweise höchste Zugriffspriorität haben) den Zugang zu ihren eigenen Rechnern zu verwehren.“[607]

In einem Interview spricht Kevin Mitnick Aspekte des Wettkampfs an. Kevin Mitnick ist einer der berühmtesten Hacker. Zum ersten Mal machte er 1985 Schlagzeilen, als er in die Computer des amerikanischen Verteidigungsministeriums eingedrungen war. Daneben hat er

[603] Eckert u.a. 1991, S. 166ff.
[604] Social Engineering ist ein wahrscheinlich auf die frühen 1970er-Jahre zu datierender Begriff, der den Optimismus ausdrückt, mit dem man damals glaubte, die menschliche Gesellschaft mit rationalen, eben ingenieurmäßigen, Methoden zum Besseren umgestalten zu können.
[605] Anonymus 2003, S. 80f.; http://lexikon.rhein-zeitung.de/ (zuletzt aufgerufen am 17.09.04).
[606] Eckert u.a. 1991, S. 167.
[607] Eckert u.a. 1991, S. 168.

noch unzählige anderer Hacks begangen. Am 9. August 1999 wurde er zu 46 Monaten Haft und drei Jahren Bewährung verurteilt.

„My motivation was the quest for knowledge, the intellectual challenge... My hacking involved pretty much exploring computer systems and obtaining access to the source code of telecommunication systems and computer operating systems, because my goal was to learn all I can about security vulnerabilities within these systems... My goal wasn't to cause any harm, it wasn't to profit in any way. I never made a red cent from doing this activity. And I acknowledge that breaking the computers is wrong, and we all know that. I considered myself a trespasser, and my motivation was more of – I felt kind of like as an explorer on these computer systems... And that's a completely different motivation of somebody who's really out for financial gain or foreign country or competitor trying to obtain information, like economic espionage, for instance."[608]

Neben dem intellektuellen Wettkampf sieht Kevin Mitnick den Forschungsdrang als einen für ihn gewichtigen Motivationsfaktor an. Er unterscheidet diese Motivation von derjenigen, aus ökonomischen Gründen zu hacken. Es stellt sich hier die Frage, ob Virusschreiber, die ebenfalls zu der Kategorie der Hacker zählen, ähnliche Ambitionen hegen. Dies wird durch ein Interview mit einem Virusprogrammierer deutlich:

„I write viruses as a challenge. I like programming, and writing spreadsheet and database software etc. The idea of a little program that can make a copy of itself even when watched by software specifically designed to stop it intrigues me. The developers of the software have a team of full-time, highly paid programmers working constantly to stop viruses, and here's me, someone who has hardly programmed at all in comparison, working out of my house in my spare time and actually beating their software. That's a challenge, it's a buzz when it works, that's why I do it. I do not spread or encourage the spreading of my (or any other) viruses. I have no interest in spreading my creations to see them in the wild-list, I have no interest in causing damage to anyone's computer, I write only for my own self-recognition.... In the end, you won't stop me by telling me what to do. If you want to stop me, you must understand why I do it, then convince me that I'm doing wrong. I don't think I am, and until I'm convinced by a well thought-out, rational argument by you, I'm not likely to change my mind."[609]

Auch hier erkennt man den intellektuellen Wettkampf als Motivationsgrund. Es zeichnet sich hier auch ein Kampf in der Dimension „David gegen Goliath" ab, wenn dem Virusprogrammierer viele professionelle Antivirenunternehmen gegenüberstehen.

---

[608] http://www.pbs.org/wgbh/pages/frontline/shows/hackers/whoare/testimony.html (zuletzt eingesehen am 19.09.04).

[609] http://vx.netlux.org/lib/vmn01.html (zuletzt eingesehen am 19.09.04).

Eckert u.a. sprechen im Zusammenhang mit der Herausforderung als Motiv in ähnlicher Art und Weise wie Sherry Turkle von der perfekten Beherrschung des Computers als Motiv. Dies wird auch an den von Eckert u.a. aufgezeigten Aussagen einzelner jugendlicher Hacker deutlich:

Johannes, 21 Jahre, Hacker
„Es ist ein Sport, in dieses System reinzukommen, ein Passwort zu finden. Wenn du im System bist, versuchst du, ein höheres Privileg zu erreichen, auf dem du Systemmanager werden kannst, mit allen Privilegien. Ein Systemmanager kann alle Akten lesen etc. Er kontrolliert das System und das ist der Sport, wenn du versuchst, das höchste Privileg zu erreichen (...). Du versuchst, alles über das System herauszufinden und wenn du alles auf dem System tun kannst, ja dann ist das Telefonat beendet."

Detlef, 28 Jahre, Hacker
„Besonders reizvoll ist es, wenn der Super-User eines anderen Netzes bemerkt, dass jemand eingedrungen ist und seinerseits versucht, den Eindringling zu eliminieren. Es ist für jeden Hacker der Höhepunkt, die totale Kontrolle über das andere Netz erreicht zu haben. (...) Da drauf kommt es an, das ist das Ziel eines Hacks."

Diese Hacker versuchen, ihr technisches Können mit denen ihrer Gegner zu messen, und arbeiten ausdauernd an den dafür notwendigen Lösungen, sie treibt die intellektuelle Herausforderung und der Reiz, technische Möglichkeiten auszuloten.[610] Der Lernprozess gestaltet sich zumeist autodidaktisch oder unter Zuhilfenahme Gleichgesinnter, wobei jeder Lehrer und Schüler zugleich ist. Pekka Himanen vergleicht diesen Lernprozess mit der Akademie Platons, der den Schüler nicht als Objekt der Wissensvermittlung betrachtet, sondern als Partner beim Lernen (synetheis). Aus dieser Sicht ist der Hauptzweck des Lehrens, die Fähigkeiten des Lernenden zu festigen, Probleme zu erkennen, Gedankengänge zu entwickeln und kritische Fragen zu stellen:[611] „Der typische Lernprozess des Hackers beginnt mit einem interessanten Problem. Dann arbeitet er unter Verwendung verschiedener Quellen auf eine Lösung hin und unterzieht sie umfangreichen Tests."[612] Wichtige Quellen stellen dabei Chats oder Diskussionsforen dar, in denen alle denkbaren Probleme miteinander besprochen und analysiert werden. Dabei ist jeder Hacker selbst Empfänger und Sender von

[610] Eckert u.a. 1991, S. 169.
[611] Himanen 2001, S. 99.
[612] Himanen 2001, S. 97.

siert werden. Dabei ist jeder Hacker selbst Empfänger und Sender von Ideen. Auf diese Art und Weise stellen sich Hacker nicht nur alleine, sondern gemeinsam bestimmten Herausforderungen und Problemen, die zu überwinden sind. Auch wenn Pekka Himanen in erster Linie von echten Hackern spricht, so sind die Lernprozesse auch bei den Crackern identisch.

Paul A. Taylor sieht ein noch intensiveres Motiv als die Herausforderung oder die Beherrschung des Computers als Grund für das Hacken:
„Linked to the previously mentioned notion of machismo in hacking culture is the motivational factor of power... Without doubt, however, feelings of power do complement the main motivation of curiosity. Breaking into a bigger or more important System, or acquiring root-status can give you a real feeling of power and you seem to have proved yourself better than the System administrator... It is a dream of recovering power and wholeness by seeing wonders and by not being seen."[613]

Taylor sieht das Machtgefühl als einen wichtigen Motivationsfaktor an. Das Ziel von Hackern sei es, die höchste Zugriffspriorität zu haben. Je mehr Zugriffsmöglichkeiten er besitzt, desto mehr Macht kann er über das System und den Nutzer ausüben. Interessant ist hierbei auch, dass Eckert u.a. die höchste Zugriffspriorität als intellektuelle Herausforderung betrachten und Taylor dies als Ausübung von Machtgefühlen beschreibt. Obwohl das Ziel dasselbe ist, bleibt der Weg zur höchsten Zugriffspriorität jedoch eine Herausforderung. Das Ziel ermöglicht sodann auch Macht auszuüben, so dass sich beide Aussagen trotz der unterschiedlichen Ausgangslage nicht widersprechen. Die immerwährende Beherrschung des Systems, ohne entdeckt zu werden, gibt dabei einigen Hackern Allmachtsgefühle.

In ähnlicher Weise antwortet auch Anonymous in einem Interview auf die Frage, was für ihn ausschlaggebend fürs sein Handeln war:
„Well, everybody likes to feel in control. It's intellectual. It stimulates my mind. It's a challenge."[614] Kontrolle ist also ein weiteres Motiv für Hacker und eine Form der Machtausübung. Gerade die Kontrolle über wichtige Daten wie Staatsgeheimnisse, die zum Beispiel an fremde Regierungen gegeben werden, verschafft Macht und Einfluss.[615]

[613] Taylor 2001, S. 56ff.
[614] http://www.pbs.org/wgbh/pages/frontline/shows/hackers/interviews/anon.html (zuletzt eingesehen am 19.09.04).
[615] Russel/Cunningham 2001 S.51.

Charles Tittle entwickelte in einem solchen Zusammenhang die „Kontrollbalance-Theorie“.[616] Danach habe das Verhältnis zwischen der Kontrolle, die eine Person selbst ausüben kann, und der Kontrolle, welcher sie unterworfen sei, einen erheblichen Einfluss auf die Kriminalitätsentstehung. Es scheint, als ob bei Hackern ein Kontrollüberschuss vorhanden sei. Tittle führt hierzu aus:

„The theory also contends that control ‘surpluses’ reflecting ability to exercise more control than that to which one is subject will express themselves in ‘autonomous’ forms of deviance, exploitative, plunderous, or decadent. Consequently, the greater the control surplus, the greater the chances of some form of autonomous deviance.”[617]

Der Hacker kann die volle Kontrolle über das System ausüben, ohne selbst kontrolliert werden zu können.[618] Ist ein Hacker in ein System eingedrungen, versucht er, seine Kontrollmöglichkeit zu verstärken, indem er die uneingeschränkte Zugriffpriorität erhalten möchte. Hat er eine solche, kann er seine Machtposition in jeglicher Form nutzen („exploitation“).[619] Die höchste Form der Machtausübung stellt der Ausschluss des Systemadministrators von seinem eigenen System dar. In diesem Zusammenhang stellten Mark Colvin u.a. die Frage, ob der Kontrollüberschuss nur dann ein kriminogener Faktor ist, wenn das soziale Umfeld die egozentrische Verfolgung des eigenen Vergnügens propagiert. Betrachtet man diesbezüglich die unterschiedlichen Hackergruppierungen, so könnte die altruistische Haltung einiger Hacker, z.B. des CCC, dazu führen, dass Hacker durch dieses Umfeld versuchen, Unternehmen und Institutionen über systembedingte Schwachstellen aufzuklären, ohne Schäden zu verursachen.

Gröndahl beurteilt Macht aus einem anderen Blickwinkel. Seiner Ansicht nach betrachten Hacker den Staat und die ganze Gesellschaft als einen Komplex, dem sie zwar überlegen seien, der aber ungerechtfertigterweise große Macht über sie habe. Die Hauptziele von Hackern sei der Schutz vor der Macht des Staates und der Industrie. Andererseits zeigt diese Einstellung, dass Hacker Macht haben oder sie zumindest in dem vorhandenen Rahmen behalten wollen, ohne dass der Staat weitere Sanktionen oder andere Eingriffe in den Bereich der Computertechnologie vornimmt.

[616] Tittle 1995.
[617] Tittle 1995, S. 180.
[618] Die einzige Möglichkeit bestünde durch Strafverfolgungsbehörden.
[619] Tittle 1995, S. 181.

Hier zeigt sich wiederum die Definitionsmacht des Staates gegenüber den Hackern. Sie haben das Gefühl, dass sie anhand von Regeln gemessen und verurteilt werden, an deren Definitionsprozess sie nicht beteiligt waren und die sie nicht akzeptieren.

3.8.4 Spieltrieb und Probehandeln

Wetzstein u.a.[620] sehen im Bereich der Verbreitung von Computerviren auch den Reiz, etwas Verbotenes zu tun und Neugierde und Spaß zu befriedigen. Hierfür zitieren sie einige Aussagen aus Interviews, bei denen es um Hoaxes geht:[621]

„Man will eben einfach mal ausprobieren, ob es denn tatsächlich funktioniert. Das ist einfach ein Scherz, so wie man sich früher im Keller versteckt hat, ein Portemonnaie auf die Straße gelegt hat, und das dann mit einem Faden weggezogen hat, wenn sich jemand danach gebückt hat."

„Es gibt Leute, die machen es hauptsächlich wegen dem Spaß. Das würde ich auch noch nicht als Virus bezeichnen. Das ist halt nur ein Programm, was sich weiterverbreitet und ja, irgendwann auch mal aktiv wird und irgendeinen doofen Spruch auf den Monitor schreibt, aber mehr auch nicht."

„Das ist das Spiel mit dem Feuer, vielleicht auch ein bisschen der Reiz, ein Verbrechen zu begehen, ohne dass man hinterher dafür belangt werden kann."

Die Intention ist vielmehr der Reiz, „sich einen Schabernack zu erlauben" oder „etwas Verbotenes zu tun". Die Gefahr, die auch mit der Verbreitung eher harmloser Viren verbunden sein kann, wird dabei häufig nicht erkannt. Die Täter sind oftmals Jugendliche oder sogar Kinder. Hinter diesen Computerviren stecken keine bösen Absichten, sondern es ist die Freude am Ausprobieren, vergleichbar mit dem Spielen. Nun wird aber nicht mehr mit Kinderspielzeug

[620] Bei diesem Werk handelt es sich um eine weitere von Roland Eckert geleitete Studie über die Kultur der Computernetze. Die Studie wurde zwischen den Jahren 1991 und 1994 von der „Arbeitsgemeinschaft sozialwissenschaftliche Forschung und Weiterbildung an der Universität Trier e.V." geführt. Die Studie beschäftigt sich mit den Nutzern von nichtkommerziellen Computernetzen. Soziale und kulturelle Aspekte dieses expandierenden Marktes werden dabei untersucht. Was wird sich ändern, bei uns selbst, in unseren persönlichen Beziehungen, in den Formen des Redens, Schreibens, Hörens und Lesens? Welche neuen Formen der sozialen Kontrolle und des abweichenden Verhaltens entwickeln sich? Welche Dimensionen von Gleichheit und Ungleichheit setzen sich durch? Welche angleichenden und differenzierten Effekte ergeben sich in der modernen Kultur? Welche Konsequenzen also hat die weltweite Vernetzung?

[621] Wetzstein u.a. 1995, S. 240.

gespielt, sondern mit Programmcodes. Dies wird vor allem bei so genannter Hoaxes (Scherzviren) erkennbar.[622] Armin Medosch sieht den Erfolg von Hoaxe-Urhebern darin, durch geschicktes Social Engineering urmenschliche Eigenschaften wie Angst, Gutgläubigkeit und Hilfsbereitschaft auszunutzen.[623] Dabei spielt auch das Klima der Virenhysterie, das von den Medien geschaffen wurde, eine Rolle. Diese Hysterie wurzelt nach Ansicht von Medosch und Janko Röttgers in irrationalen Ängsten vor einer Seuche, die sich nicht kontrollieren lässt und die plötzlich Fehlfunktionen im menschlichen Organismus oder dem Computer auslöst. Neben Ängsten werfen Hoaxes ihrer Ansicht nach zusätzlich einen Köder aus. Wer die Warnung rechtzeitig weiterleitet, macht sich bei Freunden beliebt.[624] Das Motiv ist die gelungene Täuschung.

Der Spaßfaktor muss vor allem bei den Script-Kiddies vermutet werden. Dabei geht es darum zu testen, ob die angewandte Taktik Wirkung zeigt; jemandem einen Streich zu spielen oder einfach zu sehen, was mit einem selbst geschaffenen Programm geschieht. Script-Kiddies schreiben jedoch nicht nur Hoaxes, sondern auch Viren, die einen tatsächlichen Schaden anrichten. Neben Viren verschaffen sich Script-Kiddies mit vorgefertigten Zugangstools Zugang zu fremden Computern, verunstalten Webseiten und starten DoS-Attacken.[625] Pekka Himanen sieht den Spaßfaktor des Hackens im spielerischen Erkunden, im „Experimentieren mit dem Computer“ und im „Herumbasteln am Softwarespielzeug“.[626] Es scheint, als ob Kinder keine Berührungsängste mit dem Computer haben. Sie nutzen ihn als Spielzeug, einerseits auf der Hardwareebene, indem sie zum Beispiel Festplatten austauschen, neue Hardware selber einbauen oder Rechner miteinander vernetzen. Andererseits bewegen sie sich auf der Softwareebene, indem sie mit Programmen herumspielen oder das Internet nutzen.

Debra Littlejohn Shinder[627] sieht im Computer ebenfalls ein Spielzeug und im Internet den dazugehörigen Spielplatz.[628] Sie unterteilt jugendliche Hacker, deren Motivation hauptsächlich darin liegt, ihren persönlichen Spaß zu haben, in die vier folgenden Gruppen:

---

[622] Wetzstein u.a. 1995, S. 239 f.
[623] Medosch/Röttgers 2001, S. 89.
[624] Medosch/Röttgers 2001, S. 90.
[625] Medosch/Röttgers 2001, S. 117.
[626] Himanen 2001, S. 22.
[627] Debra Littlejohn Shinder ist eine ehemalige Polizistin und Ausbilderin an einer Polizeiakademie. Sie und ihr Ehemann, Thomas W. Shinder, haben computertechnische Beratungsdienste für Unternehmen angeboten, leiteten Vorträge und Übungen an Hochschulen und führten Seminare. Sie hat sich auf Netzwerke und Computersicherheitssysteme spezialisiert und in diesem Zusammenhang viele Bücher und über 100 Artikel in Zeitschriften veröffentlicht. Ihr Buch beschreibt die Problematik der Computergesellschaft aus technischer und soziologischer Sicht und kann dadurch Computerspezialisten sowie Wissenschaftlern und Politikern nützlich sein. Interessant ist dabei, dass das Buch nicht aus Sicht eines Insiders, sondern aus der Sicht einer Person geschrieben ist, die

„Pioneer types, who are fascinated by the technology. Scamps playful hackers who don't intend to do any harm. Explorers, who get their kicks out of going where no hacker has gone before or at least, where they themselves have never been. Game players, who look at hacking into Systems as a game."[629]

„Pioneer types" sind von der Technologie fasziniert, sie lernen dabei, wie der Computer funktioniert, durch das „Trial-and-error-Prinzip". Der Spaßfaktor liegt hier in erster Linie im eigenen Lernprozess. „Scamps" sind die harmlosen und verspielten Hacker. Sie verändern Webseiten und fügen Initialen oder kleine Späße hinzu, zerstören jedoch nicht mutwillig fremde Daten. „Explorers" sind die Forscher unter den Hackern. Hier steht die Entdeckungslust im Mittelpunkt. Sie brechen in Netzwerke ein, um sich umzuschauen, ohne etwas zu zerstören. „Game players" spielen mit dem System. Ihre Gegner sind dabei die Systemadministratoren. Die Motivation des Spiels liegt darin, gegen diese zu gewinnen. Diese Motivationslage wurde bereits bei den Hackern erläutert, die Macht und Kontrolle ausüben wollen.[630] Diese vier Typen von Hackern haben keine praktischen oder finanziellen Absichten, vielmehr ist das Hacken hier wie ein Hobby zu betrachten.[631]

Den Scamps vergleichbar beschreibt Roland Girtler eine Gruppe von Hackern als „verspielte Spaßmacher", die auf harmlose Weise Unruhe verbreiten wollen.[632] Daneben nennt er Neugier als weiteres Motiv. Dabei vergleicht er Hacker mit Entdeckern, die mit ihren Schiffen auslaufen, um unbekannte Orte aufzuspüren. Der Anschluss eines Computers an das Internet gleicht dabei der Gründung eines neuen Hafens.[633] Dieser Vergleich erscheint bezeichnend, da gerade beim typischen Hacking, bei dem in fremde Rechner eingedrungen wird, im Vorwege die Ports[634] ausgekundschaftet werden müssen. Im Jahr 2001 reichte der offene Port 1433 aus, um Zugriff auf die Datenbanken des Weltwirtschaftsforums in der Schweiz zu be-

---

eher auf der staatlichen Seite steht. Ihre Herangehensweise weicht daher teilweise von derjenigen der Szene ab, hat aber trotzdem vergleichbare Motivationslagen entdeckt.

[628] Shinder 2002, S. 114.

[629] Shinder 2002, S. 113.

[630] Shinder 2002, S. 113 ff.

[631] Shinder 2002, S. 114.

[632] Girtler 2003, S. 218.

[633] Girtler 2003, S. 217.

[634] Port bezeichnet Zusammenhang mit Computerhardware eine Schnittstelle, an die man weitere Geräte z. B. mit einem Kabel (z. B. Parallelport oder USB-Port) anschließen kann oder in die man Steckkarten einschieben kann (z. B. PCI-Port). Daneben wird der Begriff Port auch noch für die logische Repräsentierung bei der Adressierung dieser Schnittstellen verwendet. Ports sind dabei Adresskomponenten, die in Netzwerkprotokollen eingesetzt werden, um Datenpakete den richtigen Anwendungen zuzuordnen. Sind diese ungesichert, werden sie als „offen" bezeichnet.

kommen.[635] Der CCC beschreibt die Entstehung virtueller Welten mit den Seefahrten eines Christoph Columbus. Diese Beschreibungen ähneln dabei den Explorers von Debra Littlejohn Shinder. Neugier wird im Allgemeinen überhaupt als der wichtigste Motivator für das Hacken angesehen.[636]

Eckert u.a. zitieren in diesem Zusammenhang drei Auszüge aus Interviews:

„Achim, 22 Jahre
‚Ich habe mal über einen Typen eine Telefonnummer bekommen und habe dann auch versucht, das System zu hacken. Das war so eine Idee, da mal reinzuschreiben, ich war da. Es war eigentlich nur reine Neugierde. Die halbe Zeit klappt das sowieso nicht.'

Harald, 22 Jahre
‚Ich habe das Hacken halt auch mal so versucht. Es geht eigentlich darum, einige Sachen auszuprobieren, einen höheren Status zu bekommen. Das macht einfach Spaß, mal ein bisschen rumzutesten. Mal gucken, ob man auf die Ideen, die andere Leute hatten, auch kommt. Aber ich mache es nicht regelmäßig. (...) An sich mache ich ja andere Sachen am Computer. Ich programmiere sehr viel, das macht mir am meisten Spaß (...).'

Hans-Magnus, 29
‚Warum hacke ich? Eigentlich ist es reine Neugier. So richtig interessiert mich das ganze nicht. Das war so die paar Mal, wo ich gehackt habe. Mehr nicht. Überhaupt mache ich es auch nur ganz selten, ich bin eigentlich auch kein Hacker.'"[637]

Es zeigt sich, dass die Hauptmotivation darin liegt, die eigene Neugier zu befriedigen sowie sich hiermit zu zerstreuen. Ihnen geht es dabei nicht um Kniffe und Tricks des Hackens, sondern vielmehr um das reine Ausprobieren, ob es wirklich geht. Deshalb sind ihre Strategien unsystematisch, so dass sie mit vielen Fehlversuchen konfrontiert werden. Jedoch kann das Interesse durch das Ausprobieren geweckt werden, so dass aus einst harmlosen professionelle Hacker werden.[638] Auch für Paul Taylor ist die Neugier ein Grund für das Hacken:

[635] Girtler 2003, S. 217.
[636] Russel/Cunningham 2001, S. 50 f.
[637] Eckert u.a. 1991, S. 164.
[638] Eckert u.a. 1991, S. 164.

„In this light, hackers emphasise how such innate curiosity is the fundamental basis from which most technological improvements and adaptations are ultimately derived. The 'hacker mentality' therefore is seen as a positive attribute that drives forward technological development."

Der Autor beschreibt das Hacken als eine Notwendigkeit für die technische Weiterentwicklung. Eckert u.a. sprechen auch von „Thrill-Erlebnissen" und „emotionalen Kicks". Das Hacken befriedigt spezielle Gefühle und ist nichts Alltägliches, vielmehr wird es zum Erlebnis, bei dem die Akteure zu „Sensation-Seekers" werden. Gerade für Hacker, die sich schon lange mit dem Computer beschäftigen, wird vieles Routine, so dass Langeweile aufkommt. „Erst die Kicks und Thrills beim Öffnen eines fremden Computers bringen wieder Abwechslung, Spannung oder Euphorie."[639]

In einem Interview im Jahr 2001 mit dem damals 18-jährigen Raphael Gray (alias Curador) wird das Hacken als ein Äquivalent zu „Sex, Drugs and Rock-and-Roll" bezeichnet.[640]

„After the first ten minutes, when I was waiting for the five and a half thousand credit cards I was to download from the first site ... certainly there was a great rush, so to speak. You do get a rush from doing it, definitely. There is a lot of adrenaline, if nothing else, while you're trying to track it down. I sometimes spent two days solid trying to do something without sleep, without anything, just constantly trying to do it. And when you finally get through, the relief is not just from the fact that you got it, but now you can sleep."

In den Aussagen zeigen sich deutlich Parallelen zum Spaß am Spielen. Ist ein Spiel erst einmal gewonnen, z.B. gegen einen Systemadministrator, so folgt die Suche nach einem neuen Spiel, bei dem man wieder einen Kick erfahren kann. Den Kick erleben auch Hacker, die es sich zur Aufgabe gemacht haben, Kopierschutzprogramme zu knacken. Auch hier macht es ihnen umso mehr Spaß, je ausgefeilter der Kopierschutz ist.[641] Dabei kann auch vermutet werden, dass neben dem Kick als weiterer Auslöser für das Hacken die Langeweile des Altbekannten ebenfalls als Auslöser des Hackens zu nennen ist. Aufklärerische Gedanken stehen dabei in keiner Weise im Vordergrund. Neben dem Spiel gegen eine andere Person ist auch das Spielen mit der Sache selbst von Bedeutung. In einem Interview mit Sarah Gordon, einer Soziologin, die sich mit der Hackerkultur beschäftigt,[642] werden diese Aspekte deutlich:

---

[639] Eckert u.a. 1991, S. 165.

[640] http://www.pbs.org/wgbh/pages/frontline/shows/hackers/interviews/curador.html (eingesehen am 27.09.04).

[641] Medosch/Röttgers 2001, S. 39.

[642] Sarah Gordon untersuchte aus soziologischer Sicht Virenautoren. Da sie unter anderem das Bild des krankhaften Virenprogrammierers zu revidieren versuchte, erfuhr sie in der Szene einen gewissen Bekanntheitsgrad.

„Basically, they think it's a game. They don't realize the impact. They play with computers at school and at home, and we encourage that, but we don't encourage responsible behavior on the computer. They find a virus and tinker with it, and they don't realize what they're doing. These kids generally don't have mal-intent. But keep in mind, it only takes two or three people to send out a virus, and it multiplies over and over, and it can really mess up the system. So while they may not realize the impact, the effects can be quite destructive.“[643]
Hier wird vor allem deutlich, dass die fehlende Erziehung zum verantwortungsvollen Umgang mit dem Computer als ein großes Defizit angesehen wird. Dies mag mit dem mangelnden technischen Verständnis auf Seiten der Eltern zusammenhängen.

3.8.5 Anerkennung der Gruppe

Sherry Turkle sieht in dem Streben, etwas Besonderes sein zu wollen, einen wichtigen Grund für das Hacken. Dafür zitiert sie die Aussage eines jugendlichen Hackers: „Da ich anders war, so anders, dass ich zu den Typen irgendwie nicht passte, hab ich, glaube ich, beschlossen, wirklich anders zu werden, richtig anders. Ich wollte immer schon etwas Besonderes sein.
Und wenn ich hacke, ist es mir wichtig, mein eigenes Territorium zu haben. Ich glaube, dass die echten Hacker alle so empfinden. (…) Ich empfinde ein sehr starkes Bedürfnis danach, anders zu sein. Ich habe mein ganzes Leben im Abseits verbracht und habe gelernt, dass das die richtige Art zu leben ist. Mein Traum ist, dass ich jemand sein möchte, der etwas tut, etwas entdeckt, etwas schafft, dass die Leute mich anschauen und sagen: Bah, der Typ ist echt was Besonderes – mit dem möchte ich gern zusammen sein. Das ist alles, was ich mir jemals gewünscht habe. Von allen auf der ganzen Welt geliebt zu werden. Hacken ... das ist eine andere Welt. Es war ein Ort, wo ich mir einen Namen machen konnte, weil es um etwas ging, das ich gut konnte, womit ich umgehen konnte, etwas, was mich von anderen unterscheidet – was mich abseits stellt... das macht mich glücklich. Ich weiß nicht, warum ich das brauche.“[644]
Der Computer bietet genügend Möglichkeiten, sein eigenes Territorium zu finden, um auf diese Art und Weise in einem speziellen Bereich etwas Besonderes sein zu können. Es fängt dabei mit der eigenen Webseite an, die eine Person so aufbaut, dass sie ein Bild von ihr widerspiegelt, wie sie gern von außen wahrgenommen werden will. Daneben kann man sich

---

Einige Virenprogrammierer sehen in ihr eine Verbündete. Z.B. stand im Programmcode der berühmten Mutations Engine von Dark Avenger eine Widmung: Wir widmen diesen kleinen Virus Sarah Gordon, womit sie schlagartig in der Szene berühmt wurde.
[643] Konrad 2002.
[644] Turkle 1984, S. 265.

über ein spezielles Fachwissen auf verschiedenen Sektoren profilieren. Spiele, Musik, Filme, Sicherheit, Hardware- oder Softwareprobleme sind nur ein kleiner Teilbereich von möglichen Profilierungsgebieten. Dadurch, dass der Computer heutzutage einen wichtigen Stellenwert auf dem Spielesektor, in der Wirtschaft und in privaten Haushalten hat und nur von ganz wenigen Nutzern beherrscht wird, können sich Hacker durch Wissen und Hilfestellungen hier gegenüber Erwachsenen oder Freunden profilieren. Die Möglichkeiten reichen bis hin zur Berühmtheit durch bekannte Viren oder Hacks, wobei hier gerade ein Problem mit der Anerkennung entsteht. Offenbart man sich gegenüber seiner Gruppe, besteht die Gefahr der strafrechtlichen Verfolgung, verheimlicht man seine Taten, so bleibt die gesellschaftliche Anerkennung versagt. Somit erlangen einige Hacker nur Annerkennung innerhalb ihrer Community.[645] Zum Teil wird dieses Problem aber mit sogenannten Pseudonymen gelöst.[646] Dabei geben sich die Virenautoren oder Hacker die kuriosesten Namen. Bei Viren wird das Pseudonym häufig in den Quellcode geschrieben, den nur Eingeweihte oder zumindest Menschen mit einem gewissen computertechnischen Fachwissen entschlüsseln können.[647] Wenn Viren sich weit verbreitet haben, zeigt dies, dass der Hacker gut programmieren kann und Systeme und ihre Schwachstellen erkannt hat.[648] Hacker hinterlassen in dem System an speziellen, für den Systemadministrator auffindbaren Stellen ebenfalls ihre Pseudonyme. Damit zeigen sie ihm, dass das System gehackt wurde, von wem es gehackt wurde, und wenn derselbe Hacker immer wieder eindringen kann, zeigt er somit seine Überlegenheit, da der Administrator ansonsten nicht erkennen kann, wer in das System eingebrochen ist. Der Hacker lebt mit der Vorstellung, dass er sich zumindest gegenüber dem Administrator Respekt und Anerkennung verschafft hat. Zeigt er seine Überlegenheit öffentlich an, z.B. in IRCs, erlangt er gegenüber der Hackergemeinde ebenfalls Berühmtheit.

Ryan Russel und Stace Cunningham nennen dieses „etwas Besonderes sein“ Anerkennung und sehen in ihr den häufigsten Beweggrund für Hacker.[649] Es geht Hackern um Ruhm, um den Aufbau des persönlichen Renommees oder einfach nur um Angeberei. Sie sehen den Ursprung im Bedürfnis nach Zuwendung, das jedem Menschen innewohne.[650]

[645] Medosch/Röttgers 2001, S. 120.
[646] Russel/Cunningham 2001, S.49.
[647] Turkle 1984, S. 288.
[648] Turkle 1984, S. 288.
[649] Russel/Cunningham 2001, S. 47 ff.
[650] Russel/Cunningham 2001, S. 48.

Dabei geht es um die Annerkennung durch die Hackergemeinde sowie durch den Rest der Menschheit, was durch einen Auszug aus der Hacker-Cologne des CCC verdeutlicht werden soll:

„Hacker bauten das Internet, Hacker machten das UNIX Betriebssystem zu dem, was es heute ist, Hacker betreiben das Usenet, Hacker brachten das World Wide Web zum Laufen, Hacker schufen noch viel mehr. Wenn du ein Teil dieser Kultur bist, wenn du zu ihrem Sein und ihrer Entwicklung beigetragen hast, wenn andere Mitglieder wissen, wer du bist und dich einen Hacker nennen, erst dann bist du auch wirklich ein Hacker. (…) Wie in den meisten Kulturen ohne Geldwirtschaft basiert die Hackergemeinde auf Ruf und Ansehen der Mitglieder. Du versuchst, interessante Probleme zu lösen, aber wie interessant und wie gut deine Lösungen wirklich sind, entscheiden nur diejenigen, die dir ebenbürtig oder überlegen sind. Folglich wirst du, wenn du den Hacker-Weg wählst, lernen müssen, dich hauptsächlich auf Grund der Achtung und der Haltung der anderen Hacker gegenüber deinen Fertigkeiten einzuschätzen.“[651]

Die Autoren nennen zudem noch eine Variante der Anerkennung, die Bewunderung von Anderen. Es handelt sich dabei meist um Kinder und Jugendliche, die aus Bewunderung für andere Hacker die Hackertechniken erlernen möchten, vergleichbar mit Idolen aus der Musikkultur. Den Hackern kommt somit eine Vorbildfunktion zu. Leider erscheinen mehr Berichte über spektakuläre Hackerangriffe als Berichte über Hackertechniken, die der Gesellschaft weiter geholfen haben.[652] Gerade Script-Kiddies versuchen, in die Fußstapfen berühmter Hacker wie z.B. Kevin Mitnick zu treten.[653]

Im Sinn der differenziellen Identifikation spricht Daniel Glaser in diesem Zusammenhang davon, dass nicht generelle Kontakte zu dissozialen Personen oder Gruppen kriminelle Handlungen auslösen, sondern es innerhalb dieser Personenmehrheiten wiederum ganz bestimmte Personen sind, mit denen sich jemand identifiziert, um sie dann als Vorbild für die eigenen Motive und Verhaltensweisen zu nehmen.[654] Die Identifikation mit Hackern, die als Vorbilder gesehen werden, könnte somit ebenfalls ein Motiv darstellen, das andere Personen dazu veranlasst, kriminelle Handlungen mit dem Computer zu begehen.

[651] http://koeln.ccc.de/prozesse/writing/artikel/hacker-howto-esr.html (zuletzt eingesehen am 28.09.04).
[652] Russel/Cunningham 2001, S. 49 f.
[653] Anonymus 2003, S. 230.
[654] Glaser 1956, S. 440.

Pekka Himanen beschreibt diesen Aspekt als den Wunsch nach einem „Sozialleben“.[655] Das ist das Bedürfnis dazuzugehören, anerkannt und geliebt zu werden. Jeder Mensch benötigt das Gefühl der Gruppenzugehörigkeit. Das Dazugehören stellt dabei aber nur einen Teil der Bedürfnisse dar. Dies zeigt sich durch die Erfahrung, ein Teil einer Gemeinschaft zu sein, ein „Wir-Gefühl“ aufzubauen, respektiert zu werden und für andere etwas Besonderes zu sein.[656] Dadurch wird auch begreiflich, warum Hacker in ihrer Freizeit Programme schreiben und kostenlos weitergeben. Hacker streben nach Anerkennung durch Gleichgesinnte, die ihre Leidenschaft teilen. Pekka Himanen vergleicht Hacker mit Forschern an Universitäten, für die seiner Ansicht nach die Bestätigung durch die Gruppe eher entscheidend ist als z.B. Geld. Es geht um die Schaffung von Innovationen für die Gemeinschaft.[657] Hierin liegt auch die Motivation für Projekte im Open-Source-Modell begründet.

Boris Gröndahl betitelt diese Motivationslage mit dem Begriff Respekt und sieht im Hacken eine zum Teil soziale Tätigkeit. Hacker bilden für ihn eine Elite, die bestimmte Qualifikationen verlangt. Im Elitedenken sieht er auch die Abgrenzung zum Rest der Gesellschaft begründet. Viele gesellschaftliche Autoritäten, die faktisch die Macht über die Computertechnologie besitzen, werden daher nicht anerkannt.[658] Das erklärt auch, dass Hacker für die Freiheit der Daten plädieren und es sich nicht gefallen lassen wollen, dass der Staat oder Unternehmen den Zugang zu diesen Daten nicht allen zugänglich machen. Es scheint, als sähen sie sich als Hüter der Computertechnik. Sie dringen ohne zerstörerische Absichten in Systeme ein oder verschicken Viren, um zu demonstrieren, dass sie das System beherrschen und es auch zerstören können. Nach Boris Gröndahl unterscheiden sich die Hacker in ihrem Elitedenken nicht von anderen Subkulturen. Allerdings ist bei Hackern der Leistungsaspekt auch intern begründet, so dass im Unterschied zu vielen anderen Subkulturen auch ein Wettkampf innerhalb der Gemeinschaft stattfindet.[659] Er bezeichnet dies als Meritokratie,[660] womit er meint, dass derjenige am meisten Ansehen genießt, der in irgendeiner Form am meisten geleistet hat.

Neben dem Elitedenken besteht auch eine eigene Sprache und Hierarchie in der Hackerszene, so dass diese an die von Albrecht K.Cohen und James F. Short beschriebene „konfliktorientierte Subkultur“ erinnert: „Die Banden haben einen Namen, einen ausgeprägten Sinn für

[655] Himanen 2001, S. 70 ff.
[656] Himanen 2001, S. 70.
[657] Himanen 2001, S. 73 ff.
[658] Gröndahl 2000, S. 17.
[659] Gröndahl 2000, S. 17.
[660] Wohl von meriotisch verdienstlich, sachlich, inhaltlich.

Korpsgeist, haben eine eigene Persönlichkeit oder einen Ruf (´rep´) in der Bandenwelt. Der Status der Bande wird weitgehend bestimmt durch ihre Härte, d.h. durch ihre Bereitschaft, sich mit anderen Gangs in physischen Konflikt einzulassen.“[661] Die Kampfhandlungen werden hierbei online ausgetragen und richten sich grundsätzlich nicht gegen andere Hacker, sondern gegen Institutionen. Im Grad der Organisiertheit unterscheidet sich die Hackerszene wiederum von den beschriebenen Bandenstrukturen. Cohen und Short sehen jedoch auch bei Banden strukturärmere Verhältnisse als vorherrschend an: „Wahrscheinlich ist eine Zwischenform des Konflikt-Gangs und der Basis-Subkultur weiter verbreitet als der hier beschriebene Bandentyp: eine locker organisierte und amorphe Koalition von Cliquen mit einem nur vagen Zusammengehörigkeitsgefühl, die sich häufig zur Ausübung offener Gewalt sporadisch zusammenschließen.“[662]

Im Cracken von Software sehen Eckert u.a. ähnliche Motive und zitieren hierfür einen Jugendlichen:

„Albrecht, 19 Jahre
‚Wir waren eine Zeitlang wohl die größte Crackergruppe in Europa. Mit größte ist jetzt nicht gemeint, die Anzahl der Leute, sondern wie schnell man das Programm bekommen hat und dann auch gecrackt natürlich. (...) In der Szene wird das so beurteilt: Gut bedeutet, wenn man das Programm möglichst noch gecrackt hat, bevor es auf den Markt kommt. Je früher man das schafft, desto besser ist man (...) Wichtig ist auch, auf welche Weise die Programme gecrackt sind, ob alle Abfragen raus genommen sind, oder nicht.’“[663]

Denis Moschitto und Evrim Sen[664] sehen im Bereich der Softwarepiraterie ein Wettrennen der Softwarecracker gegen die Industrie sowie ein Wettrennen der Softwarecracker untereinander. Die beiden Autoren kamen schon im Alter von 13 und 15 Jahren in Kontakt mit legendären Hackergruppen wie „Skid Row“ oder „Paranoimia“. Die Szene selbst nutzt sog. Boards zur weltweiten Verbreitung von Raubkopien.[665] Boards oder genauer Bulletin Board System (BBS) sind eigens von der Szene entwickelte Mailboxsysteme, um sich nicht der öffentlichen

[661] Cohen/Short 1979, S. 378 f.
[662] Cohen/Short 1979, S. 379.
[663] Eckert u.a. 1991, S. 223.
[664] Die beiden jungen Autoren beschreiben den Grenzbereich zwischen Legalität und kriminellen Handlungen der Hackerszene, in der sie sich selbst seit vielen Jahren bewegen. Auch wenn das Buch kein Detailwissen vermittelt, so zeigt es durch die einzelnen Schilderungen die Motivationsgründe einzelner Hacker. Positiv ist zu bewerten, dass neuere Szenen wie die Demoszene ausführlich beschrieben werden. Seinen Wert erhält dieses Buch vor allem dadurch, dass es von Insidern geschrieben wurde.
[665] Moschitto/Sen 1999 S. 31f.

Kommunikationssysteme bedienen zu müssen.[666] Diese Programme sind ausschließlich für die Handhabung von Software entwickelt worden und unterscheiden sich daher im Aufbau von gewöhnlichen Mailboxprogrammen. Zugang erhält man nur durch Mitgliedschaft in der Szene selbst und diese nur durch Kontakt zu einzelnen Mitgliedern. Selbst wenn man den Zugang unberechtigterweise erlangt hat, sind die Boards dergestalt komplex strukturiert, dass sie für unerfahrene Nutzer ungeeignet sind. Auf diese Weise sollen die Boards vor Außenstehenden geschützt werden.[667] Denis Moschitto und Evrim Sen beschreiben die Mitgliedschaft folgendermaßen: „Szenemitglieder selbst werden in den Boards nur so lange 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.“[668] Je schneller ein Softwarecracker gecrackte Versionen einer Software in seinem Sortiment anbieten kann, desto höher steht er im Ansehen der anderen. Besonders schnelle Boards veröffentlichen Software bereits am Tag der offiziellen Erscheinung als gecrackte Version. Im Szenejargon nennt man dies „O-Day-Warez“, d.h., dass der Crack noch keinen Tag alt ist. Üblich ist dabei, dass Softwareprodukte am Tag der Neuerscheinung schon gegen Mittag gecrackt und am Abend in allen Boards der Welt bereitgestellt werden. Der Anreiz für die Mühen ist der Ruhm in der Szene, d.h. bekannter zu sein als die Anderen.[669] Deutlich wird hier neben dem Aspekt der Anerkennung der Szenenmitglieder auch eine Verknüpfung zum intellektuellen Wettkampf untereinander.

Dabei sind es nicht nur einzelne Softwarecracker, die für sich im Stillen arbeiten, sondern organisierte Gruppen. Es bestehen ausgefeilte Strukturen, über die neu erschienene Software bezogen werden kann. Die Kontakte reichen über alle Kontinente. Ist das Programm erst einmal gecrackt, erfolgt ein ausgeklügeltes Verteilungssystem für die Software, die so schnell wie möglich alle erreicht.[670] Um die Anerkennung zu steigern, werden vor die gecrackten Versionen selbst entwickelte Demos (Intros) gesetzt. Die Demos sind oft künstlerisch gestaltet und beinhalten zumindest das Pseudonym des Softwarecrackers.[671]

[666] Bekannte Boards sind sind zum Beispiel Ami-Express (/X) oder Fame.
[667] Moschitto/Sen 1999 S. 33.
[668] Moschitto/Sen 1999, S. 34 ff.
[669] Moschitto/Sen 1999, S. 101 ff.
[670] Eckert u.a. 1991, S. 224.
[671] Eckert u.a. 1991, S. 226 f.

3.8.6 Wirtschaftliche Gründe

Pekka Himanen beschreibt wirtschaftliche Motive der Hacker. Dabei sieht er zwischen der traditionellen Hacker-Ideologie und dem Kapitalismus eine Spannung. Grundsätzlich weisen beide Begriffe in unterschiedliche Richtungen.[672] Es handelt sich hierbei um Hacker, die eher eine ethische und philosophische Gesinnung in ihrer Tätigkeit sehen. Dies ist auch die Sichtweise derjenigen, die sich selbst als die wahren Hacker bezeichnen.

Daneben gibt es Hacker, die sagen, dass Hacker zu sein in erster Linie bedeute, den eigenen Interessen zu folgen und frei über seine Zeit verfügen zu können. Sie sehen es als kein Problem an, im Kapitalismus kontinuierlich Geld zu verdienen.[673] In diesem Sinn nennt Himanen Bill Gates als einen der berühmtesten Hacker.[674] Es geht ihm dabei weniger um Hacker, die in Systeme eindringen, sondern eher um den Hackerbegriff im Sinn von Programmieren, um auf diesem Weg die Gesellschaft einen Schritt weiterzubringen. Bill Gates programmierte in seinen Kinderjahren mit Leidenschaft und verbrachte viele Stunden täglich vor dem Computer. Hochachtung erfuhr er zudem, als er seinen Interpreter[675] für die Programmiersprache BASIC programmierte, ohne Zugang zu dem Computer zu haben, für den er bestimmt war. Seine ursprüngliche Absicht war die Entwicklung neuer Programmiersprachen. Im weiteren Verlauf seiner Karriere gewann Profitstreben immer mehr den Vorrang gegenüber den ethischen Interessen.[676] Profitstreben kann ebenfalls ein Motiv für Hacker sein.

Als Beleg dafür, dass Hacker kein moralisches Problem mit dem Profit haben, nennt Boris Gröndahl die zahlreichen Hacker der Gründerzeit, die mittlerweile zu Millionären geworden sind. Die Hacker Steve Jobs und Steven Wozniak haben zum Beispiel mit Anfang Zwanzig Blueboxes entwickelt. Diese Blueboxes wurden in den Anfängen der Computertechnik von sog. Phreakern[677] dazu benutzt, umsonst zu telefonieren. Phreaker gelten im Allgemeinen als Vorläufer der heutigen Hackerkultur. Computerphreaks saßen zum Teil mehr als 4 Stunden täglich vor dem Computer und waren in dieser Zeit hauptsächlich online. Zu dieser Zeit exis-

[672] Himanen 2001, S. 76 ff.
[673] Himanen 2001, S. 78.
[674] Himanen 200,1 S. 79.
[675] Ein Interpreter ist ein Software-Programm, das nicht in Maschinensprache codierte Programme einliest, analysiert, übersetzt und ausführt.
[676] Himanen 2001, S. 79 f.
[677] Die Bezeichnung Phreaker erlangte insbesondere durch den Telefonhacker John T. Draper (Aliasname Captain Crunch) in den späten 60er Jahren Berühmtheit. Es setzt sich aus den Elementen „Phone“ und „Freak“ zusammen. Das erste Element ist an die Angrifftechnik der Phreaker angelehnt, welche zu dieser Zeit vornehmlich im Zusammenhang mit dem Telefonnetz stattfand. Das zweite Element ergibt sich aus dem Begriff Freak, welcher die Bezeichnung für die damaligen Hacker war.

tierten noch keine Flatrates, so dass die Telefonrechnungen immens hoch waren.[678] 1977 bauten und verkauften Steve Jobs und Steven Wozniak einen der ersten Personalcomputer und gründeten im weiteren Verlauf die Firma Apple, mit der sie zu den weltweit führenden Herstellern aufstiegen.[679]

Es ist unklar, inwieweit Spam zu den kriminellen Richtungen von Hackern gehört; klar ist jedoch, dass die unerwünschten E-Mails von Unternehmen kommen, die sich damit einen Gewinn erhoffen. Um an die vielen Adressen zu gelangen, müssen Programmierer spezielle Techniken und Programme nutzen.

Speziell die illegale Seite des Hackens beschreibt Anonymous, indem er das riesige, weltumspannende Computernetzwerk Internet mit dem Wilden Westen im Amerika des 19. Jahrhunderts vergleicht.[680] Vieles ist noch nicht ergründet und viele Ebenen veranlassen Menschen dazu, euphorisch zu werden, wie die New Economy oder der Versuch, alle Lebensbereiche zu digitalisieren, zeigen. Dabei wird eine Bank nicht mehr mit einem Revolver, sondern mit einem Computer ausgeraubt. Deutlich wird dies anhand eines spektakulären Falles, bei dem ein 24-jähriger Hacker aus Russland die Citibank um zehn Millionen Dollar erleichterte. Zur Zeit verbüßt er seine Haftstrafe in den USA.[681] In dieser Goldgräberstimmung gibt es auch Personen, die diese Gelegenheit zu illegalen Betrügereien ausnutzen.[682] Betrugsformen im Online-Banking, Kreditkartenbetrug oder Betrug mit Hilfe von Dialern sind dabei nur die Spitze des Eisbergs. Je mehr geschäftliche Transaktionen digital abgewickelt werden, desto mehr auch Betrügereien gibt es. Geht es um das Beschaffen von Passwörtern, Kreditkartennummern oder um das Installieren von Dialern auf fremden Rechnern, so bedarf es Hackertechniken, um diese Ziele umzusetzen. Sind diese erst einmal herausgefunden, können sie über verschiedenste Wege vertrieben werden. Sind die Passwörter oder Kreditkartennummern auf speziellen Tauschbörsen oder Webseiten zu finden, können auch computertechnisch unversierte Nutzer an diese Daten gelangen und ohne hohen Aufwand Betrügereien begehen. Gerade beim Diebstahl geistigen Eigentums und der Industriespionage haben Hackertechniken einen hohen Stellenwert. Viele Daten und Betriebsgeheimnisse werden mittlerweile digital gespeichert. Früher musste man in die Räumlichkeiten einbrechen, um an Informationen zu gelangen. Heute ereignen sich solche Einbrüche unerkannt über das Internet. Besonders betroffen sind

[678] Zimmermann 1996, S. 69 ff.
[679] Gröndahl 2000, S.22.
[680] Die Idealisierung erscheint wie ein Mythos, mit dem sich einige Hacker umgeben.
[681] Freedman 2000.
[682] Anonymus 2003, S. 232.

hiervon Softwareunternehmen, die ausschließlich digitale Produkte entwickeln.[683] Außerdem sollen mittlerweile über 80 Prozent der Geschäftsgeheimnisse digital gespeichert sein.[684] Experten bezeichnen Netzspionage und computergestützte Spionage gegenwärtig als die größte Gefahr für Unternehmen. Sie stufen dabei Hacker als besonders gefährlich ein, da diese Daten kopieren und manipulieren können, ohne Spuren zu hinterlassen.[685] Jedoch handelt es sich bei der Industriespionage nicht ausschließlich um Hacker, sondern auch um verärgerte Mitarbeiter[686] oder um staatlich subventionierte Wirtschaftsspionage, die speziell aus den USA kommen soll.[687] Aber nicht nur die USA benutzen Hackertechniken, um an Daten zu gelangen. Der Spiegel berichtete im Oktober 2004, dass das kommunistische Nordkorea bis zu 600 IT-Experten als Hacker ausgebildet hat, um gegebenenfalls Computersysteme der USA und Südkorea anzugreifen. Der ehemalige US-Regierungsberater Richard Clarke weist zudem darauf hin, dass auch Länder wie Irak, Iran, China und Russland Hacker für den „Krieg im Internet" ausbilden.[688]

Als „Berufshacker" bezeichnen Denis Moschitto und Evrim Sen Hacker, die versuchen, über ihr Können Aufmerksamkeit bei Unternehmen zu gewinnen, um auf diesem Weg zu einem Job zu gelangen. Speziell in Unternehmen, die sich mit Computersicherheit befassen, sind Hacker oft bessere Fachleute als geschulte und akademische Fachkräfte.[689] Ein berühmtes Beispiel hierfür ist Kim Schmitz (alias Kimble), der in mehrere Telefongesellschaften eindrang. Er knackte Großrechner und fälschte Kreditkarten, spähte Daten aus, manipulierte Computer und machte sich des mehrfachen Betrugs schuldig. Zu seinen Meisterstücken gehörte das Eindringen in den Rechner des Deutschen Beamtenbundes, wo er geheime Dokumente wie die Korrespondenz mit dem Bundeskanzler ausspähte.[690] Kim Schmitz ist 1994 wegen Betrugs mit Millionenschaden zu einer Jugendstrafe von zwei Jahren verurteilt worden. Sein Prozess brachte ihm damals mehr Nutzen als Nachteile.[691] Durch die Publicity erlangte er erstmals auch außerhalb der Hackerszene einen Namen. Kim Schmitz wurde nach Verbüßung seiner Haft Geschäftsführer einer Datensicherheits-Firma mit mehr als 30 Mitar-

[683] Anonymus 2003, S. 233 ff.
[684] Power 2001, S. 198.
[685] Power 2001, S. 198.; dies ergeben u.a. auch Untersuchungen von PricewaterhouseCoopers in Los Angeles.
[686] Power 2001 S. 195.; 216 ff.
[687] Power 2001 S. 204 ff.
[688] http://www.spiegel.de/netzwelt/politik/0,1518,322681,00.html (zuletzt eingesehen am 22.10.04); dieser Hinweis scheint berechtigt zu sein, so soll aber nicht unerwähnt bleiben, dass wohl vermutet werden kann, dass auch westliche Regierungen dem nicht nachstehen werden.
[689] Moschitto/Sen 1999, S. 82 ff.
[690] http://www.onlinekosten.de/news/artikel/6144 (zuletzt eingesehen am 03.10.04).
[691] http://www.heise.de/newsticker/meldung/25048 (zuletzt eingesehen am 03.10.04).

beitern und weltweiten Patenten.[692] Im Mai 2002 verurteilte das Amtsgericht München den Internet-Unternehmer Kim Schmitz wegen verbotenenen Insiderhandels mit Aktien zu einer Bewährungsstrafe von einem Jahr und acht Monaten. Schmitz musste zudem als Bewährungsauflage eine Geldstrafe von 100.000 Euro zahlen.[693] Für Kim Schmitz war der Profit immer der Anlass für den Einsatz seiner Hackertechniken, was in einem mit ihm im April 2003 geführten Interview noch einmal deutlich wurde: „Geld ist ein Werkzeug für mich. Es erlaubt mir Visionen umzusetzen, sowohl im Geschäft als auch privat. Geld macht glücklich, wenn man versteht, es richtig einzusetzen. Ich habe dies stets verstanden."[694] Solche Beispiele zeigen das irritierende Verhältnis der heutigen Unternehmen zu den Hackern. Unternehmen engagieren Hacker, um sich selbst vor unberechtigten Zugriffen in das System zu schützen.
Eine neue Variante dieser Problematik entsteht gerade im Bereich der Virenprogrammierung. Einige Hacker sehen wohl im Virenprogrammieren den Vorläufer einer möglichen Karriere. In neueren Virenversionen werden Bewerbungen mit in den Quellcode integriert.[695] Verbreitet sich ein Virus gut, so soll dies wohl als Qualifikationsnachweis gelten.

Boris Gröndahl nennt als weiteren wirtschaftlichen Aspekt Armut als einen Grund, illegal zu hacken. Während in der westlichen Welt Programmierer gut bezahlt werden, sieht es speziell in Russland ganz anders aus. Viele russische Computerfachleute verdienen sich aus der Notwendigkeit heraus auf dem ausufernden russischen Schwarzmarkt mit Softwarepiraterie ihr Geld.[696] Somit können vielleicht einige Hacker als die Obdachlosen oder Verarmten der Zukunft bezeichnet werden, die nicht mehr in Kaufhäuser gehen um zu stehlen, sondern einen Computer nutzen, um von zu Hause weltweit ihre Existenz zu sichern.

3.8.7 Schadensabsicht und Rache

Die Absicht, anderen Schaden zuzufügen, ist nach Eckert u.a. ebenfalls ein reales Motiv. Sie beziehen sich hierbei hauptsächlich auf sog. Crasher. Der Begriff Crasher kann mit dem Begriff Cracker verglichen werden. Der Begriff wird von den Autoren aber deshalb benutzt, weil durch den Bezug auf das englische Wort „Crash", also Absturz oder Unfall, gezeigt werden kann, dass diese Personen gezielt Schäden verursachen. So geht es ihnen nicht allein um das

[692] http://www.onlinekosten.de/news/artikel/6144 (zuletzt eingesehen am 03.10.04).
[693] http://www.123recht.net/article.asp?a=2916&f=nachrichten_neue~urteile_kimschmitzprozess&p=1 (zuletzt eingesehen am 03.10.04).
[694] http://www.planet-interview.de/interviews/pi.php?interview=schmitz-kim (zuletzt eingesehen am 03.10.04).
[695] http://www.sec-world.net/news/67433-sasser-der-wahre-gewinner-im.html (zuletzt eingesehen am 03.10.04).
[696] Gröndahl 2000, S.22.

Eindringen in Systeme, um darin herumzustöbern oder Daten auszuspähen und gegebenenfalls weiterzugeben. Ausschließliches Ziel ist es, Daten und Systeme zu zerstören.[697] Um dies zu verdeutlichen, zitieren die Autoren Passagen aus Interviews:

„Wolfgang, 23 Jahre, Crasher
‚Ich bin schon regelmäßig am Crashen. Das sind eigentlich kleine Spielereien. Aber wenn z.B. die Chemiefirma XY zum xten Male den Rhein versaut, dann werde ich – vorausgesetzt ich finde einen Zugang – denen sämtliche Daten auf ein paar Rechnern löschen und schreibe ihnen eine Meldung in der Form: Das war das letzte Mal Jungs, ansonsten lege ich Euch ALLE Rechner flach.'

Ben 24 Jahre, Crasher
‚Daten werden gecrasht aus den gleichen Gründen, wie Menschen umgebracht werden: Aus Rache oder einfach weil man nicht gut ´drauf´ ist. Wenn ich z.B. den ganzen Tag über Ärger gehabt habe, dann nehme ich mir schon mal einen Rechner vor. (...) Ich glaube, das ist wohl so ähnlich wie bei den Fußballfans. Es ist einfach nur Randale und Abreagieren. (...) Manchmal ist da auch das Gefühl des absoluten Triumphes dabei. (...) Einen echten Sinn hat das ganze nicht, wieso auch (...).'"

Die persönliche Frustration scheint ein mögliches Motiv für Hacker zu sein. Es scheint, als ob das Zerstören von fremden Daten oder das Zum-Absturz-Bringen fremder Rechner oder ganzer Netzwerke als Kanalisierungsfunktion für persönliche Spannungen dient. Vergleichbar mit dem Abreagieren von Aggressionen, wenn jemand auf einer anderen Ebene frustriert wurde und es nicht gelernt hat, diese Gefühle anders zu kompensieren. Aus diesem Grund vergleichen die Autoren 1991 Crasher mit Streetgangs oder Hooligans.[698] Sie plädieren deshalb dafür, Crasher deutlich von Hackern zu unterscheiden und die Begriffe deshalb auch nicht zu verwechseln.[699] Andererseits übersehen die Autoren eine an sich nicht mögliche Unterscheidung zwischen Hackern und Crashern. Zu den Crashern sagen sie selbst, dass sie genauso wie Hacker in Systeme eindringen, nur noch einen Schritt weitergehen und dem System bewusst Schaden zufügen.[700] Dabei scheint schon der Begriff „Schaden" problematisch. Ist es ein Schaden, wenn Webseiten manipuliert werden, wenn andere Inhalte, evtl. politische, dar-

[697] http://www.elektroniknet.de/elex/show.php?k=c&id=11706 (zuletzt eingesehen am 04.10.04).
[698] Eckert u.a. 1991, S. 186 f.
[699] Eckert u.a. 1991, S. 187.
[700] Eckert u.a. 1991, S. 185.

auf abgebildet werden, die problemlos vom Administrator wieder beseitigt werden können? Oder entsteht ein Schaden erst, wenn sämtliche Daten vernichtet wurden? Daneben gehen die Autoren davon aus, dass es Hacker gibt, die in Systeme eindringen und niemals Daten zerstören werden und Crasher, die sich darauf spezialisiert haben, Daten zu zerstören. Eine solche Zweiteilung scheint recht naiv und geht von einem Hackerbild aus, bei dem diese nur idealistisch und moralisch unverwerflich handeln. Wie bereits an anderen Stellen gezeigt, verschwimmen aber diese Bereiche; was dem einen legitim erscheint, ist für einen anderen Hacker schon kriminell. Viele Cracker nennen sich Hacker, aber wer hat das Recht für sich gepachtet, dies Selbstbild den anderen abzusprechen? Crasher sind meines Erachtens nichts anderes als Hacker, oder wohl besser Cracker, die bei Gelegenheit und spezieller Motivation, sei es durch Frustration, Ärger oder aus politischen Motiven, ihr Talent ausnutzen. Um diesem Gefühl Ausdruck zu geben, zerstören sie Daten. Dieses Problem wird wohl auch von den Autoren erkannt, weswegen sie Crasher als abtrünnige Hacker bezeichnen.[701] Aber ist jemand, der einmal gestohlen, hat für immer ein Dieb oder ist jemand, der eine Sache mal zerstört hat, immer ein Vandale?

Speziell das Motiv Rache wird von Frank Hartmann[702] als wichtiger Beweggrund genannt. Er stellt hierfür ein Beispiel aus den USA vor: Timothy Allen Lloyd war bei Omega Engineering als Administrator für die Computersicherheit beschäftigt. Nach Ansicht des Arbeitgebers war er nicht bereit, die ihm unterstellten Mitarbeiter hinreichend weiterzubilden, weshalb er seine Führungsposition verlor. Aus Rache setzte er ein Programm in das Computersystem, das alle Programme lahm legte, die zur Fertigung benötigt wurden. Mit der Sabotage-Software löschte Lloyd alle wichtigen Programme samt Sicherheitskopien. Erst Monate nach dem Racheakt ermittelte ein auf Datenrettung spezialisiertes Unternehmen den Grund für das Verschwinden der Programme. Bei einer Hausdurchsuchung in Lloyds Wohnung wurden schließlich Kopien der gelöschten Programme gefunden.[703]

---

[701] Ebd.

[702] Frank Hartmann arbeitet als freier Journalist und Medientrainer für die Publikums- und Fachpresse. Er recherchiert seit Jahren auf den Gebieten der Wirtschaftsspionage und der Computerkriminalität, kennt Behörden, Betroffene und Hacker. Er gibt einen detaillierten Einblick in die Gefährdungspotenziale und die Geschäftsrisiken durch Datenspionage und Computermissbrauch. Das Buch bietet dem Leser Anregungen und führt ihm die Tragweite der Problematik von Online-Kriminalität vor Augen. Trotz zeitlicher Bezüge zwischen einzelnen Vorfällen beschäftigt er sich vor allem mit grundsätzlichen Risiken durch Computer- und Internetkriminalität und ihren Auswirkungen auf Staat, Wirtschaft und Gesellschaft, wobei der Autor immer wieder darauf hinweist, dass die Problematik entweder unterschätzt oder falsch behandelt wird. Gerade die enthaltenen Interviews sowie zahlreiche Informationen und Zitate sind exklusiv und können für die vorliegende Arbeit bereichernd wirken. Andere Informationen beruhen auf Quellen wie Büchern, Zeitschriften und Zeitungen, Redemanuskripten, Pressemitteilungen und Online-Medien im World Wide Web.

[703] Hartmann 2001, S. 96 ff.

Ryan Russel und Stace Cunningham berichten im Zusammenhang mit dem Motiv Rache, dass sich in speziellen Foren Hacker tummeln, die Hilfegesuche an andere, zumeist bessere Hacker richten, die ihnen helfen sollen, Angriffe auf Dritte zu führen. Zumeist fühlt sich der Bittsteller ungerecht behandelt und will sich rächen.[704] In einigen Fällen bezieht sich der Racheakt gegen einen ehemaligen Freund oder eine ehemalige Freundin. Dabei werden vielseitige Racheakte besprochen, die von Passwortklau bis zur Fälschung der Führerscheindaten des Opfers gehen. Nach Aussage der Autoren enden erfreulicherweise die meisten solcher Hilfegesuche darin, dass die übrigen Hacker sie darauf hinweisen, dass sie selber die Techniken erlernen sollen.[705]

Einen Fall der Rache beschreiben Armin Medosch und Janko Röttkers.[706] Der Computerfachmann Steve Gibson versuchte vergeblich, DDoS-Attacken auf den Firmenserver zu unterbinden, die von über 400 weltweit verstreuten Windows-PCs ausgingen und die vermutlich von ein und derselben Person veranlasst wurden. Um den Hacker aufzufinden, bediente sich Gibson, der selbst ein Hacker war, seiner alten Kenntnisse, um an diese Person zu gelangen. Er führte Ermittlungen im Netz-Underground durch und stieß auf einen 13-jährigen Jugendlichen mit dem Nicknamen „Wicked“, der sich als Urheber dieser Attacken bekannte. Von ihm erfuhr er, dass Wicked zu Ohren gekommen war, dass Steve Gibson ihn als Script-Kiddie betitelt hatte. Dieser überflutete wegen dieser Aussage Gibsons Firmenserver. Erst als Steve Gibson seine Niederlage eingestand und ihm gesagt hatte, dass er ihn nie als Script-Kiddie bezeichnet habe, beendete Wicked die Rache-Attacken.[707]

3.8.8 Sucht

Die Sucht nach dem Computer und dem Hacken soll ebenfalls einen Grund für kriminelle Handlungen darstellen. Dabei steht die Sucht im engen Zusammenhang mit dem Begehren seitens der Hacker einen wiederkehrenden „Kick“ oder „Thrill“ zu erleben. Dieser Kick resul-

[704] Russel/Cunningham 2001, S. 52 ff.
[705] Russel/Cunningham 2001, S. 53.
[706] Armin Medosch ist Mitbegründer und Redakteur des Online-Magazins Telepolis und lebt in London. Janko Röttgers lebt und arbeitet als freier Journalist und Autor in Berlin. Das Buch ist unterteilt in verschiedene Sektionen und versucht anhand einer Sammlung von sehr gut recherchierten Artikeln eine möglichst objektive Betrachtung der Geschehnisse zu liefern. Dabei versuchen die Autoren mehr auf gesellschaftliche als auf computertechnische Aspekte einzugehen. Zudem liegt der Gehalt dieses Buches darin, dass nicht übertrieben wird, Vorurteile aufgedeckt und meist die Sicht beider Seiten, Hacker und Polizei, dargestellt werden.
[707] Medosch/Röttgers 2001, S. 122.

tiert dabei unter anderem aus dem Gefühl Verbotenes zu tun. Paul A. Taylor zitiert hierfür einige Aussagen:

"Jean-Bernard Condat, President of the French Computer Chaos Club:
'All the hackers that I know in France, have (or have had) serious problems with their parents. Some speak only by Computer or only the Computer matters. Hacking for a real hacker is the only reason to live! Without background ideas. Like drinking water for a human body. The lack of Computers/Software to hack makes the hacker ill at ease.'"[708]
"Interview mit einem Hacker:
'I just do it because it makes me feel good, as in better than anything that I've ever experienced. Computers are the only thing that have given me this feeling ... the adrenaline rush I get when I'm trying to be authority, the thrill I get from having written a program that does something that was supposed to be impossible to do, and the ability to have socialtions with other hackers are all very addictive. I get depressed when away from a networked Computer for too long. I find conversations in the Cyberspace much more meaningful and enjoyable than conversing people in physical-reality real mode. For a long time, I was extremely around others, and I am able to let my thoughts run free when I am alone with my Computer and a modem hooked up to it. I consider myself addicted to hacking. If I were ever in a position where I knew my Computer activity was over with for the rest of my life, I would suffer withdrawal.'"

Es erscheint erstaunlich, dass der Präsident des französischen CCC von sehr vielen gestörten Familienverhältnissen ausgeht. Fehlt diesen Hackern Zuneigung, Sicherheit oder andere Gefühle, die sie dadurch kompensieren, dass sie exzessiv hacken? Es gibt ihnen ein gutes Gefühl, vielleicht ein Gefühl geliebt zu werden auf ihre Weise. Es fragt sich zudem, ob eine gestörte Kommunikationsfähigkeit bei diesen Hackern vorliegt, wenn sie Onlinekommunikation der realen vorziehen. Fehlt ihnen das nötige Selbstbewusstsein, einem Menschen gegenüberzutreten, um mit ihm zu sprechen? Die Sucht scheint verbunden zu sein mit der Sucht nach dem Kick und dem Adrenalinstoß.

Thomas Barth spricht das Thema Computersucht ebenfalls an und spricht hierbei von einer Pathologisierung der Computerfreaks, womit nicht nur Hacker gemeint sind, sondern alle ex-

[708] Taylor 2001, S. 47.

zessiven Computernutzer.[709] Er zitiert hierfür einem Zeitungsartikel der Tageszeitung Die Welt: „Immer mehr Kinder werden computersüchtig. In Großbritannien schätzen Pädagogen und Erziehungsberater, dass schon jedes zehnte Kind ein ´Computer-Junkie´ ist. Die Folgen für Psyche und Entwicklung der Kinder sind schwerwiegend. Sie ziehen sich immer mehr aus dem alltäglichen Leben zurück und verlieren den Bezug zur Wirklichkeit; vernachlässigen Freunde und Schule, werden völlig egozentrische Außenseiter. Im Extremfall haben die jungen Technikfans nur noch einen Freund: den Computer.“[710]

Dabei lehnt er die Erkenntnisse Joseph Weizenbaums über das „zwanghafte Programmieren“ ab, wonach es zwei Arten gibt. Die eine Art des Programmierens liegt im strukturierten Erarbeiten von Lösungen und darin, die Lösungswege zu dokumentieren, um diese Erfahrungen bei zukünftigen Problemen nützlich verwerten zu können. Die andere Art des Programmierens ist aus Sicht Joseph Weizenbaums die unstrukturierte Vorgehensweise seitens der Hacker. Seiner Ansicht nach probieren Hacker auf gut Glück einfach alles aus, bis es klappt.

Die Soziologin Sherry Turkle dagegen spricht von „sanften und harten“ Programmierstilen. Der sanfte Programmierstil soll der Tätigkeit eines Künstlers ähneln, der harte ist dagegen ein Mittel zur Kontrolle.[711] Beide gelangen trotzdem zu ähnlichen Profilen. Schwerpunkt ist die Beherrschung der Maschine und das Bedürfnis nach Perfektion. Individualismus und Unsinnlichkeit sollen prägende Eigenschaften der Hackerkultur sein. Der Computer soll zudem einen „schizoiden Kompromiss“ zwischen Einsamkeit und der Angst vor Nähe bieten.[712] Thomas Barth setzt sich mit diesen Ansätzen soziologisch wie auch philosophisch auseinander und vergleicht vor allem die Macht, die in der Verschaffung von Informationen liegt, mit Foucault’s Machtausübung im Bereich der Sexualität.[713] Thomas Barth bezieht sich bei diesen Diskussionen auf ältere Studien von Joseph Weizenbaum und Sherry Turkle. Da diese Studien aus den Jahren 1976 und 1984 stammen und auf den Erkenntnissen über die Anfänge der Computertechnologie beruhen, scheint es zweifelhaft, ob die damals gewonnenen Erkenntnisse den heutigen Strukturen der Hackerszene gerecht werden. Die Hackerszene ist nicht nur gewachsen, es sind zusätzlich gänzlich neue Szenen hinzugetreten. Trotzdem sollte an dieser Stelle auf die Darstellung der damals gewonnenen Erkenntnisse nicht verzichtet werden.

[709] Barth 1997, S. 168 ff.
[710] Die Welt vom 17.01.1990.
[711] Barth 1997, S.171.
[712] Barth 1997, S. 172.
[713] Barth 1997, S. 174.

3.9 Aktuelle empirische Studien

Es werden im Folgenden nur noch Studien vorgestellt, die nach dem Jahre 1997 veröffentlicht wurden. Alle älteren Studien sind bereits in den vorhergehenden Teil eingeflossen. Nur bei den neueren Studien ist es noch interessant, weiterführend zu beschreiben, wie hierbei vorgegangen wurde, welche Fehlerquellen existieren und welche Ergebnisse bezüglich der heutigen Szene zu nennen sind.

3.9.1 „Where have all the Hackers gone?" von Tom Mulhall

Tom Mulhall hat im Jahr 1997 eine Studie mit dem Titel „Where have all the Hackers gone?" veröffentlicht. Auch wenn sie durch die heutige rasante Entwicklung der Computertechnik und der damit sich schnell wandelnden Hackerszene ein wenig veraltet ist, so hat sie trotzdem erstaunliche Erkenntnisse hervorgebracht, sodass sie an dieser Stelle vorgestellt wird.

Mit der Studie werden mehrere Fragestellungen behandelt. Zum einen geht es darum, ob die Bedrohung durch Hacker eine reale Gefährdung darstellt. Sind Hacker auf andere computergestützte Kommunikationssysteme ausgewichen? Welche Motive leiten sie? Welchen Einfluss haben die Gesetze auf ihr Verhalten? Und welches Verhalten ist notwendig, um Hacker von ihren Tätigkeiten abzuhalten?

Die Studie ist das Ergebnis einer 10 Jahre dauernden Beobachtung der kriminellen Vorfälle, die mit Hackern zusammenhängen. Der Begriff Hacker wird dabei im folgenden Sinn gebraucht: Hacker sind alle Personen, die enthusiastisch mit der Computertechnologie umgehen, welche den Zugriff auf fremde Systeme beinhaltet. Unter Computerkriminalität versteht der Autor wiederum alle Taten, die in irgendeiner Weise mit dem Computer zu tun haben.

Der Autor hat für die Ergebnisse dieser Studie unterschiedliche Wege beschritten. Zum einen hat er viele Zeitungsartikel der vergangenen Jahr ausgewertet. Daneben recherchierte er auch im WWW und führte Telefoninterviews durch. Zusätzlich wertete er auch Gutachten und Umfragen von Instituten aus, die sich mit Computersicherheit beschäftigen, um festzustellen, ob und inwieweit Hacker eine Bedrohung darstellen. Zudem bezieht er eine im Jahr 1996 veröffentlichte englische Studie ein.

Der Autor weist darauf hin, dass solche Ergebnisse wichtig seien, um kriminelle Trends im Bereich der Computertechnik erkennen zu können. Bei seiner Recherche stieß er auf eine Fülle von Informationen zu Hackern. Es erschien sehr schwer, hieraus geeignetes Material herauszufiltern. Dabei handelte es sich zumeist um Berichte und Forschungsergebnisse, die sich mit Systemsicherheit beschäftigen und somit rein technisch orientiert sind. Diese Problematik kann in dieser Arbeit bestätigt werden, da es z.B. unzählige Zeitungsartikel zu Hackern gibt, diese jedoch meist ihre Techniken darstellen. Wenn es nicht um den technischen Inhalt geht, dann handeln die Berichte zumeist von der Gefährlichkeit der Hacker. Empirische Studien, die sich mit Motivationslagen und der Szene beschäftigen, sind nur sehr selten und zumeist veraltet.

Zunächst weist Mulhall darauf hin, dass Computerkriminalität durch Hacker nach seinen Forschungserkenntnissen eine reale Bedrohung darstellt. Die Bedrohung ergibt sich aus den Motiven seitens der Hacker. Auch wenn die Motive aus Sicht der Hacker als ehrenwert angesehen werden, verursachen sie denoch enorme wirtschaftliche Schäden. Der Wert der Studie liegt hierbei in den umfangreichen Erkenntnissen zu den Motivationslagen der Hacker. Dabei bewertet er zunächst Aussagen von Hackern selbst. Auch wenn die Artikel aus den Jahren 1988 und 1995 stammen und somit bereits veraltet sind, besitzen sie trotzdem eine gewisse Aussagekraft, die auch die heutige Motivationslage von Hackern beschreiben dürfte. Wissensdrang und computertechnisches Wissen stehen seines Erachtens im Vordergrund. Damit zusammenhängend sieht Mulhall die Tendenz, durch das eigene Wissen Machtgefühle gegenüber der Technik ausdrücken zu wollen. Daneben sieht er auch den Profilierungsdrang gegenüber den anderen Hackern und das Demonstrieren der eigenen Fähigkeiten als einen weiteren wichtigen Beweggrund.

Des Weiteren stellt der Autor im Bereich der Motive eine englische Studie vor, die zwischen Januar 1995 und April 1996 und im Auftrag der englischen Regierung erarbeitet wurde. Dabei wurden 32 verhaftete Hacker interviewt, von denen 16 Studenten, 11 Arbeitslose und 5 Angestellte waren. Der Altersdurchschnitt lag bei 21 jahren, wobei der Jüngste 14 und der Älteste 35 Jahre alt war. Unter den Hackern befand sich nur eine Frau. 13 Personen (41 Prozent) haben als Beweggrund angegeben, kostenlos telefonieren oder ins Netz gelangen zu wollen. 4 Personen (13 Prozent) wollten das „Voicemail System“ manipulieren und auf diesem Wege Nachrichten für Freunde und Bekannte hinterlassen. Sie sagten aus, sie hätten keine bösen Absichten verfolgt. 54 Prozent wollten auf keinen Fall Schaden verursachen. 5 Hacker (33

Prozent) wollten mit den Hacks Geld verdienen, indem sie bestimmte zahlungspflichtige Vorwahlnummern manipulierten. 2 (13 Prozent) waren im Bereich der Softwarepiraterie involviert. 2 (13 Prozent) waren am Identitätsdiebstahl im Bereich der Kreditkarten interessiert.

Nach den Erkenntnissen der Forschungsarbeit sind Hacker sehr jung und fast ausschließlich männlich. Einen großen Stellenwert sehe ich in dem Nachweis, dass Hacker sich nicht nur in einem einzigen Bereich betätigten, sondern dass die Übergänge zwischen den verschiedensten technischen und kriminellen Möglichkeiten teilweise fließend waren. So wollten einige Hacker nur kostenlos telefonieren, andere waren im Bereich der Softwarepiraterie oder des Identitätsdiebstahls tätig.
Eine Erklärung, für den hohen Reiz des Freitelefonierens, liegt nach Ansicht des Autors darin, dass viele Hacker Studenten waren oder es ihnen einfach an finanziellen Mitteln mangelte. Außerdem stellt der Autor fest, dass einige Hacker es nicht für möglich hielten, aufgespürt zu werden, da sie glaubten, auf sehr geschickte Weise ihre Identität zu verschleiern. Vielen Hackern war anscheinend nicht klar, dass das Aufspüren allein davon abhängt, welchen Aufwand die Strafverfolgungsbehörden zu betreiben bereit sind, es aber grundsätzlich immer möglich ist.

Nachteilig an dieser Studie erscheint jedoch die Fragestellung, ob eine Bedrohung durch die Hacker überhaupt real sei. Dies wird heute weder von Privatpersonen noch von Unternehmen oder staatlichen Einrichtungen bezweifelt. Unternehmen entstehen hohe Kosten durch den Einsatz von Sicherheitsvorkehrungen, mit denen das Hacking unterbunden werden soll. Auch die europäische Diskussion um strafrechtliche Einführungen von Straftatbeständen zeigen, dass ein gewisses Verständnis hierfür gegeben ist. Gestritten wird vielmehr über die Art der Bedrohung und ob nicht alle Lebensbereiche zu gering gesichert sind oder ob diese ausreichend geschützt sind. Denselben Hinweis zeigt die zweite Fragestellung, ob Hacker sich auf andere computerbasierte Systeme spezialisiert haben. Diese Frage erübrigt sich heutzutage teilweise, da z.B. Organizer oder Mobiltelefone mittlerweile ebenso von Viren betroffen sind. Es stellt sich somit heute ausschließlich die Frage, ob ein bestimmter Bereich computertechnisch so fortgeschritten ist, dass er dem modernen Standard genügt. Ist dies der Fall, sind unproblematisch alle bisherigen Hackertechniken auch in diesem Bereich möglich.[714]

[714] Auch die immer wiederkehrende Beschäftigung des Autors mit dem Blueboxing zeigt das Alter dieser Untersuchung, da Blueboxing am Anfang der Hackergeschichte stand und mittlerweile bei eingesessenen Hackern eher Nostalgiegefühle weckt. Somit ist zumindest die Erkenntnis im Bereich der Motivationslagen von Hackern, dass diese gratis telefonieren wollen, veraltet. Jedoch können diese Beweggründe auf das heutige Surfverhalten

Es erscheint, als ob der Autor wegen der Schwierigkeit einer Begriffsdefinition einfach eine allgemeine für fast alle Computerbesitzer zutreffende Definition gewählt hat. Diese Schwäche der Studie zeigt sich ebenso in der Definition des Begriffs Computerkriminalität, die ebenfalls alle Handlungen beinhaltet, die in irgendeiner Weise mit dem Computer zu tun haben. Diese Definitionen sind jedoch aufgrund ihrer uferlosen Weite nicht zufrieden stellend.
Zudem zeigt die Studie, dass der Autor von einer Hackerszene ausgegangen ist, die mehr oder weniger die Jüngeren betrifft. Auf Geheimdienste, Terroristen, professionelle Wirtschaftshacker usw. geht der Autor nicht ein. Er orientiert sich nur an der typischen (u.a. von den Medien generierten) Hackerszene, die mit den Netzwerkhackern meist gemeint ist. Das Feld der Hacker ist jedoch weiter und vielfältiger.

3.9.2 „Hacker Survey" der Boston Consulting Group (BCG)

Die Boston Consulting Group (BCG) in Kooperation mit Open Source Developer Network (OSDN) veröffentlichte im Juli 2004 eine Studie über die Hackerszene mit dem Titel „Hacker Survey".[715] Die BCG ist eine seit 1963 weltweit operierende Consultingfirma, die Unternehmen im Bereich des Managements berät. Sie arbeitet hierbei mit mittlerweile über 2.800 Konsulten mit 53 Sitzen weltweit. BCG führte diese Studie an ausgewählten bei SourceForge[716] registrierten Entwicklern durch. SourceForge ist die größte Sammlung von Open-Source-Codes, Open-Source-Applikationen und Open-Source-Projekten weltweit. Dabei geht es SourceForge u.a. um Projektbetreuung, Versionskontrollen, Fehlerbehebungen oder die Verwaltung von Mailinglisten. Es werden über 450.000 registrierte Nutzer sowie über 43.000 Projekte betreut.[717] Dabei handelt es sich nicht ausschließlich um freiwillige Mitarbeiter, sondern auch um bezahlte Open Source Entwickler.[718]

Ziel der Studie war es, die Motivation von Hackern näher zu ergründen. Dabei ging es in dieser Studie um Open-Source-Entwickler, die von den Autoren als essenzieller Bestandteil der Hacker-Kultur gesehen werden.[719] Hier wird der Begriff Hacker im ursprünglichen Sinn verwendet, also als Bezeichnung für einen talentierten Programmierer. Nicht alle Programmierer

---

von Hackern übertragen werden. Die Parallele zum früheren Blueboxing ist das heutige kostenlose Surfen im Internet (besser: das Surfen auf Kosten fremder Personen).
[715] Einzusehen unter http://www.osdn.com/bcg/bcg/bcghackersurvey.html.
[716] Zu finden unter http://sourceforge.net/index.php.
[717] Nach eigenen Angaben kommen pro Tag ca. 700 neue Nutzer und ca. 60 neue Projekt hinzu.
[718] Fehlt bei bestimmten Projekten computertechnisches Fachwissen, so werden Programmierer engagiert.
[719] Kennzeichnend ist im Open-Source-Bereich vor allem, dass der Quellcode für alle offen ist.

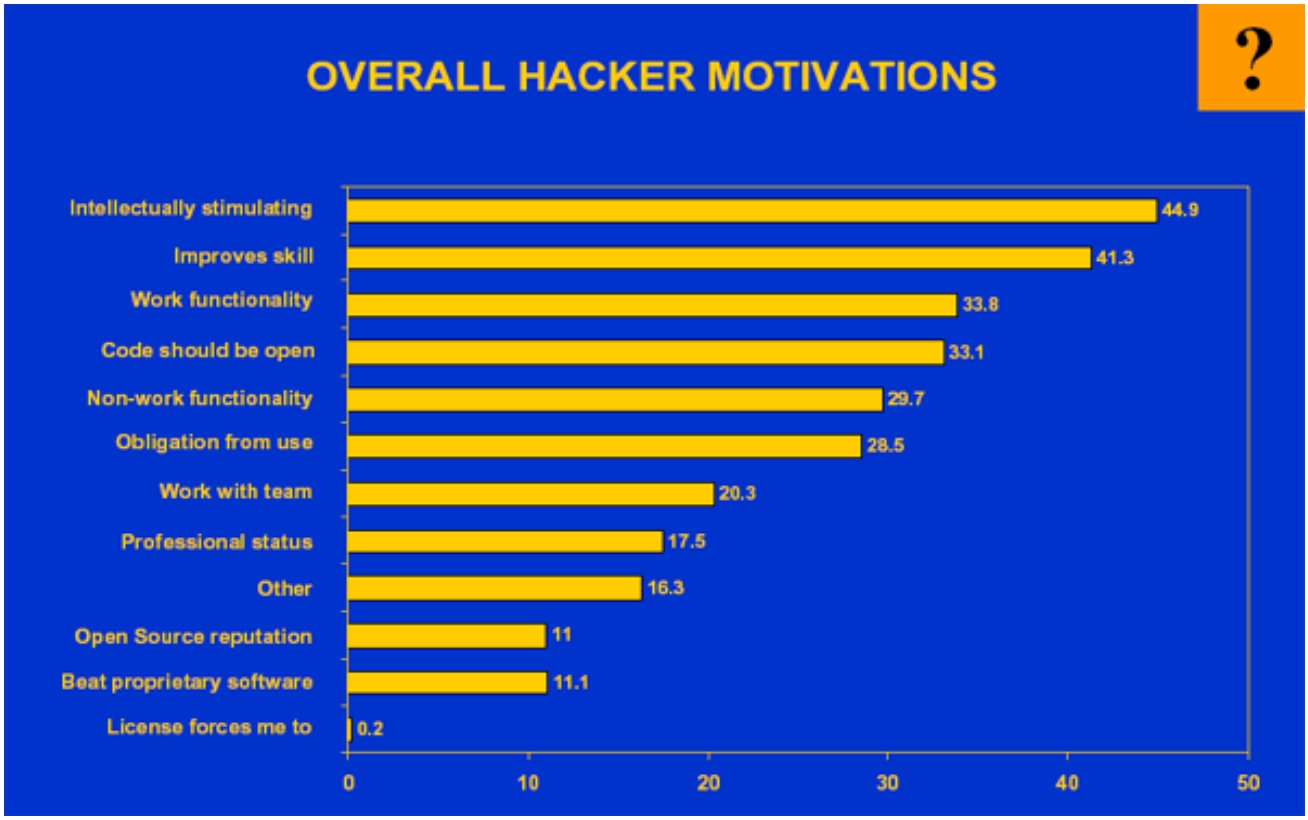
haben kriminelle Absichten, so dass die Studie vor allem auf allgemeine Motivationslagen abzielte. Der Unterschied zu Personen, die bösartige Software programmieren oder Zugang zu Rechnern verschaffen und die korrekt als Cracker bezeichnet werden, wird in dieser Studie ebenfalls herausgestellt. Es werden also Motive von Hackern aufgezeigt, die sich selbst oft als die „echten Hacker“ oder „White Hacker“ betiteln. Auch wenn die Studie nicht direkt kriminelle Handlungen von Hackern analysierte, so können die Erkenntnisse über allgemeine Motive auch für diese Arbeit von Nutzen sein, da gerade diese Gruppierung häufig als Hacker bezeichnet wird[720] und die Übergänge zu kriminellen Hackern oft fließend sind. Zudem sollen auch die Motive derer, die sich als die eigentlichen Hacker sehen und somit zu einer Darstellung einer nichtkriminell ausgestalteten Hackerszene beitragen möchten, nicht unerwähnt bleiben.

Für die Untersuchung wurden 684 Entwicklern per E-Mail ein Fragebogen zugesandt. Die E-Mail-Anfragen wurden in zwei große Personengruppen geteilt: Zum einen wurden Entwickler aus Alpha- und Betabereichen[721] befragt und zum anderen Entwickler, die an Projekten arbeiten, die unmittelbar vor der Veröffentlichung stehen.

Dabei betrachteten 61,7 Prozent das Projekt, an dem sie arbeiten, als die kreativste Tätigkeit, die sie bislang in ihrem Leben geleistet hätten. 48,4 Prozent verglichen ihre Arbeit mit Poesie oder Musik. 72,6 Prozent sagten, sie verlören beim Programmieren ihr Zeitgefühl.

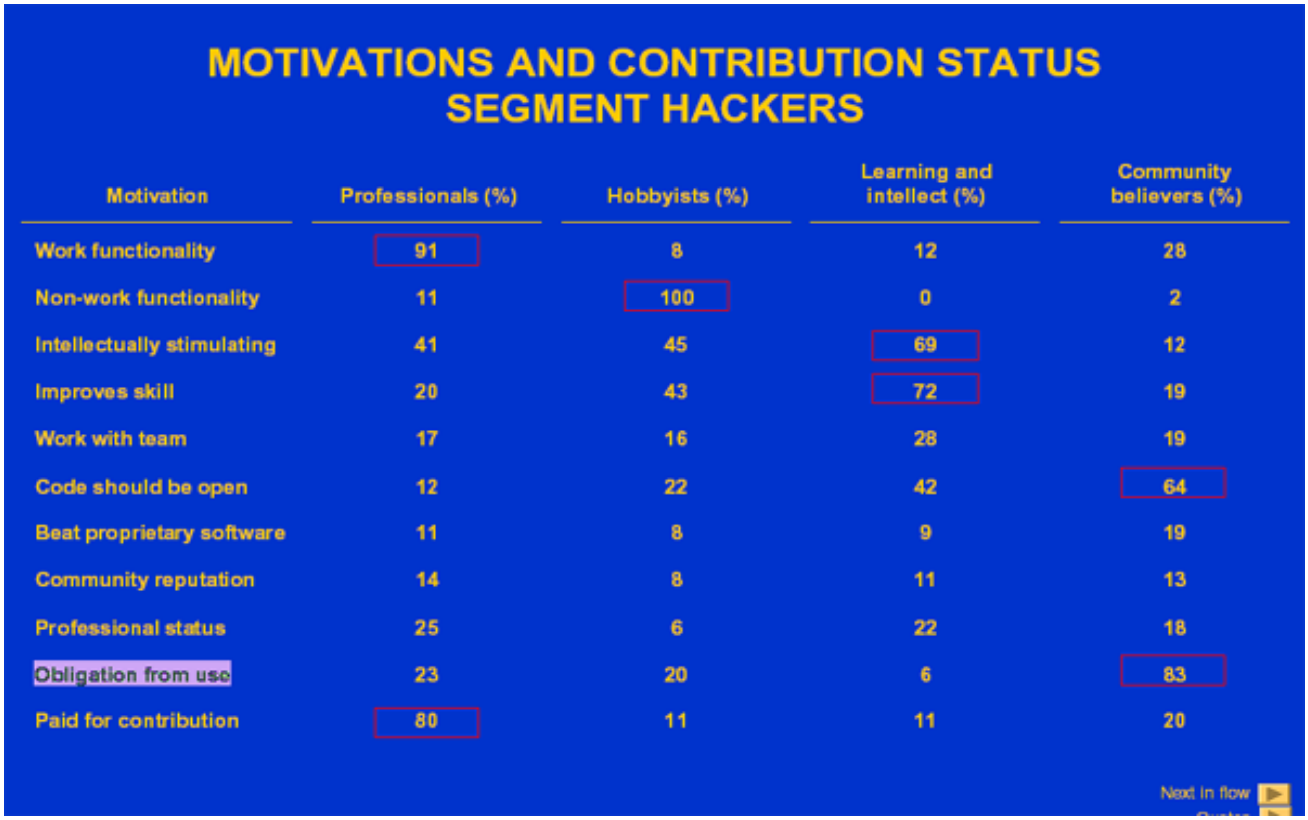
[720] Siehe hierzu vor allem das Buch „The Cathedral & the Bazaar“ von Eric Raymond mit seinen ausführlichen Darstellungen über die Open Source Gemeinde im Hinblick auf den Begriff Hackerszene.
[721] Dabei handelt es sich um noch unfertige Software und um Software, die als Beta-Version zum Testen und zur Fehlerbehebung verteilt wird.

Gesamtdarstellung von Hackerbeweggründen



Die Graphik zeigt, dass 44,9 Prozent der Hacker die intellektuelle Stimulation als wichtigsten Grund für ihr Vorgehen sehen. In einer ähnlichen Kategorie kann hier wohl auch die Verbesserung der Fähigkeiten gesehen werden, die mit 41,3 Prozent an zweiter Stelle steht. An vierter Stelle steht mit 33,1 Prozent der Beweggrund, dass der Programmcode frei sein soll. Das heißt, nur etwa ein Drittel der Open-Source-Mitglieder programmieren mit der Absicht, den Code allen anderen Menschen frei zugänglich zu machen. Dies erscheint deshalb erstaunlich, da viele Autoren diesen Grund nennen, wenn es um Open-Source-Projekte geht. Es scheint hier aber, als ob persönlicher Eifer und Spaß an der Arbeit mehr im Vordergrund stehen. Dies wird auch dadurch deutlich, dass nur 11,1 Prozent der Hacker ihre Motivation darin begründet sehen, sich der rechtlich geschützten Software zu erwehren. Es scheint also, dass der Kampf der Open-Source-Gemeinde gegen die private Wirtschaft nicht so wichtig ist, wie immer dargestellt wird. Ebenfalls gering mit nur 11 Prozent erscheint der Drang nach Anerkennung.

Motivations- und Wirkungsbereich von Hackern



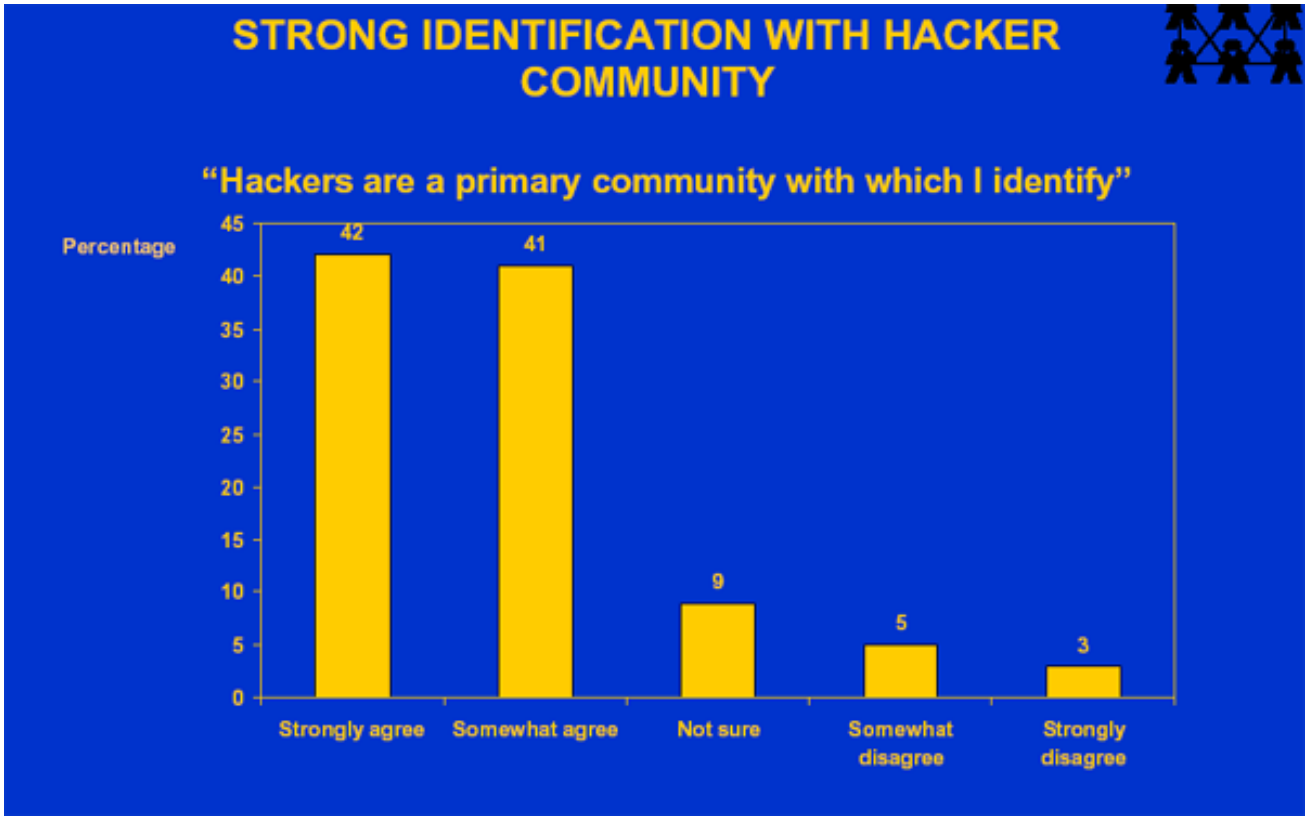
MOTIVATIONS AND CONTRIBUTION STATUS
SEGMENT HACKERS

Motivation	Professionals (%)	Hobbyists (%)	Learning and intellect (%)	Community believers (%)
Work functionality	91	8	12	28
Non-work functionality	11	100	0	2
Intellectually stimulating	41	45	69	12
Improves skill	20	43	72	19
Work with team	17	16	28	19
Code should be open	12	22	42	64
Beat proprietary software	11	8	9	19
Community reputation	14	8	11	13
Professional status	25	6	22	18
Obligation from use	23	20	6	83
Paid for contribution	80	11	11	20

Next in flow

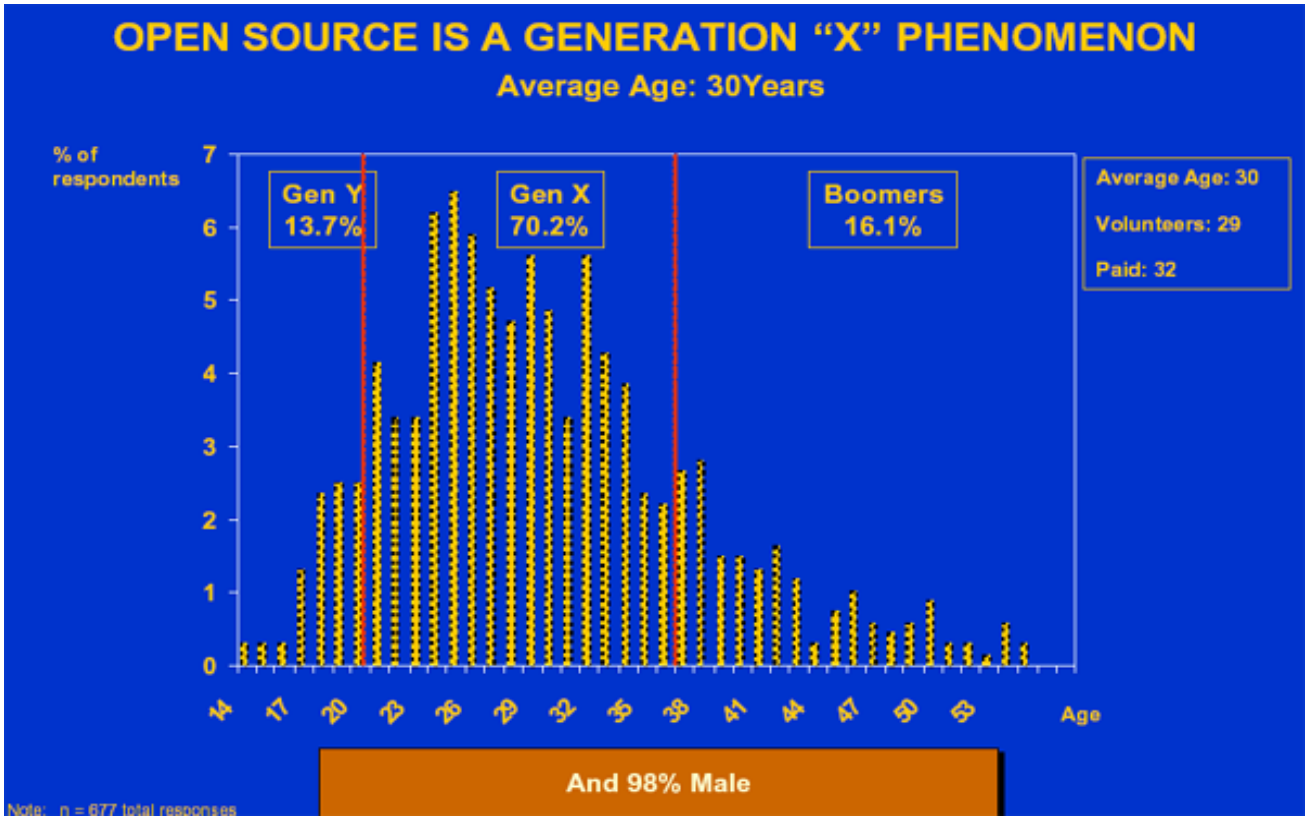
Die Autoren der Studie teilten Programmierer in vier unterschiedliche Gruppen ein: „Community Believers“ mit 19 Prozent, „Professionals“ mit 25 Prozent, „Hobbyists“ mit 27 Prozent und „Learning and intellect“ mit 29 Prozent. Die Community Believers fühlen sich hierbei der Gemeinde verpflichtet (83 Prozent) und wünschen sich einen freien Zugang zum Code (64 Prozent). Die Professionals sehen den Nutzen ihrer Arbeit im arbeitstechnischen Bereich (91 Prozent) und programmieren vor allem, weil sie dafür bezahlt werden (80 Prozent). Die Hobbyists programmieren, um die Software vor allem im privaten Bereich nutzen zu können (100 Prozent). Die Gruppe Learning and intellect hackt vor allem zum Spaß (69 Prozent) und um ihre Fähigkeiten zu verbessern (72 Prozent). Hierin wird wieder deutlich, dass die Programmierer der Open-Source-Gemeinde keineswegs einheitlich motiviert sind und sehr unterschiedliche Ausgangslagen besitzen. Interessant ist auch, dass nur die Professionals die Bezahlung als wesentlichen Faktor angeben, während die Übrigen dies eher als Nebensache ansehen. Hier wird der freiwillige Charakter vieler Open-Source-Programmierer deutlich. Interessant ist zudem, dass bei den Community Believers mit 19 Prozent der höchste Anteil an Personen zu messen ist, die es als wichtig ansehen, die kommerzielle Software zu bekämpfen.

Identifikation mit Hackern



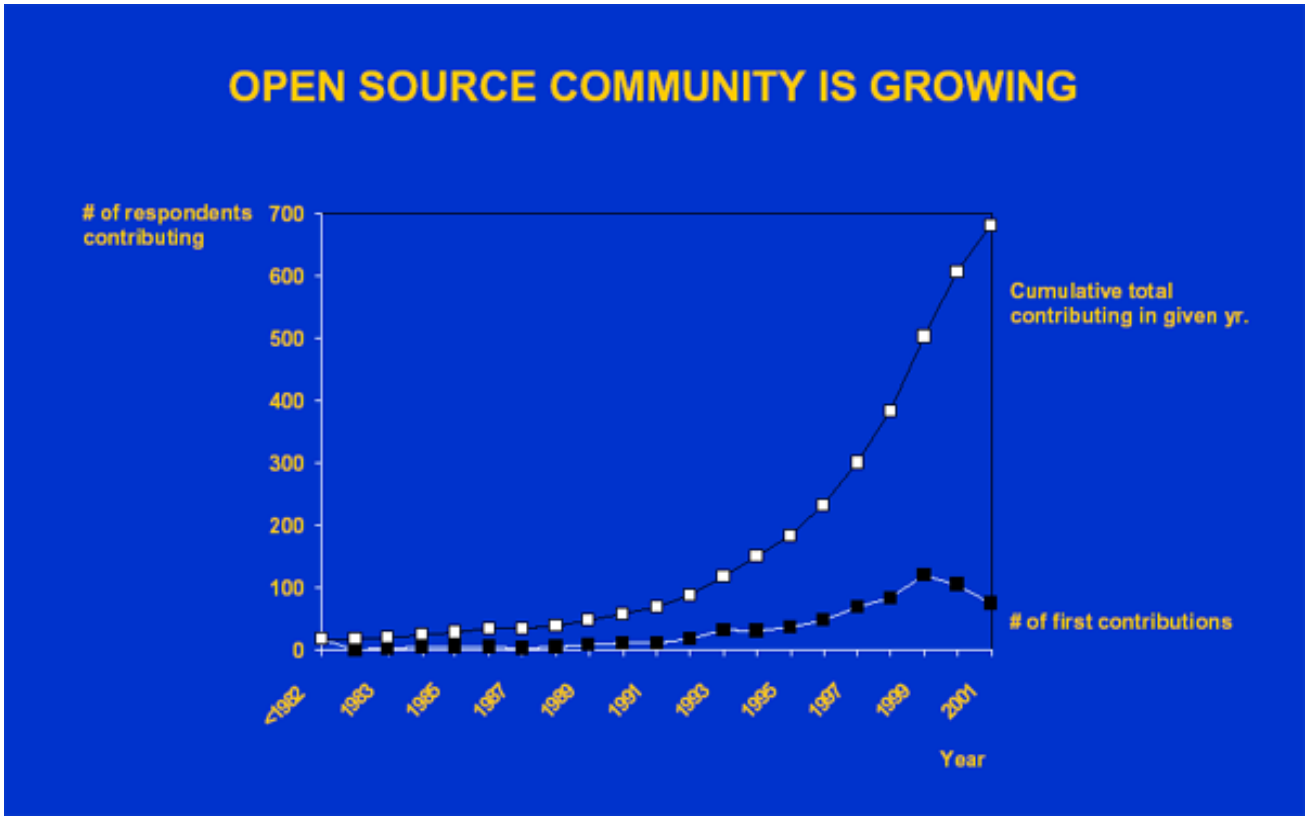
83 Prozent der Open-Source-Programmierer können sich zum Teil oder sehr mit der Hackerszene identifizieren, und nur 8 Prozent können sich damit nicht identifizieren. Dies zeigt die starke Verknüpfung der Programmierszene, die aufgrund der Motivationslage zum Teil zur Hackerszene dazu gezählt werden muss. Wie weit die Verstrickungen gehen und wie weit Programmierer, speziell der Open-Source-Gemeinde, selber auch kriminelle Hacker sind, ist hierbei nicht ersichtlich. Es kann aber vermutet werden, dass hier die Übergänge fließend sind und dass gerade die Hobbyisten dazu neigen, aktiv die kommerzielle Software durch spezielle Vorgehensweisen, wie das Ausspähen von Daten oder die Entschlüsselung des Codes, zu unterwandern. Dies wird auch noch mal durch die folgenden zwei Grafiken bestätigt, die mit ihren Aussagen stark an die Motive von kritisch-kreativen Hackern erinnert.

Alters- und Geschlechtsstruktur der Open Source Szene



Die Open-Source-Gemeinde ist mit einem Geschlechtsanteil von 98 Prozent fast ausschließlich männlich dominiert. Die Studie unterteilte die Hacker in drei Generationen. „Generation Y“ bis 21 Jahre, „Generation X“ bis 38 Jahre und die „Boomers“ ab 39 Jahren aufwärts. Die meisten Hacker sind der Generation X zuzuordnen und 22-37 Jahre alt. Das Durchschnittsalter liegt hier bei 30 Jahren, wobei die drei Spitzenjahre 26-28 Jahre sind. Die meisten Programmierer haben hier über 10 Jahre Programmiererfahrung, was vermuten lässt, dass es sich bei ihnen um ursprüngliche Programmierer und Hacker der Anfangszeit des Computers und des Internets handelt. Dies würde auch die Neigung erklären, weshalb so viele Angehörige dieser Szene sich zur allgemeinen Hackerszene zugehörig fühlen.

Wachstum der Open-Source-Gemeinde



Die Graphik verdeutlicht den starken Zuwachs der Open-Source-Gemeinde. Anzunehmen ist in diesem Zusammenhang, dass auch die gesamte Hackerszene proportional zunimmt.

3.9.3 „Account Missbrauch im Internet“ des Bundeskriminalamts (BKA)

Das Bundeskriminalamt veröffentlichte im Jahr 2003 eine Studie mit dem Titel „Account-Missbrauch im Internet“. Die Studie besteht aus zwei Teilen und behandelt mehrere Missbrauchsfälle im Bereich Internet. Jens Vick beschreibt im ersten Teil der Studie die Erfahrungen der Ermittlungskommission „INET“ beim Polizeipräsidium Münster, und Franz Roters analysiert und typologisiert anschließend aus kriminologischer Sicht die Tatverdächtigen.

Am 14. April 1999 begann ein im Münsterland ansässiger Internet-Provider seine Dienste anzubieten. Als sich bald darauf sehr viele Kunden über zu hohe Rechnungen beschwerten, wurden die Verbindungsdaten überprüft. Dabei stellte sich heraus, dass Zugangsdaten vieler Kunden aus dem gesamten Bundesgebiet ausgespäht, zum Teil missbraucht oder verändert wurden und einige Benutzer sich mit falschen Personalien angemeldet hatten. Die Opfer erstatteten sodann Anzeige bei der zuständigen Polizeistelle. Die Polizei stellte relativ schnell fest, dass es sich hier um sog. Fake-Accounts (Betrug durch Angabe falscher Personalien),

missbrauchte Accounts (missbräuchliche Nutzung echter Kundenzugänge), auf Web-Seiten veröffentlichte Zugangsdaten und Hinweise auf Hacker (Ausspähen von Daten mit so genannten „Trojanern“) handelt. Viele Tatverdächtige nutzten zudem gleich mehrere Kundenzugänge. Einzelne Kundenzugänge waren wiederum für mehrere Tatverdächtige zugänglich. Mit der unrechtmäßigen Beschaffung und Nutzung von fremden Kundendaten konnten sich die Tatverdächtigen in das Providernetz einwählen und deren Dienste nutzen.[722] Die Verbindungen wurden dabei hauptsächlich genutzt, um im Internet umsonst zu surfen oder um mit Hilfe von Trojanern weitere Daten auszuspähen. Durch den Missbrauch der einzelnen Accounts entstanden Verbindungskosten in Höhe von ca. 1,5 Millionen Euro. Dem Provider entstand ein Gesamtschaden von ca. 4,5 Millionen Euro. Bei den Kunden entstanden im Einzelfall Online-Kosten von bis zu 12.000 Euro. Nach Auswertung der beschlagnahmten Daten mit über 8.500 Telefonanschlussinhabern konnte die Ermittlungskommission mehr als 3.600 tatverdächtige Personen ermitteln.

Im Zusammenhang mit dem geschilderten Sachverhalt wurde im August 2000 das Kriminalistische Institut (KI) des Bundeskriminalamts vom Polizeipräsidium Münster beauftragt, ein Forschungsprojekt im Bereich der Computerkriminalität durchzuführen, das mit diesem Ermittlungsverfahren wegen Account-Missbrauchs gegen mehrere Tausend Verdächtige in Deutschland verbunden war. Ziel der darauf folgenden Auswertung aller Daten war es, eine Tätertypologie für Computerkriminelle zu erstellen, um sinnvolle Präventions- und Repressionskonzepte im Bereich der Computerkriminalität zu entwickeln.

Es wurde relativ schnell vermutet, dass nicht die Telefonanschlussinhaber die eigentlichen Täter sind, sondern deren Kinder. Es wurden Fragebögen an die Staatsanwälte verschickt, die diese wiederum an die zuständigen Polizeibeamten weiterleiteten. Darauf folgte die Auswertung der Daten. Insgesamt wurden 663 Fragebögen an das BKA zurückgeschickt, von denen 599 zumindest zum Teil verwertbar waren. Es wurde bei der Auswertung schwerpunktmäßig differenziert nach Geschlecht, Alter, Lebensumständen, Einbringen von Trojanern und Vorsatz.

[722] Die Tatverdächtigen nutzen hierfür echte Daten von Kunden, die sie zuvor selbst ausgespäht hatten und/oder echte Daten von Kunden, die von anderen Personen ausgespäht und im Internet veröffentlicht wurden und/oder falsche Kundendaten, die sie zuvor selbst eingegeben hatten und/oder falsche Kundendaten, die von anderen im Internet veröffentlicht wurden.

Von den 599 Tatverdächtigen waren nur 35 Frauen. Interessant ist auch die unterschiedliche Altersstruktur. Die Frauen waren im Durchschnitt 12 Jahre älter als die Männer und lebten aufgrund ihres höheren Alters im Gegensatz zu den Männern nicht mehr bei ihren Eltern. Der Altersdurchschnitt bei den Männern lag bei 22,2 und bei den Frauen bei 34,7 Jahren. Auch in der EDV-Erfahrung und der EDV-Austattung unterschieden sich die Geschlechter. Die EDV-Erfahrung der Frauen wurde signifikant geringer eingestuft. Die männlichen Tatverdächtigen hatten zudem die neueren Rechner und gaben im Durchschnitt mehr als das Doppelte für das Aufrüsten und die Peripheriegeräte aus.

Die Motive der Frauen beschränkten sich weitgehend auf das „Ausprobieren“ und auf „wirtschaftliche Gründe“, und sie verwendeten weniger Accounts als die Männer. Erstaunlich ist auch, dass die Frauen wesentlich seltener wussten, dass sie eine strafbare Handlung begingen. Gerade dies erscheint aufgrund des höheren Alters erstaunlich. Das Alter und die Lebensumstände der Tatverdächtigen zeigen, dass die durchschnittliche Altersstruktur mit ca. 23 Jahren vom klassischen „Jugendlichen“ abweicht. Jedoch war die Altersgruppe der 16- bis 21-Jährigen mit 65,8 Prozent am häufigsten vertreten, insgesamt 72,2 Prozent der Tatverdächtigen lebten während der Tatbegehung bei ihren Eltern.

Eine Unterteilung der Tatverdächtigen in zwei Altersgruppen, die der unter 22-Jährigen und die der über 22-Jährigen, brachte weitere Erkenntnisse. Die ältere Gruppe hatte signifikant mehr EDV-Erfahrung, mehr Geld zur Verfügung und wesentlich weniger Accounts verwendet als die jüngere Gruppe. Dies wirkt sich auch auf die Motivationslagen aus. So gaben 301 Personen wirtschaftliche Gründe als Motiv an, wovon 251 (83,39 Prozent) aus der Gruppe der unter 22-Jährigen und nur 50 (16,61 Prozent) aus der älteren Gruppe stammten. Dies könnte daran liegen, dass die Älteren bereits über eigenes Einkommen verfügten. Die höhere Erfahrung mit Computern kann einfach darin begründet sein, dass sich die Älteren bislang mehr mit Computertechnologie beschäftigen konnten. Das Ausprobieren, das von 192 Personen als Motiv angegeben wurde, scheint ein Spezifikum der jüngeren Nutzer zu sein. So nannten 151 (79,7 Prozent) jüngere und nur 39 (20,3 Prozent) ältere Tatverdächtige dieses Motiv. Weitere Unterschiede beider Gruppen gab es im Hinblick auf sonstigen Beschäftigungen. So betrieben 18 Prozent der jungen Tatverdächtigen Mannschaftssport, aber nur 7 Prozent der Älteren. 36 Prozent der jüngeren Tatverdächtigen trafen sich in Cliquen, aber nur 9 Prozent der Älteren. 35 Prozent der jüngeren Tatverdächtigen beschäftigten sich mit Fernsehen, Video, Musik; aber nur 17 Prozent der älteren.

Kaum Unterschiede gab es bei der Schulbildung, der Zeit am Computer, der monatlichen Aufwendungen für den Internetzugang oder der Schadenshöhe. Im Ergebnis wird vermutet, dass die Unterschiede darin begründet sind, dass im Alter von etwa 22 Jahren ein Lebenswandel stattfindet. Dabei spielen Faktoren wie die Abnabelung vom Elternhaus, die damit verbundene Selbstständigkeit und die verringerte Kontrollmöglichkeiten seitens der Eltern eine wesentliche Rolle.

Die Autoren unterschieden zwei Gruppen: Die erste Gruppe spähte mit Hilfe von Trojanern Zugangsdaten, speziell die Benutzernamen und die dazu gehörigen Passwörter, von Internetnutzern aus und veröffentlichte diese sodann auf Hackerseiten. Die zweite Gruppe spähte keine Daten aus, sondern nutzte die Zugangsdaten ausschließlich, um kostenlos zu surfen. Interessant ist jedoch, dass die erste Gruppe nur 6 Prozent der Gesamtzahl beträgt. Diese Gruppe ist jedoch ausschlaggebend, da nur sie die Daten herausfanden, um diese zur freien Verfügung zu stellen. Alle übrigen Tatverdächtigen sind eher Nutznießer. Das heißt jedoch nicht, dass die erste Gruppe nicht auch Nutznießer anderer Hackerveröffentlichungen ist. Diese Gruppe war sehr heterogen und über das ganze Bundesland verteilt. Ob direkte Kontakte z.B. über Chatrooms bestanden, konnte nicht ermittelt werden. Dies liegt wohl auch daran, dass Informationsweitergabe und Hilfestellungen nicht nur unter einem Synonym stattfinden, sondern zudem meist recht wahllos geschehen. Jeder stellt auf mehreren Plattformen seine Erkenntnisse, hier die Zugangsdaten, allen Nutzern zur Verfügung. Aus diesem Grund werden diese Szenen auch als Geschenkkultur angesehen.[723] Jedoch bleibt zu bedenken, dass hier oft fremde Güter verschenkt werden, die in diesem Fall zudem für die kostenlose Nutzung des Internets missbraucht wurden.

[723] Raymond 1999, S. 80 ff.

Die folgenden Grafiken zeigen die Motivationslagen, die bei dieser Studie herausgefunden wurden.

Anzahl der Motive	*Fälle*	*in %*
Kein Motiv	147	24,5
Ein Motiv	287	47,9
Zwei Motive	115	19,5
Drei Motive	39	6,5
Vier Motive	8	1,3
Fünf Motive	2	0,3
Sechs Motive	1	0,2

Fast ein Viertel der Tatverdächtigen (24,5 Prozent) gab kein Motiv an. Knapp die Hälfte (47,9 Prozent) gab jedoch zumindest ein Motiv an. Das restliche Viertel (27,8 Prozent) hatte zwei und mehr Motive angegeben. Von den 75,7 Prozent, die zumindest ein Motiv für ihr Handeln angaben, wurden die Arten der Motive in folgende Kategorien gegliedert:

Motive	*Fälle*	*in %*
Wirtschaftliche Gründe	307	51,3
Ausprobieren	198	33,1
Technische Möglichkeiten	72	12
Sonstige Gründe	49	8,2
Reinlegen	16	2,7
Gruppen-Anerkennung	9	1,5
Wettkampf	6	1
Anerkennung im Internet	4	0,7
Geheimdienst	2	0,3
Ausspionieren	nicht genannt.	0
Jemanden Schaden zufügen	nicht genannt	0

Besonders hervorzuheben ist die Auswahl der Fragen in Bezug auf die Motive der Tatverdächtigen. So scheint eine Einteilung in Gruppenanerkennung, Wettkampf, Ausprobieren und wirtschaftliche Gründe sinnvoll.

Auffällig ist, dass die Gruppenanerkennung nur mit 1,5 Prozent und der Wettkampf untereinander nur mit 1 Prozent vertreten sind. Dies mag daran liegen, dass die hier ermittelten Tatverdächtigen evtl. nicht dem typischen Hackerprofil entsprechen. So werden Personen, die fremde Accounts nutzen, nur im entfernten Sinn zu den Hackern gezählt. Vielmehr ist die kleine erste Gruppe als typische Hacker zu qualifizieren. Leider resultieren aus der Studie keine Erkenntnisse, ob der Wettkampf untereinander und die Gruppen-Anerkennung bei diesen Tatverdächtigen gewichtiger erscheinen. Die wirtschaftlichen Gründe werden mit 51,3 Prozent als hauptsächliches Motiv angegeben. Dies liegt vor allem daran, dass die hier ermittelten Täter hauptsächlich als Nutznießer in Erscheinung traten. Ihnen war es wichtig, kostenlos zu surfen und nicht, sich gegenüber Anderen zu profilieren.

Der typische Täter hat nach den Ergebnissen dieser Studie nur wenig finanzielle Möglichkeiten und kommt mit diesen nur mühsam oder gar nicht aus. Die zentrale These aus Mertons Anomietheorie lautet, „dass abweichendes Verhalten als Symptom für das Auseinanderklaffen von kulturell vorgegebenen Zielen und von sozial strukturierten Wegen, auf denen diese Ziele zu erreichen sind, betrachtet werden kann.“[724] Es scheint, als ob das Bedürfnis, mit dem Internet an Informationen und Funktionen zu gelangen, durch die für die Täter subjektiv als zu hoch empfundenen Kosten behindert wird.

Das Ausprobieren liegt mit 33,1 Prozent an zweiter Stelle. Es mag vor allem für Einsteiger ein gewichtiger Grund sein. Neugier als Motivationsfaktor kann auch durch diese Studie belegt werden. Interessant ist auch, dass niemand das Ausspionieren als Motiv genannt hat. Ein Grund könnte darin liegen, dass sie ihre Handlungen nicht als ein Ausspionieren ansehen und somit in ihrer Sicht ihre Handlungen sich neutralisieren. Ein anderer Grund könnte wiederum darin liegen, dass die Befragten aus Angst vor Konsequenzen keine Angaben hierzu gemacht haben. Ebenfalls erstaunlich erscheint, dass niemand die Schadenszufügung als Motiv nannte. Dies mag daran liegen, dass die Tatverdächtigen unter Motiv nur den Ausgangsansporn gesehen haben. Das Wissen um die Konsequenzen auf Seiten der Opfer wird dabei wohl nicht als

[724] Merton 1979, S. 289.

Motiv gewertet, obwohl man vermuten kann, dass die meisten wussten, dass dem wahren Accountbesitzer höhere Kosten entstehen würden.

Im Bereich des Vorsatzes und der Möglichkeit der Zurückverfolgung wurde festgestellt, dass 230 Tatverdächtige weder wussten, dass die Tat zurückverfolgt werden kann, noch dass ihr Handeln strafbar ist. Dem stehen 76 Personen gegenüber, denen bekannt war, dass ihr Verhalten zurückverfolgt werden konnte und denen ebenfalls bekannt war, dass sie eine strafbare Handlung begehen würden (16,1 Prozent). 103 Personen (21,8 Prozent) war zwar bekannt, dass sie eine strafbare Handlung begingen, aber sie wussten nichts über die Zurückverfolgungsmöglichkeiten. Bei 63 Personen war es umgekehrt: Sie wussten, dass ihr Verhalten zurückverfolgt werden konnte. Es war ihnen aber nicht klar, dass sie eine strafbare Handlung begehen würden (13,3 Prozent). Hier wird wiederum der Irrtum deutlich, dass das Internet anonym sei. Grundsätzlich sind alle Verbindungen nachvollziehbar. Die Rückverfolgung lässt sich jedoch aufgrund der dezentralen Struktur des Internets nur mit einem immensen Aufwand bewerkstelligen, so dass zumeist davon abgesehen wird und nur in Fällen mit einer hoher Schadensumme ermittelt wird.[725] Aber auch der Irrtum einiger Nutzer wird hier deutlich, dass man im Internet nicht viel falsch machen könne.

Zeigt das Entdeckungsrisiko eine zu geringe Wirkung auf die Tätergruppe, so muss von einer höheren Deliktrate ausgegangen werden.[726] In dieser Untersuchung schien zumindest dieses Entdeckungsrisiko für 230 Personen nicht existent. Es zeigen sich Anknüpfungspunkte zum Rational-Choice-Ansatz. Der subjektive Wert liegt hierbei im kostenlosen Surfen, wobei die Wahrscheinlichkeit, dass mit den gefundenen fremden Zugangsdaten der gewünschte Erfolg eintritt, sehr hoch ist. Insbesondere das subjektiv wahrgenommene Entdeckungsrisiko scheint aufgrund dieser Ergebnisse sehr gering zu sein; über 230 Personen dachten, dass diese Handlungen aufgrund der Anonymität des Internets nicht entdeckt werden könnten. Somit war die Gelegenheit günstig, Hindernisse schienen nicht bereit zu stehen, und die normkonformen Alternativen schienen nicht attraktiv, da diese mit privaten Kosten verbunden waren.

[725] Die Meinung, dass anhand der Zugangsdaten, bei denen sich jeder Nutzer auch Synonyme geben kann, eine Ermittlung der Person nicht möglich ist, ist ein verbreiteter Trugschluss. Grundsätzlich kann anhand des physikalischen Anschlusses und der Log-Dateien der jeweilige Haushalt ermittelt werden. Auch so genannte Anonymizer bieten je nach Qualität nur teilweise Möglichkeiten zur Anonymisierung. So kann z.B. das benutzte Betriebssystem oder sogar die IP-Adresse verschleiert werden. Natürlich ist es wie bei allen Straftaten möglich, verschiedene Möglichkeiten zu kombinieren und es den Ermittlern zu erschweren, den Täter zu finden.
[726] Karstedt/Greve 1996, S. 178.

Aufschlussreich ist die Auswertung der Faktoren in Bezug auf den typischen Täter. Danach ist der typische Computerkriminelle ein männlicher Schüler oder Auszubildender zwischen 16 und 21 Jahren, der bei seinen Eltern lebt. Motive für sein Handeln ist die Bereicherungsabsicht und das Probierhandeln. Er hat eine mittlere bis gehobene Schulbildung (zwischen Real- und Oberschule) und mittlere bis hohe Computerkenntnisse, die er sich größtenteils autodidaktisch angeeignet hat. In seiner Freizeit beschäftigt er sich außerdem mit Cliquen, Fernsehen und Musik. Aufmerksam über die Möglichkeit einer Tatbegehung wurde er über Chats, Webseiten oder Freunde.

Effektive und effiziente kriminalpolizeiliche Sachbearbeitung war nach der Überzeugung der Kommission nur durch die Zusammenführung aller Ermittlungsverfahren möglich, da einzelne Ermittlungen bundesweit zu vielen Überschneidungen und Parallelen führen würden. Dies zeigt wiederum, dass durch den Computer und das Internet neue kriminalistische Ermittlungen notwendig sind.[727] Außerdem waren die Autoren über die verwendeten Kommunikationsformen wie Chats oder Hacker-Webseiten erstaunt. Das verdeutlicht die bislang mangelnde Fachkenntnis der Behörden bezüglich der Computerkriminalität, da sich gerade in diesem Bereich viele Kriminelle bewegen.

Außerdem war der Provider nicht bereit, der Polizei zu helfen und Auskünfte zu geben. Vielmehr wurde versucht, Daten und Informationen zu verbergen, weshalb eine Durchsuchung veranlasst wurde. Zudem erstattete der Provider erst nach der Durchsuchung ebenfalls Anzeige. Die Begründung war, dass dem Provider eigentlich kein Schaden entstanden sei, da gemäß AGB die Kunden den Schaden tragen müssten. Ob dies der alleinige Grund war, scheint hier zweifelhaft, da der Provider ja gerade auf den Markt getreten war und offensichtlich einen Imageschaden fürchtete.

Die Kommission stellte fest, dass nur wenige Mitarbeiter und Sachbearbeiter des Verfahrens Erfahrungen im Bereich der Computerkriminalität hatten. Es wurde schnell deutlich, dass in diesem Bereich qualifizierte Sachbearbeiter unentbehrlich waren, die „Neuland betreten" müssten. Sie forderte deshalb auch umgehend Fortbildungsmaßnahmen für die Mitarbeiter, um dieser neuen Erscheinungsform der Kriminalität sachgerecht begegnen zu können. Die Kommission erstellte eine neue Datenbankanwendung, in der die 990.000 Einzelverbindungen, 29.000 Kundendaten, 8.600 Telefonanschlussinhaber und 3.600 Tatverdächtigen derge-

[727] Es stellt sich diesbezüglich die Frage, ob in dieser digitalisierten und globalen Welt Polizeiarbeit überhaupt noch Ländersache bleiben kann?

stalt verknüpft werden konnten, dass automatisiert strafwürdige Verhaltensweisen herausgefiltert werden konnten. Trotzdem zeigt die Studie, dass die Behörden rein technisch mit diesem Phänomen kaum zurecht kamen. Allein für die Erstellung der Anzeigen wurden über 70.000 Blatt verbraucht und zu diesem Zweck ein Hochleistungsdrucker geleast.

Vor allem stellte die Kommission fest, dass es sich bei der Internetkriminalität um eine neue Form der Massen- und Jugendkriminalität handelt. Nachdem den Ermittlern dies bewusst geworden war, legten sie bei den Ermittlungen ein besonderes Augenmerk auf die pädagogische Wirkung der Strafverfolgung. Einige Tatverdächtige, die nur einen geringen Schaden verursacht hatten, bekamen trotz Einstellung der Verfahren einen Brief mit Hinweisen auf die Strafbarkeit und Recherchierbarkeit des Verhaltens im Internet. Gerade in diesen Fällen meldeten sich viele Eltern zurück, dass sie ihre Erziehungsaufgabe im Zusammenhang mit den neuen Technologien mangels entsprechender Kenntnisse nicht mehr richtig wahrnehmen könnten und froh seien, dass ihre Kinder noch rechtzeitig „erwischt" wurden. Dies zeigt, wie uninformiert die Eltern der neuen Technologie gegenüberstehen und wie wenig oder keine Kenntnisse darüber vorhanden sind, welche Straftaten mit dem Computer und dem Internet von zu Hause begangen werden können. Es muss allerdings hier bedacht werden, dass eine Auswertung wahrscheinlich nur derjenigen Tatverdächtigen stattfinden konnte, die mindestens 16 Jahre alt waren. Alle anderen Verfahren wurden aufgrund der mangelnden Strafwürdigkeit von den Behörden eingestellt, so dass Motive und Beweggründe von Tätern unter 16 Jahren hier nicht mit in die Analyse einfließen konnten.
Insgesamt bietet die Studie trotz kleiner Defizite insgesamt Aufschluss über die Motive und sozialen Hintergründe der Hacker. In Zukunft sollten bei der Ermittlung von Computerkriminalität weitere solcher Studien folgen, um einen besseren Einblick in die Gesamtheit dieses weiten Feldes zu gewinnen.

3.9.4 RSA-Studie: „Understanding a hacker's mind"

Im Jahr 2004 wurde unter der Leitung von Christian Fötinger und Wolfgang Ziegler von der Donau-Universität Krems eine Untersuchung veröffentlicht. RSA Security hat das Zentrum für praxisorientierte Informatik der Donau-Universität Krems[728] mit einer Abhandlung über

[728]Weitere Informationen unter http://www.donau-uni.ac.at/de/studium/fachabteilungen/tim/zentren/zpi/studienangebot/security/index.php

die psychologischen Beweggründe für den Diebstahl von Identitäten[729] beauftragt. RSA Security unterstützt Unternehmen beim Aufbau von sicheren und zuverlässigen E-Business-Infrastrukturen mit Hilfe seiner Produkte RSA SecurID (Zwei-Faktor-Authentifikation), RSA ClearTrust (Autorisierungslösung), RSA BSAFE (Verschlüsselungssoftware) und RSA Keon (PKI-Lösung). Das Unternehmen blickt auf über 20 Jahre Erfahrung auf dem Gebiet der Sicherheitslösungen zurück und möchte das vorhandene Knowhow in die steigenden Bedürfnisse im Bereich des E-Business einbringen. Mehr als dreizehn Millionen Benutzer weltweit nutzen das RSA SecurID-Verfahren und eine Milliarde der RSA BSAFE-Lizenzen befinden sich bereits auf dem Markt.[730]

Die Studie stellt die bislang neueste Untersuchung zum Thema Hackerszenen dar. Diese hat das Ziel, die Beweggründe von Hackern zu durchleuchten und gegebenenfalls eine Typologie zu erstellen. Es wurden Projekte und Forschungsergebnisse berühmter Akademiker und Experten untersucht. Dabei wurden die Anwendungsbereiche und die Absichten von Hackern erforscht. Die Studie bezieht sich auf die psychologischen und soziologischen Beweggründe für illegale Einbrüche in Systeme. Dabei stand der Identitätsdiebstahl im Vordergrund.

Das fünfzigseitige Dossier von Christian Fötinger und Wolfgang Ziegler, beide sind Teilnehmer des Master of Science-Lehrgangs „Information Security Management“, beschäftigt sich dabei hauptsächlich mit der Intention, den psychologischen Motiven und praktischen Methoden von Hackern. Darüber hinaus werden Empfehlungen gegeben, wie sich sowohl Anwender als auch Unternehmer bestmöglich schützen können. Dabei wurde zum Schluss die oben dargestellte Studie des BKA einbezogen.

Zunächst stellen die Autoren die bedrohliche Lage dar, die durch die Computerkriminalität entstanden ist. So betrifft der im Vordergrund stehende Identitätsdiebstahl mittlerweile mehr als 10 Millionen US-Bürger und verursacht jährlich Schäden von mehr als 53 Milliarden US-Dollar. Durch Computerkriminalität wurde in den USA im Jahr 2003 einen Gesamtschaden von über 221 Milliarden US-Dollar verursacht. Die Autoren sehen es trotz der Definitionsproblematik ebenfalls als notwendig an, in ihren Ausführungen grundsätzlich von Hackern und Crackern zu sprechen.

[729] Als Identitätsdiebstahl wird die missbräuchliche Nutzung personenbezogener Daten einer natürlichen Person durch Dritte bezeichnet. Bei einem Identitätsdiebstahl werden persönliche Daten, wie beispielsweise Geburtsdatum, Anschrift, Führerschein- oder Sozialversicherungsnummern, Bankkonten oder Kreditkartennummern entwendet, um eine rechtsverbindliche Identitätsfeststellung zu umgehen oder diese zu verfälschen.
[730] Weitere Informationen unter http://www.rsasecurity.com/

Ausführlich beschreiben die Autoren die Vorgehensweisen und Methoden der Hacker. Da dies bereits ausführlich dargestellt wurde und sich aus den hier vorgetragenen Ergebnissen nichts wesentlich Neues ergibt, wird auf eine Darstellung dieser Ergebnisse verzichtet. Im Bereich des Identitätsdiebstahls scheinen die Hacker entweder durch Gewinnstreben motiviert zu sein oder weil sie zeigen wollen, was sie können. Die Autoren untersuchen zunächst die sozialen Zusammenhänge, die Psychologie sowie die gesellschaftliche Stellung von Hackern. Dabei nehmen sie hauptsächlich zwei Expertenmeinungen zu Hilfe. Zum einen handelt es sich hierbei um Marc Rogers, einen Meinungsforscher ("behavioural sciences researcher") an der Universität von Manitoba in Winnipeg, Canada, und zum anderen um Jerrold M. Post, einen Psychiater an der George Washington University in Washington, D.C. Rogers und Post haben einige grundlegende Verhaltensmerkmale bei Hackern herausgearbeitet. Rogers stellt vor allem das gemeinsame Merkmal von Hackern heraus, die Konsequenzen ihrer Handlungen zu minimieren und ihr Verhalten in eine nützliche Dienstleistung für die Gesellschaft umzudeuten, welches von einigen Forschern auch das „Robin-Hood-Syndrom" genannt wird.

Gresham M. Sykes und David Matza stellen in diesem Zusammenhang fest, „dass Techniken der Neutralisation für die Verhinderung der Wirksamkeit sozialer Kontrollen wesentlich sind und dass sie einem großen Teil delinquenten Verhaltens zugrunde liegen. (…) Wir meinen vielmehr, dass der Delinquent häufig und in einer unklaren Weise fühlt, dass sein Verhalten trotz der Tatsache, dass es gegen das Gesetz verstößt, keinen wirklichen Schaden anrichtet. (…) Der Delinquent verschiebt seine Aufmerksamkeit von seinen eigenen abweichenden Akten auf die Motive und das Verhalten derjenigen, die seine Verfehlungen mißbilligen. Seine Verdammer sind, mag er behaupten, Heuchler, Abweichler, die sich verstellen oder angetrieben werden durch persönlichen Hass."[731] Hacker verharmlosen ihr Verhalten, indem sie es als nützliche und notwendige Dienstleistung gegenüber der Gesellschaft darstellen. Zum Robin-Hood-Syndrom passt auch, dass Feindbilder geschaffen werden, wie sie sich beispielsweise in Microsoft oder staatlichen Institutionen manifestieren, um das eigene Verhalten sich selbst gegenüber zu rechtfertigen. In diesem Sinne sprechen Sykes und Matza von der Ablehnung des Opfers: „Das Unrecht, so könnte behauptet werden, ist in Wirklichkeit kein Unrecht; es ist vielmehr eine Form gerechter Rache oder Strafe. Durch die subtile Alchemie verwandelt sich der Delinquent in einen Rächer und das Opfer wird zu einem Übeltäter. (…); aber Robin Hood und seine Nachfahren wie der harte Detektiv, der außerhalb des Gesetzes Gerechtigkeit

[731] Sykes/Matza 1979, S. 366 ff.

verwirklichen will, nehmen noch immer die allgemeine Phantasie gefangen, und der Delinquent mag seine Handlungen als Teil einer ähnlichen Rolle sehen.“[732]

Der Psychiater Post spricht von einer „ethical flexibility“, die Hacker gemeinsam haben, womit gemeint ist, dass durch die minimierten direkten menschlichen Kontakte das Hacken nur als Spiel angesehen wird, weshalb die Konsequenzen leicht ignoriert werden können. Das Handeln der Hacker richtet sich nicht gegen Personen, sondern gegen Institutionen oder den Computer. Sie sehen ihr abweichendes Verhalten als Wettkampf mit den Administratoren, Antivirenherstellern oder Programmierern. Die Konsequenzen werden neutralisiert, da eine gewisse Anonymität darin liegt, dass sich die Personen nicht persönlich gegenüberstehen, sondern ausschließlich über das Medium Computer kommunizieren oder anderweitig in Kontakt treten.

Sykes und Matza formulieren in diesem Zusammenhang folgende Aussage: „Soweit das Opfer physisch abwesend, unbekannt oder eine vage Abstraktion (was oft bei Eigentumsdelikten der Fall ist) ist, wird die Wahrnehmung der Existenz des Opfers geschwächt.“[733] Durch die Entpersonalisierung der Opfer zeigt sich hier wiederum eine Form der Neutralisation, durch die sich das eigene Verhalten leichter rechtfertigen lässt.

Der Meinungsforscher Rogers teilt Hacker in vier Kategorien ein und stellt dabei fest, dass nicht alle Hacker kriminell sind: „Old School Hackers“, „Script-Kiddies oder Cyber-Punks“, „Professional Criminals, or Crackers“, „Coders and Virus Writers“. Mit Old School Hackers meint Rogers die ursprünglichen Hacker vom MIT. Sie haben ein Interesse an Programmcodes und analysieren gerne Systeme. Sie haben grundsätzlich keine bösen Absichten und glauben an das Internet als freies und offenes System. Dagegen fallen Script-Kiddies auf, da sie im Internet mit ihren Taten protzen und dadurch auch verstärkt ins Blickfeld der Behörden geraten. Nach Rogers sind sie zwischen 12 und 30 Jahre alt, gebildet, weißer Hautfarbe und männlich. Sie sind gelangweilt von der Schule, aber dafür sehr geschickt im Umgang mit der Computertechnologie. Sie laden Skripte runter und hacken sich in Systeme ein, um dort zu vandalisieren. Die Professional Criminals oder Crackers brechen in Systeme ein, um diese Informationen zu verkaufen. Sie sind von Unternehmen oder Regierungen engagiert, können aber auch Verbindungen zu organisierten kriminellen Gruppen haben. Bezogen auf die vierte Gruppe, die Coder und Virus Writer, bemängelt Rogers zunächst die mangelnde Forschungs-

[732] Sykes/Matza 1979, S. 368.
[733] Sykes/Matza 1979, S. 368.

arbeit auf diesem Gebiet. Die Coder und Virus Writer sehen sich selbst als eine Art Elite und haben grundsätzlich einen hohen Programmierkenntnisstand und schreiben Programmcodes, ohne diese selbst zu nutzen.

Rogers ordnet Script-Kiddies und Cyber-Punks einer Gruppe zu. Dies verwundert, da die Cyber-Punk-Kultur kaum etwas mit den Hackern im heutigen Sinn gemeinsam hat, da sie eher den Lebensstil einer Fankultur darstellt. Bei den Professional Criminals oder Crackers bezieht sich Rogers ausschließlich auf professionelle Hacker. Problematisch ist, dass es viele Cracker gibt, die allein aus Spass und aus Wettkampfgedanken sabotieren und deren Verhalten nicht zwangsläufig professionellen Charakter aufweist. Rogers bezieht ausdrücklich die Spionagetätigkeiten von Regierungen mit in den Hackerbegriff ein, was wiederum zeigt, wie schwer eingrenzbar dieser Begriff ist, da die Handlungen von Regierungen grundsätzlich einer Legitimation unterworfen sind. Somit spiegelt sich anhand des Hackerbegriffs die Kriminalisierung einzelner Handlungen und Tätergruppen wider.

Bei den Coders und Virus Writers übersieht Rogers jedoch, dass viele Virenautoren gerade keine hohen Fachkenntnisse haben, sondern nach dem Baukastenprinzip Viren generieren. Gerade die Unterteilung in Virenschreiber und Script-Kiddies erscheint problematisch, da viele Script-Kiddies sich auf das Herstellen von Viren spezialisiert haben und dies als das große Problemfeld der Zukunft angesehen wird, da ihnen wegen des jungen Alters oft noch das Verständnis für ihr Verhalten fehlt. Hierin zeigt sich auch die Problematik dieser Thematik, da keine eindeutigen Abgrenzungen möglich sind und eindeutige Abgrenzungen stets zu einer falschen Darstellung der Szene führen müssen. Dies liegt meines Erachtens vor allem daran, dass die Szene nicht direkt abgrenzbar ist, sich hauptsächlich online trifft und die Interessen mit der Zeit wechseln. Rogers bemängelt zudem, dass die von ihm vorgestellte Unterscheidung in der Bevölkerung nicht existiert. Dort gibt es nur „die kriminellen Hacker“. Trotzdem heißen die Autoren die Vorgehensweisen von echten Hackern nicht gut, was durch die folgende Aussage verdeutlicht wird, bei der sie Hackertechniken mit dem Hausfriedensbruch vergleichen: „A person who enters your house and leaves a message on your fridge saying, ‚I was testing the security of back doors in the neighborhood and found yours unlocked. I didn’t take anything, but you should fix your system!’“ Auch wenn die Vorgehensweisen von echten Hackern teilweise nicht strafrechtlich verfolgbar sind, sehen die Autoren diese als verwerflich an. Es könnte sich hierbei um eine sog. „moralunternehmerisch definierte

Computerkriminalität“ handeln, wie sie von Hess und Scheerer bezeichnet wird.[734] Rogers und Post betonen jedoch, dass diese Hacker wohl nicht schwerpunktmäßig das Problem darstellen, mit dem sich die Behörden beschäftigen müssen. Eher stellen es die typischen Cracker, also Professionelle und Script-Kiddies dar.

Rogers stellt fest, dass es trotz der bislang geringen Anzahl empirischer Studien so aussieht, als bestehe keine homogene Hackerszene, sondern viele Untergruppen. Er ist der Meinung, dass die Untergruppen am besten klassifiziert werden können in Abhängigkeit von ihren Motiven und ihren Beweggründen: „The subgroup the hacker would be classified as depends on the motives and causes behind the behaviour”.

Als weiteren Experten nennen die Autoren Bernhardt Lieberman, der im Bereich Soziologie an der Universität von Pittsburgh im August 2003 eine empirische Studie über Hacker beendet hat. Er beschäftigte sich über 10 Jahre mit der Hackerkultur. Lieberman interviewte Hacker in Westpennsylvania und gab ihnen Fragebögen, in denen nach ihren Einstellungen zu Gesetzen und zu anderen sozialen Interaktionen gefragt wurde. Er fand heraus, dass Hacker sich von anderen Gruppen und Personen nicht unterscheiden. Interessant ist zudem, dass er zwei grundlegende Definitionen von Hackern entwarf: „A hacker is either someone who does elegant programming on computers and is considered positive in the public’s eyes, or a hacker is someone who intrudes upon another’s computer and is viewed as someone who does harm.” Somit sieht er auch den Programmierer als zur Hackerszene zugehörig an. Die zweite Definition zielt vor allem darauf ab, dass der Hacker in andere Systeme eindringt und dort Schäden verursacht. Leider sind damit gerade die sog. echten oder ethisch motivierten Hacker nicht wirklich zuzuordnen. Sie programmieren nicht ausschließlich, sondern dringen auch in fremde Systeme ein. Jedoch zerstören sie dort nicht, sondern decken nur Sicherheitslücken auf. Diese Gruppe würde nach Lieberman unter keine der Definitionen fallen. Man muss aber diese Gruppe definitiv zu den Hackern zählen, da sie solche Organisationen wie den CCC hervorgebracht hat und einen Teil der Hackerszene darstellt.

Lieberman fand heraus, dass der intellektuelle Wettkampf und die hohe Lernmotivation die zwei Hauptmotive darstellen. Gegen Gesetze zu verstoßen und Bekanntheit zu erlangen, spielte eher eine untergeordnete Rolle. Die Hacker haben Liebermann zufolge sogar hohen Respekt vor dem Gesetz, auch wenn sie dagegen verstoßen. Auch ihre sozialen Kontakte sind

[734] Hess/Scheerer 2004, S. 74.

normal. Sie haben meist eine Freundin und auch sexuellen Kontakt zu ihr. Die einzig zutreffende Stereotypenbildung ist, dass Hacker fast ausschließlich männlich sind.

Die Autoren zeigen zudem Selbstbewertungen in verschiedenen Bereichen durch Hacker. Dabei zitieren sie ausschließlich aus dem Jargon File, der in diesem Bereich eine Aufzählung einzelner Fakten darstellt. Danach stufen Hacker sich selbst als intelligent und neugierig ein, sie lesen Zukunftsromane, hören Musik, spielen Schach und intellektuelle Spiele aller Art. Sie sind zumeist Hochschulabsolventen oder haben eine vergleichbare Qualifikation. Dabei stehen Interessen zur Informatik, Elektrotechnik, Physik, Mathematik, Linguistik und Philosophie im Vordergrund. Sie verabscheuen Produkte von IBM oder Microsoft, Bürokratien, dumme Leute, einfache Hörmusik, Unehrlichkeit und Langeweile. Aus politischer Sicht sind sie eher liberal gesinnt und neigen dazu, antiautoritär zu sein. Rassistisch und ethnisch motivierte Vorurteile sind eher selten. Alle Religionen sind vertreten. Sie haben schlechte Kommunikationsfähigkeiten zu anderen Personen in der alltäglichen Interaktion und können sich schlecht emotional mit Nicht-Hackern identifizieren. Sie neigen generell zur Ungeduld und haben eine schlechte Handschrift.

Wie dieses Profil bei der Eigendarstellung durch die Hacker im Jargon File entstand, erscheint schon problematisch. Es reflektiert Anmerkungen zu Hunderten von USENET-Antworten. Jedoch wurde dabei nicht festgehalten, wer diese Angaben machte, wie alt die Personen waren usw. Vielmehr ist es eine wahllose Aneinanderreihung von Einzeldarstellungen. Auch wenn die einzelnen Darstellungen stimmen mögen, erscheint es zweifelhaft, ob diese Aneinanderreihung das tatsächliche Bild der Hackerszene repräsentiert. Zudem haben nur die Hacker zur Erstellung dieses Profils beigetragen, die sich im Usenet aufhalten, was wohl eher auf die typische von den Medien dargestellte Hackerszene zutrifft. Politische und professionelle Hacker oder Script-Kiddies sind wohl eher nicht in diesem Profil enthalten. Somit ist es zwar ein gewisser Anhaltspunkt für die Eigenwahrnehmung der Hacker, muss aber vorsichtig und mit teilweisen Einschränkungen betrachtet werden. Erstaunlich erscheint trotzdem, dass nach eigenen Angaben die Stereotypenbildung bezüglich unkommunikativen Hackern von ihnen selbst bestätigt wird, obwohl heutzutage die meisten Autoren versuchen, gerade das Bild des eingeschränkten und selbstzentrierten unkommunikativen Hackers zu widerlegen.

Die Autoren sehen Hacker zudem nicht als altruistische Wesen an. Ihre Hauptanliegen beruhen stattdessen vornehmlich in der Gewinnung von Ansehen und Respekt, außerdem in der

eigenen Bestätigung. Die Autoren zitieren als Beleg hierfür Eric S. Raymond, der fünf Handlungsformen für Hacker beschreibt, bei deren Beachtung der Hacker Respekt von anderen erhält: 1. Open-Source-Software schreiben, 2. Open-Source-Software testen und debuggen, 3. Veröffentlichung von nützlichen Informationen, 4. helfen, dass die Infrastruktur funktioniert und 5. der Hackerkultur selbst dienen.

Abschließend stellen die Autoren die bereits oben dargestellte Studie des BKA sowie Sicherheitsvorkehrungen für Private und Unternehmen dar. Da die Autoren diese Studie lediglich übersetzt und daraufhin in ihre Arbeit eingefügt haben und Sicherheitsvorkehrungen für diese Arbeit nicht von Belang sind, wird hier auf weitere Ausführungen verzichtet.

Nach Ansicht der Autoren ist die wichtigste Erkenntnis, dass zwischen Hackern und Kriminellen unterschieden werden muss. Unternehmen, Organisationen und Regierungsstellen sollten die Hacker im Kontext der Kriminalität fürchten, zumal sie heutzutage stark unterschätzt werden. Es erscheint den Autoren sehr wichtig, dass Hacker studiert werden, so dass ihre Absichten und ihre Beweggründe deutlich werden. Die Gesellschaft muss ein besseres Verständnis über soziale und psychologische Hintergründe gewinnen, um die Gesellschaft zu schützen. Hierbei ist es nötig, zwischen Hackern und Crackern unterscheiden zu können. Dabei sollte der Fokus auf Crackern und Script-Kiddies liegen.

3.9.5 Der „Virtual Criminology Report" von McAfee

Im Februar 2005 veröffentlichte McAfee[735] die Studie „Virtual Criminology Report" zum Thema Computerkriminalität. Der „Virtual Criminology Report" wurde im Auftrag von McAfee von dem unabhängigen Schweizer Internetsicherheitsexperten und Computerkriminologen Peter Troxler[736] (Researcher des ETH Zürich, Eidgenössisches Technologie-Institut der Schweiz) zwischen Juli und Dezember 2004 mit behördlicher Unterstützung in Deutschland, Großbritannien, Frankreich, den Niederlanden, Spanien und Italien durchgeführt. Hierbei arbeiteten führende Wissenschaftler und High-Tech-Experten aus der Strafverfolgung europaweit zusammen. Auch wenn die Studie sich nur am Rande mit den Motiven von Hackern be-

[735] McAfee bietet als Softwareunternehmen mit Hauptsitz in Santa Clara, Kalifornien (USA), Sicherheitslösungen an, die Netzwerke von Störungen wie Viren freihalten und Computersysteme vor Attacken und Bedrohungen schützen.
[736] Peter Troxler von der Eidgenössischen Technischen Hochschule Zürich (ETHZ) ist ein unabhängiger Experte für Internetsicherheit und berät Organisatoren aus dem privaten und öffentlichen Sektor, um Verwaltungssysteme für die Wissensökonomie zu entwickeln.

schäftigt, so stellt sie jedoch die bislang neueste Untersuchung zur Hackerkriminalität dar. Die gewonnenen Erkenntnisse müssen jedoch mit einiger Skepsis bewertet werden, da McAfee als Spezialist für Antiviren-Software hier als Auftraggeber der Studie auftritt und vermutet werden kann, dass ein Bedrohungsszenario der Computerkriminalität für ein Antivirenunternehmen eher lukrativ erscheint. Ihr Wert liegt jedoch in der Darstellung der Entwicklung der Hackerkriminalität und der neu entstehenden Kooperation zwischen Hackern und der organisierten Kriminalität. Zudem ist es die erste länderübergreifende Studie, die in Zusammenarbeit mit den europäischen Strafverfolgungsorganen erfolgte. Sie ist als Ausblick für künftige Studien im Bereich der Kriminologie von großem Wert und soll an dieser Stelle vorgestellt werden.

Die Studie teilt sich in vier Abschnitte, die den Wandel der Computerkriminalität, die Entwicklung krimineller Organisationen, organisiertes Verbrechen im Internet und einen Ausblick auf zukünftige Computerstraftaten beschreiben. Die Studie geht dabei von einer Zweiteilung von Computerstraftaten aus: „neue Verbrechen, die nur online begangen werden können“ und „herkömmliche Verbrechen, die jetzt auch online begangen werden können.“[737] Den ersten Bereich bilden Straftaten gegen die Vertraulichkeit, Integrität und Verfügbarkeit von Computerdaten und -systemen. Dabei stehen das Hacking und die Virenherstellung im Vordergrund. Der zweite Bereich betrifft alle bisherigen, vor der Computerkriminalität bekannten Straftaten, die neuerdings mit Hilfe des Computers begangen werden. Dabei werden vom Autor die Erpressung und der Betrug in den Vordergrund gestellt. Diese Zweiteilung steht in genereller Übereinstimmung mit der in dieser Arbeit operierenden Unterscheidung zwischen Computerkriminalität im engeren und im weiteren Sinn.

Beginnend stellt Troxler den Wandel der Computerkriminalität dar. Der Autor geht davon aus, dass bis zum Jahr 2000 Computerkriminalität hauptsächlich von Hackern und Script-Kiddies begangen wurde. Die Motive für kriminelle Handlungen sieht John Suler, Experte für Cyberspace-Psychologie an der Rider-Universität in Lawrenceville, New Jersey, USA, in folgenden Aspekten: „Einige von ihnen sind von der Herausforderung und der Aufregung fasziniert, die mit dem Eindringen in einen verbotenen Bereich einhergeht. Die Tatsache, dass sie etwas tun, das andere nicht können, vermittelt ihnen ein Gefühl von Leistungsfähigkeit, Beherrschung und Macht. Sie beziehen ihr Selbstwertgefühl aus der Tatsache, dass sie mit ihren Handlungen andere, und hierbei besonders andere Hacker, beeindrucken können. Indem sie

[737] Troxler 2005, S.5.

das etablierte System knacken, umgeben sie sich den autoritären Systemen gegenüber mit einer Art Aura des Rebellentums. (…) Ein Hacker fühlt sich dazu gedrängt, darzustellen, dass er besser und schlauer ist als andere. Das Katz-und-Maus-Spiel gegen das System gerät zum nimmermüden und unnachgiebigen Streben nach Selbstbestätigung."[738]

In den letzten Jahren sieht der Autor einen Wandel im Bereich der Tätergruppe. Nicht allein Hacker oder Script-Kiddies werden im Bereich der Computerkriminalität tätig, sondern zunehmend herkömmliche kriminelle Vereinigungen, die den Computer und das Internet zur Straftatbegehung nutzen.[739] Den Vorteil des Internets für Kriminelle sieht der Autor vor allem in folgenden Aspekten: „Da das Internet keine Staatsgrenzen aufweist, konnte sich das organisierte Verbrechen spielend leicht weltweit ausbreiten. (…) Das Internet verändert das Aussehen des organisierten Verbrechens, also die Art und Weise, in der die Kriminellen sich und die Durchführung ihrer Verbrechen organisieren. Die Internetkriminalität kommt ohne die Kontrolle über ein bestimmtes geografisches Gebiet aus, man benötigt also weniger Kontakte und braucht sich bei den Beziehungen zu anderen Kriminellen nicht mehr so stark auf Vertrauen und die Einhaltung der Disziplin zu verlassen. Und damit bedarf es dann auch keiner formalen Organisation mehr."[740] Eine solche neue Struktur wurde laut dem Autor kürzlich in Russland zerschlagen. Dabei haben organisierte Kriminelle, die jung und gebildet waren und denen jeweils bestimmte Aufgaben zugeteilt waren, von zu Hause aus relativ selbständig operiert.

Im zweiten Abschnitt wird dargestellt, wie kriminelle Organisationen zunehmend Jugendliche benutzen, um ihr kriminelles Konsumstreben zu befriedigen, da es ihnen zumeist am computertechnischen Fachwissen mangelt. „Kriminelle Organisationen werben Hacker und Skript-Kids an, die auf einen Nervenkitzel aus sind und beschaffen sich so die Expertise und die Werkzeuge, die sie zur Durchführung ´klassischer´ Verbrechen, wie z.B. Schutzgelderpressung, im Internet benötigen."[741] Der Autor bezeichnet dies als eine moderne Art der Kinderarbeit, vergleichbar mit den klassischen Hierarchien von Drogendealern und -schmugglern, bei denen skrupellose Bosse die Untergebenen, hier die Hacker und Script-Kiddies, zu immer größeren Risiken veranlassen. In diesem Zusammenhang zitiert der Autor Marc Rogers[742],

[738] Troxler 2005, S. 6.
[739] Ebd.
[740] Ebd., S. 7.
[741] Ebd., S. 8.
[742] Marc Rogers war Kriminalbeamter und ist nun außerordentlicher Professor in der Abteilung für Computertechnologie an der Purdue University, USA.

der der Meinung ist, dass kriminelle Organisationen die Gruppenanerkennung in der Hackerszene für sich ausnutzen, um dann im Rahmen einer Erpressung deren kriminelle Wünsche zu erfüllen: „Wir haben es mit mehreren Ebenen zu tun. Da sind zum einen die Jungs, die einen Virus schreiben, aber genau wissen, dass sie ihn nicht verbreiten dürfen, weil das verboten ist. Also überlassen sie die Verbreitung des Virus einem der Skript-Kids, von dem sie wissen, dass er sich in der Virenunterwelt wie ein großes Tier vorkommen wird, wenn er einen solchen Virus verbreitet. Sie wissen genau, dass einer dieser Neulinge nur auf eine solche Gelegenheit wartet.“ Dabei werden Hacker z.B. in Chaträumen von organisierten Banden angeworben, um gezielte DDoS-Attacken auszuführen oder spezielle Viren zu schreiben; über die eigentlich im Hintergrund laufenden kriminellen Operationen haben die Hacker wiederum keinen Überblick.[743]

Interessant ist zudem, dass Troxler eine gewisse Karriereleiter im Bereich der Computerkriminalität erkennt und sie wie folgt unterteilt: Script-Kiddies, Virusschreiber, Freizeit-Hacker, professionelle Hacker, Phisher[744] und Internetkriminelle auf Bestellung. Leider versäumt der Autor, den Werdegang zu begründen und darzulegen, wie eine solche Entwicklung entsteht.

Im dritten Abschnitt stellt Troxler dar, wie die organisierte Kriminalität vom Internet profitiert. Dabei vergleicht er vor allem Offline-Straftaten mit Online-Straftaten. Er vergleicht den Bankraub mit dem Hacking, den Kreditkartenbetrug mit Sniffer-Attacken, Einbrecher und Trickbetrüger mit Virenerstellern und Drogen schmuggelnde Teenager mit Script-Kiddies im Internet. Auf eine weitere Darstellung dieses Abschnitts wird verzichtet, da er keine weiter reichenden Erkenntnisse erbringt, als sie schon im ersten Teil dieser Arbeit dargestellt wurden.

Im letzten Abschnitt bietet Troxler einen Ausblick auf künftige Schwerpunkte der Computerkriminalität. Dabei sieht er einen Schwerpunkt in der Benutzung und Anmietung sog. Bot-

[743] So wurden im Fall des Internet-Hackerforums Liquid FX technisch mittelklassig versierte Jugendliche von der Hackergruppierung Liquid FX angeworben, die nach unzureichend gesicherten Computern suchen sollten. Die Hacker-Spezialisten von Liquid FX brachen sodann in die Systeme ein und modifizierten sie, damit andere dort Raubkopien von Software, Filmen und Musik lagern konnten. Parallel dazu betrieb die Organisation auch ein Bot-Netz, eine Flotte von rund 11.000 ferngesteuerten Rechnern, zu denen jedoch nur 619 deutsche Rechner gehörten. 344 Rechner waren davon unzureichend gesicherte Unternehmenscomputer. Im März 2004 durchsuchten 15 Polizeiteams 132 Wohnungen von Mitgliedern des Internet-Hackerforums Liquid FX. Insgesamt 126 Hacker wurden angeklagt. Die Ermittlungen ergaben, dass es sich bei Liquid FX um eine grenzenübergreifende Organisation handelte, der 476 Mitglieder aus 33 Ländern angehörten.

[744] Als Phisher bezeichnet Troxler Kriminelle, die über ein noch besseres Fachwissen als Hacker verfügen.

Netzwerke.[745] Daneben sieht er einen weiteren Schwerpunkt im Bereich des Cyber-Terrorismus. Es besteht seiner Ansicht eine wachsende Bedrohung durch Angriffe krimineller Hacker auf Infrastrukturen, die das Potenzial in sich bergen, Regierungsstellen oder Not- und Rettungsdienste lahm zu legen.

3.10 Zwischenfazit

In diesem Kapitel wurden unterschiedliche Motive, Aneignungsformen, Bedeutungsmuster und Sinnwelten von Hackern untersucht. Die Ausführungen zeigen, dass eine klare Abgrenzung kaum möglich ist. Empirische Studien über die Hackerszene sind kaum vorhanden und wenn, dann meist veraltet.[746] Dies liegt wohl nicht nur an der zum Teil mangelnden übergreifenden Fachkenntnis einiger Forscher. Der Begriff Hacker wird zudem bislang sehr unspezifisch und allgemein definiert, so dass viele Forscher keinen Ansatzpunkt für geeignete Studien finden können.

Die Ausführungen zeigen, dass anhand der individuellen Motivlagen, der Selbst- und Fremdwahrnehmung der genannten „Hackerkategorien“ oft eine „negative“ (und damit kriminologisch ggf. relevante) oder „positive“ (und damit eher nicht kriminologisch relevante) Einordnung stattfindet. Die politischen Hacker zeigen zwar ein delinquentes Verhalten, indem sie in ein System eindringen, ihre eigentliche Handlungsweise wird aber von positiven und letztlich durchaus auch gemeinnützigen Intentionen geleitet. Ob es mehr dem Bild eines Helfers oder eines Verräters ähnelt, wenn – seien sie auch durch ein Fehlverhalten herbeigeführte – Informationen über Sicherheitslücken in Systemen, EDV-Anlagen bekannt gemacht werden und so eine nachhaltige Entwicklung von Sicherheitstechniken z.B. für Server großer Unternehmen gewährleistet bzw. angestrengt wird, hängt ganz von der Sichtweise ab. Die Aufklärung ist jedoch zumindest hilfreich für jeden Computernutzer, da er so vor etwaigen Fallen gewarnt wird und die Möglichkeit erhält, sich wirksamer zu schützen. Cracker, Softwarecracker und Script-Kiddies sind zumindest aus der Sicht Dritter von schadhaften Intentionen geleitet. Eine

[745] Bot-Netze sind eine Sammlung von ferngesteuerten Computern, die für DDoS-Attacken o.ä. missbraucht werden können.
[746] Die meisten empirischen Studien sind technisch orientiert und zeigen Computerkriminalität und Hacker aus Sicht der Unternehmen. Sie beschreiben die unterschiedlichen Arten von Übergriffen und wie sich Unternehmen davor schützen können.

generelle Unterscheidung der Hackergruppen ist jedoch sehr schwierig, da es unterschiedliche Definitionen gibt.[747]

Festzustellen ist zudem, dass Hacker heute nicht mehr nur die ursprünglichen Programmierer sind, die es sich zur Aufgabe gemacht haben, mit Hilfe der Computertechnik die Welt mit Innovationen zu bereichern. Die Strukturen sind so vielfältig, dass die ursprünglichen Hacker nur einen kleinen Teil der heutigen Szene darstellen. Eine Kategorisierung einzelner Gruppen, die man mit den Begriffen Hacker und Cracker in Verbindung bringt, scheint für die Bewertung der Frage nach der Gefährlichkeit dieser für die Informationsgesellschaft weitaus besser geeignet als der Versuch einer Begriffsdefintion. Es zeigt sich aber auch hier, dass wohl eine stark individuelle und vom Einzelfall abhängige Beurteilung notwendig ist, um delinquente Personen eindeutig zuzuordnen. Es kann schließlich durchaus sein, dass ein Hacker, der intensive Aufklärungsarbeit leistet und damit zur Sicherheit unserer Informationsgesellschaft beiträgt, auf der anderen Seite ebenfalls ein aktives Mitglied einer Gruppe von „Softwarecrackern“ ist und sich auch hier intensiv beteiligt. Auch die Eigendarstellung der Szene variiert, so dass CCC-Hacker und amerikanische Hacker sich gegenseitig als Cracker bezeichnen. Diese Beispiele zeigen, dass eine Zugehörigkeit bzw. die Möglichkeit der Einordnung einer Person zu einer Hackerkategorie die Zugehörigkeit zu einer anderen Kategorie nicht notwendig ausschließen kann. Eine sich verändernde Karriere ist in diesem Zusammenhang ebenfalls denkbar. Das Verhalten kann sich durch Anreize wandeln, so dass aus einem ehemaligen Hacker schnell ein Cracker werden kann. Wie fließend die Übergänge sind und wie schnell ein echter Hacker doch kriminell werden kann, zeigt die Geschichte von Karl Koch, der mit dem sog. KGB-Hack Berühmtheit erlangte.[748] So wurde aus einem ursprünglich nichtkriminellen und mit der Hackerethik vertrauten Hacker jemand, der durch materielle Anreize verleitet wurde, an den KGB Informationen zu verkaufen. Selbst der Systemadministrator Clifford Stoll, der die KGB-Hacker jahrelang jagte, wird von anderen Autoren mit den Hackern selbst verglichen, da viele Ähnlichkeiten bezüglich der Obsession und Geduld der Vorgehensweisen

[747] Eine Möglichkeit wäre, nach der Schwere des Eingriffs zu gehen. Dies erscheint problematisch. Es gibt Übergriffe, bei denen Hacker nur kleine Scherzviren verschicken, die sich nach Tagen oder sogar Stunden selbst deaktivieren. Einige dringen in Systeme ein, nur um es zu schaffen, andere sehen sich zudem die vorhandenen Daten und die Inhalte an, andere kopieren Daten, andere verkaufen sie weiter, wieder andere manipulieren geringfügig Daten, und wieder andere zerstören alle Daten. Zum anderen könnte man nach der Gesinnung unterscheiden. Wie bereits gezeigt, gibt es jedoch die unterschiedlichsten Motive, die von Unwissenheit, Profitsucht über aufklärerische Gedanken bis hin zu Racheakten reichen. Zudem scheint es schwierig, Hacker einem bestimmten Lager zuzuordnen. Es gibt die Hacker, die sich privat formieren, z.B. der CCC; daneben müssen aber auch diejenigen, die für die Wirtschaft Daten ausspionieren, als solche bezeichnet werden. Ebenfalls wie sog. Script-Kiddies, denen wohl die Konsequenzen ihrer Handlungen noch mangels Reife nicht vollends bewusst sind.

[748] Stoll 2001.

und der Intentionen vorliegen.[749] Es zeigt sich, dass dem Problem der Hackerkriminalität schwer beizukommen ist, da niemand genau weiß, wer eigentlich zu dieser Gruppe gehört.

Festgehalten werden kann, dass es nur schwer eine positive Definition des Begriffs Hacker im herkömmlichen Sinn geben kann, da das Hacken in jeglicher Form zumindest das Überschreiten von Normen oder Regeln impliziert und ebenso mit verbotenen oder zumindest sozial oder ethisch problematischen Vorgehensweisen einhergeht, unabhängig davon, ob sie einen Straftatbestand darstellen. Somit kann ein Hacker ausschließlich anhand seiner außergewöhnlichen computertechnischen Fähigkeiten charakterisiert werden. Alle übrigen Faktoren wie Gesinnungen und Motive sind derart unterschiedlich, dass sie nicht zur Begriffsklärung dienen können, sondern nur zum Verständnis der Beweggründe und Motivlagen. Hacker sind aufgrund ihrer Leistungsorientierung ein Spiegel der Gesellschaft. Für Kinder und Jugendliche sind sie Idole und Vorbilder, denen nachgeeifert wird. Hieraus entsteht eine Art Leistungsdenken in Reinform, bei dem jeder Hacker versucht, der Beste zu werden. Auch wenn die eigenen Handlungen und die der Vorbilder zum Teil krimineller Art sind, so werden diese doch als Personen idealisiert.

Der Begriff Hackerszene und eben nicht der Bande oder Organisation ist jedoch meines Erachtens zutreffend. Hess und Scheerer führen dazu Folgendes aus: „Szenen entwickeln sich durch häufigen Kontakt von Personen, die von gleichen Interessen, Bedürfnissen und Vorlieben geleitet sind. Sie sind der lebensweltliche Raum, der die soziale Abstützung der eigenen Weltsicht und Lebensweise bietet. (…) Während es bei Szenen eher vage Kriterien der Zugehörigkeit gibt und auch die Beteiligten nicht immer in der Lage sind zu sagen, wer nun am Rande noch dazugehört und wer nicht, ist das bei Banden und Organisationen aller Art meist sehr viel klarer.“[750] Die Hackerszene beinhaltet einen Personenkreis, der sich aus unterschiedlichen Gründen rund um den Computer und das Internet sammelt, um Daten, Ideologien, eine eigene Sprache und sonstige Informationen zu teilen. Hacker können sich aktiv wie auch passiv, je nach Lust und Zeit, an der Szene beteiligen. Es gibt, mit Ausnahme solcher Organisationen wie dem CCC oder Teilen der Open-Source-Bewegungen, keine festen Mitgliedschaften.

[749] Gröndahl 2000, S. 75.
[750] Hess/Scheerer 2004, S. 82 f.

4. Die Entstehung der Hackerkriminalität nach der Self-Control Theory von Gottfredson und Hirschi

Im Folgenden soll anhand der General Theory of Crime (Self-Control Theory) von Michael R. Gottfredson und Travis Hirschi eine Erklärung für Computerkriminalität von Hackern gestartet werden. Zunächst wird die Self-Control Theory in ihren Grundzügen dargestellt. Es werden Kernaussagen der Theorie besprochen und auf die Hacker angewandt. Gottfredson und Hirschi stützen ihre Theorie auf empirische Studien anderer Autoren. Danach wird anhand der gewonnenen Erkenntnisse des dritten Teils und der einzelnen Theoriepunkte gezeigt, inwieweit die Theorie für eine Erklärung von Computerkriminalität geeignet ist.

4.1 Die Self-Control Theory in ihren wesentlichen Elementen

1990 haben die beiden amerikanischen Kriminologen Gottfredson und Hirschi ihr Buch „A General Theory of Crime“ vorgelegt, um eine allgemeine Theorie kriminellen Verhaltens zu entwerfen, die auf beliebige Delikte und Täter anwendbar sein soll und insofern sämtliche bislang vorliegenden Kriminalitätstheorien für obsolet erklärt.
Die General Theory of Crime von Gottfredson und Hirschi[751] hat mit der Veröffentlichung im Jahre 1990 bis zum heutigen Tage viel Interesse gefunden und Kontroversen aufgeworfen[752] und wird zum Teil als Meilenstein in der Kriminologie bezeichnet.[753] Gottfredson und Hirschi entfalten in ihrem Werk General Theory of Crime einen Ansatz der Erklärung abweichenden Verhaltens, der sich im Spannungsfeld zwischen so genannten „klassischen“ und „positivistischen“ Bereichen der Kriminologie bewegt. Sie kombiniert Aspekte der Sozialisation mit Situationsbedingungen. Diese Theorie ist ein Teil der kriminologischen Entwicklung, die die Gründe für Kriminalisierung in der Familie sucht.[754]
Gottfredson und Hirschi wollen mit der General Theory of Crime nicht nur Teilaspekte der Kriminalität erklären. Vielmehr beanspruchen sie, die Kriminalität in ihrer Gesamtheit erfasst zu haben und darüber hinaus neben verschiedenen Formen abweichenden Verhaltens ebenso auch konforme Verhaltensweisen erklären zu können. Der Bereich der Computerkriminalität und speziell die Handlungen von Hackern umfassen strafbare und nicht strafbare Handlungen, kriminelle und nicht kriminelle Bereiche, abweichende und nicht abweichende Handlungen,

[751] Gottfredson/Hirschi, A General Theory of Crime.
[752] Evans u.a. 1997, S. 476 mit weiteren Nachweisen.
[753] Akers 1998, S. 102 ff.
[754] Grasmick u.a. 1993, S. 5 mit weiteren Nachweisen.

sowie sozial verwerfliche und sozial gewünschte Handlungen. Viele Bereiche sind hierbei fließend und lassen sich nur schwer exakt eingrenzen. Eine Theorie, die sich auch mit nichtkriminellen Handlungen beschäftigt, wie Teilhandlungen der Hacker sie auch darstellen, scheint somit zur Erklärung sehr dienlich zu sein. Gerade aus diesem Grund könnte die Theorie geeignet sein, um Computerkriminalität zu erklären. Ein weiterer Grund für die Wahl dieser Theorie ist, dass viele Autoren Jugendliche als die eigentlichen Hacker ansehen. Da die Self-Control Theory auch Sozialisationsparameter mit einbezieht, die für Kinder und Jugendliche eine hohe Relevanz bei der Kriminalitätsentstehung haben, scheint diese Theorie geeignet, diesen Deliktbereich zu erklären. Als letzter Punkt trug zur Wahl dieser Theorie bei, dass die Autoren von der Relevanz der individuellen Motivation ausgehen. Die Rückbesinnung von der Ursachenzuschreibung externer Kausalitäten zur Handlungsmotivation des Individuums scheint gerade im Bereich der Hackerkriminalität mit ihren verschiedenen Motivationslagen eine geeignete Analysemöglichkeit zu bieten, um damit sozial abweichende Handlungen erklären zu können.

4.1.1 Social Bond Theory von Travis Hirschi

Die General Theory of Crime gilt als Weiterentwicklung der von Travis Hirschi im Jahre 1969 vorgestellten Social Bond Theory,[755] auch Theorie der sozialen Bindungen genannt. Sie erklärt Kriminalität mit der Schwächung oder dem Bruch der Bindungen, die ein Individuum zur Gesellschaft und ihren Gruppen besitzt.[756] Nach Travis Hirschi zerfällt die soziale Bindung in vier Elemente: „attachment, commitment, involvement and belief“. Unter attachment ist das emotionale Band zu Bezugspersonen gemeint, wodurch eine Art Zuneigung, Anhänglichkeit und Ergebenheit und wiederum eine ständige Verpflichtung entsteht, sich mit Rücksicht auf diese Personen konform zu verhalten.[757] Commitment, das rationelle Element der Theorie, entspricht dem Freudschen „Ich“. Dies bedeutet hierbei eine den konventionellen Zielen verpflichtete Lebensplanung, bei der Folgen des eigenen Handelns bedacht und auf diese Ziele bezogen werden. Die Bindungswirkung entsteht dadurch, dass man berücksichtigt, was man verlieren kann.[758] Als drittes Element nennt Travis Hirschi involvement, und meinte das Eingebundensein in konforme Aktivitäten. Wer beruflich und in seiner Freizeit viel ein-

[755] Hirschi 1969.
[756] Schneider 2001, S. 55 ff.
[757] Göppinger 1997 S. 112; Schneider 2001, S. 55 f.
[758] Göppinger 1997 S. 113; Schneider 2001, S. 56.

gebunden ist, hat keine Zeit, straffällig zu werden.[759] Belief als viertes Element beschreibt die innere Billigung und Anerkennung der moralischen Gültigkeit konventioneller Werte.[760]

4.1.2 Self-Control Theory

Die Self-Control Theory scheint auf den ersten Blick dem Bedürfnis nach Sparsamkeit wissenschaftlicher Erklärung nachzukommen. Die Theorie fokussiert das Persönlichkeitsmerkmal „Self-Control" und verweist zur Entstehung auf die Sozialisationsbedingungen vor allem in der Familie.[761] Die Variable Self-Control steht dabei in enger Verbindung mit der zweiten von den Autoren eingeführten Variable „Crime Opportunity". Self-Control und Crime-Opportunity zusammen erklären im Sinne der Self-Control Theory Kriminalitätsformen und ihre Entstehung.[762]

Self-Control

Self-Control ist dabei der zentrale Ausgangspunkt von Gottfredson und Hirschi. Sie erklären in ihrem Werk auch den Entstehungshintergrund für das Konstrukt Self-Control, der in dieser Arbeit vor allem bei der Anwendung der Theorie auf die Hacker und ihre verschiedenen Motivationslagen relevant wird. Eine Definition von Self-Control liefern Gottfredson und Hirschi in ihrem ersten Werk leider nicht, ein Mangel, der von einigen Autoren kritisiert wird.[763] Erst vier Jahre nach der Veröffentlichung ihrer Theorie liefern Gottfredson und Hirschi eine Definition von Self-Control:[764]

"The theory, simply stated, is this: Criminal acts are a subset of acts in which the actor ignores the long-term negative consequences that flow from the act itself, from the social or familial environment, or from the state. All acts that share this feature, including criminal acts, are therefore likely to be engaged in by individuals unusually sensitive to immediate pleasure and insensitive to long-term consequences. The immediacy of the benefits of crime implies that they are obvious to the actor, that no special skill or learning is required. The property of individuals that explains variation in the likelihood of engaging in such acts we call self-control."

[759] Göppinger 1997 S. 113; Schneider 2001, S. 56.
[760] Ebd.
[761] Gottfredson/Hirschi 1990 S. 94ff.
[762] Paternoster/Brame 1997 S. 50.
[763] Lamnek 1997, S. 165.
[764] Gottfredson/Hirschi 1994, S. 2 ff.

Kriminelle Handlungen sind eine Untermenge von Handlungen, in denen der Handelnde die langfristigen negativen Konsequenzen, die aus der Handlung selbst, aus der sozialen oder familiären Umgebung oder vom Staat entstehen, ignoriert.[765] Alle Handlungen, auch die kriminellen, teilen den Wesenszug von Personen, ungewöhnlich sensibel auf sofortige Bedürfnisse und eher unsensibel auf verzögerte Bedürfnisse zu reagieren. Die Eigenschaft von Personen, welche die unterschiedliche Wahrscheinlichkeit der Begehung solcher Handlungen erklärt, nennen Gottfredson und Hirschi Self-Control.[766] Besitzt eine Person ein niedriges Maß an Self-Control, so besteht die Neigung zur sofortigen Bedürfnisbefriedigung. Diesbezüglich werden negative familiäre und soziale Konsequenzen ignoriert. Besitzt eine Person dagegen ein hohes Maß an Self-Control, so erliegt sie nicht sofortigen Bedürfnissen, sondern erarbeitet sich unter Miteinbeziehung der sozialen und familiären Folgen verzögerte Bedürfnisbefriedigungen.

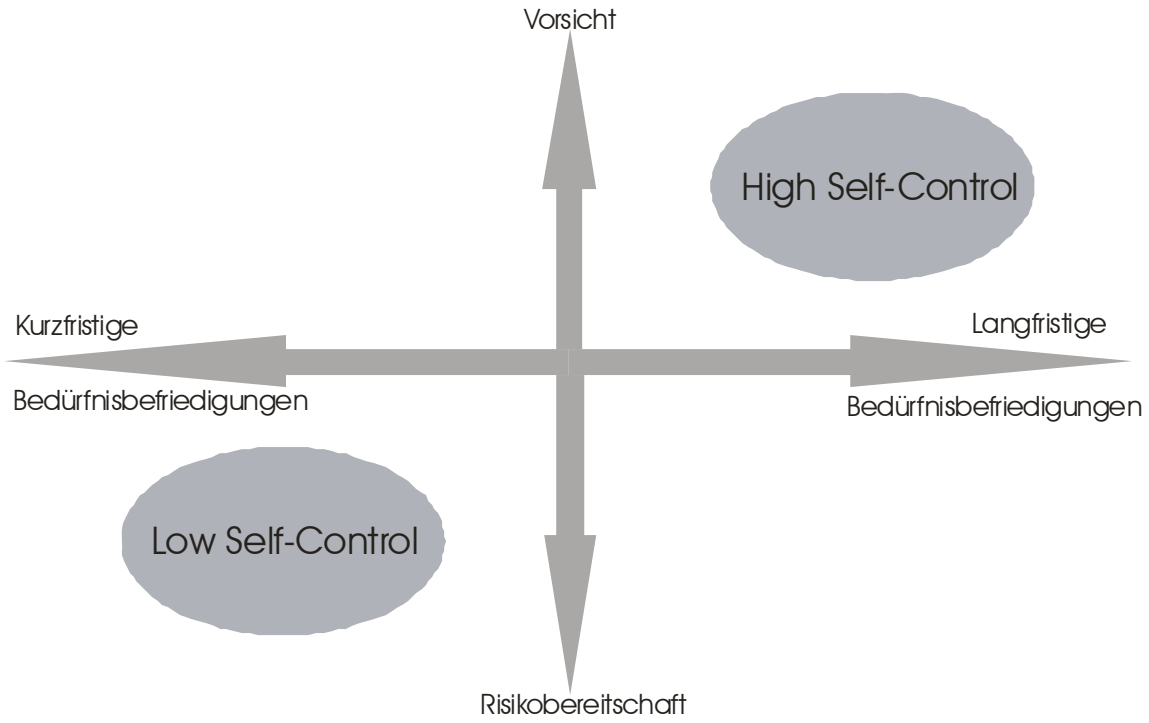
Kriminelles Verhalten ist somit die Folge niedriger Selbstkontrolle der Täter, die dazu führt, dass Kriminelle bei ihren Handlungsentscheidungen grundsätzlich dazu neigen, eher kurzfristig erreichbare Bedürfnisbefriedigungen in den Blick zu nehmen und längerfristigen Bedürfnisse weniger Beachtung zu schenken. Kriminelle unterscheiden sich dabei von Nichtkriminellen in dem Ausmaß, in dem sie Versuchungen mit möglichst kurzfristiger Bedürfnisbefriedigung erliegen.[767] Dieses Merkmal von Personen dient als zentrales Erklärungsprinzip krimineller Verhaltensweisen. Dabei sehen Gottfredson und Hirschi eine solche Neigung nicht nur bei kriminellen Handlungen, sondern ebenso bei allen übrigen den kriminellen Handlungen verwandten Verhaltensweisen wie Rauchen, übermäßigem Alkoholkonsum oder riskanten Handlungen.

Personen mit einer in Bezug auf Self-Control niedrigen Merkmalsausprägung zeichnen sich dadurch aus, dass die kurzfristige Bedürfnisbefriedigung in sehr hohem Maße positiv bewertet wird, während die langfristigen negativen Konsequenzen eines Verhaltens nicht angemessen eingeschätzt werden. Aus diesem Grund neigen Personen mit einer geringen Self-Control dazu, solche Verhaltensweisen zu wählen, die eine kurzfristige Realisierung von „pleasure“ implizieren, auch wenn mit diesen Handlungen langfristig „pain“ verbunden ist. Dies wird

[765] Evans u.a. 1997, S. 475ff.
[766] Gottfredson/Hirschi 1994, S. 1 ff.
[767] Lamnek 1997, S. 124.

von den Autoren als Low oder High Self-Control bezeichnet. Ist Self-Control erst einmal geformt, gehen die Autoren davon aus, dass es relativ stabil im weiteren Lebensverlauf bleibt.[768]

Grafische Lokalisierung von Self-Control:



Quelle: eigene Darstellung

Im Bereich der Ursachen sehen Gottfredson & Hirschi die Entstehung von Self-Control in einem Zusammenspiel angeborener Neigungen eines Kindes und seiner Erziehung.[769] Nach Gottfredson und Hirschi haben Kinder die angeborene Neigung, mehr oder weniger Self-Control zu bilden.[770] Die Autoren verneinen jedoch ausdrücklich, dass es den geborenen Verbrecher oder ein Gen für Kriminalität gebe. Jedoch sehen sie Unterschiede in der Herausbildung des Persönlichkeitsmerkmals Self-Control. Ihrer Ansicht nach sei es jedoch möglich, durch eine effektive Sozialisation diese individuelle Eigenschaft zu beseitigen. Ihrer Auffassung zufolge liegt in der Erziehung der Grundstein zur Vermittlung von High Self-Control. Eine effektive Erziehung setze dabei am Prinzip der Kontrolle an, mangelhafte elterliche Kontrolle korreliere stark mit delinquentem Verhalten. Die Autoren sehen die Hauptursachen für

[768] Paternoster/Brame 1997, S. 52.
[769] Lamnek 1997, S.146.
[770] Gottfredson/Hirschi 1990, S. 47 ff.; Gottfredson/Hirschi 1994, S. 52 ff.

die Herausbildung von Self-Control in der primären Sozialisation verortet.[771] Dabei beziehen sie sich hauptsächlich auf Forschungsergebnisse von Glueck/Glueck, McCord/McCord und Robins, die korrelierende familiäre Faktoren zur Delinquenz festgestellt haben.[772] Positive Lern- oder Kulturprozesse seien ihrer Ansicht nach nicht geeignet zur Erklärung von Kriminalität. Aspekte des elterlichen Erziehungsstils wurden als wichtigste Bedingungen für abweichendes Verhalten herausgearbeitet, wobei Glueck/Glueck den Anspruch erheben, schon im Alter von sechs Jahren Prognosen für abweichendes Verhalten stellen zu können. Inspiriert durch diese Ergebnisse sehen Gottfredson und Hirschi ausschließlich das elterliche Erziehungsverhalten in den ersten sechs bis acht Jahren als entscheidenden Faktor für die Herausbildung von Self-Control.[773]

Ist High Self-Control oder Low Self-Control erst einmal in den ersten acht Jahren herausgebildet, so erweist es sich als erstaunlich stabil über die weitere Lebensspanne.[774] Um diese These zu stützen, berufen sich Gottfredson und Hirschi u. a. auf Forschungsergebnisse von Robins.[775] Robins untersuchte verhaltensauffällige Kinder und verglich diese mit Kontrollgruppen. Man stellte dabei fest, dass Personen, die im Kindesalter auffällig waren, auch später abweichende Verhaltensweisen zeigten. Sie hatten häufiger Jobwechsel, waren häufiger arbeitslos, hatten kürzere Beziehungen, hatten delinquente Freunde und neigten mehr zum exzessiven Alkoholkonsum.[776] Gottfredson und Hirschi sehen hierin eine Bestätigung ihrer Annahme, dass Self-Control relativ stabil bleibt, wenn es sich herausgebildet hat. Ist einmal eine Neigung im Leben eines Kindes herausgebildet, eher kurzfristige und sofortige Bedürfnisbefriedigung vorzuziehen, so führt nach Meinung der Autoren diese Neigung im Erwachsenenalter immer wieder zu abweichenden und analogen Verhaltensweisen.[777]

Ausschließlich effektive Erziehung in den ersten acht Jahren führe zu High Self-Control, die in erster Linie auf Kontrolle beruhe. Nur die Familie könne Kriminalität vorbeugen; erfülle sie ihre Aufgaben nicht, würde niemand diese Aufgabe nachträglich erfüllen können. Effektiv i.S.v. High Self-Control ist das elterliche Beziehungsverhalten nur dann, wenn folgende drei Verhaltensweisen bei den Eltern gegeben sind: Beaufsichtigung, Erkennen und Bestrafung devianten Verhaltens.

---

[771] Geis 2000, S. 48; Arneklev/Grasmick/Bursit 1999, S. 307 f.; Gottfredson/Hirschi 1990, S. 47 ff., 94 ff.; Gottfredson/ Hirschi 1994, S. 52 ff.
[772] Gottfredson/Hirschi 1990, S. 94 ff.
[773] Gottfredson/ Hirschi 1994, 52 ff.; Paternoster/Brame 1997, S. 51 f.; Hayslett-McCall/Bennard 2002, S. 6.
[774] Gottfredson/Hirschi 1990, S. 108; Polakowsky 1994, S. 44.
[775] Robins 1966, S. 42 ff.
[776] Ebd.
[777] Gottfredson/Hirschi 1990, S. 94; Gottfredson/ Hirschi 1994, S. 51.

Erstens muss das Verhalten des Kindes überwacht werden. Gestützt auf Erkenntnisse von Glueck/Glueck[778], McCord[779] und Travis Hirschi sehen Gottfredson und Hirschi die Beaufsichtigung des kindlichen Verhaltens durch die Eltern als wichtigen Vorhersagefaktor für die Bildung von Self-Control, da alle weiteren Faktoren hierauf aufbauen. Durch die Beaufsichtigung soll das Kind lernen, spontane und unmittelbare Befriedigungswünsche zu unterdrücken, verzögerte oder spätere Belohnung zu erkennen. Es sollen Anliegen anderer in das eigene Handeln einbezogen und eine größere Bereitwilligkeit erzielt werden, Einschränkungen der eigenen Aktivitäten hinzunehmen.

Zweitens müssen Eltern deviantes Verhalten wahrnehmen können, wenn es sich vollzieht. Können Eltern deviantes Verhalten nicht erkennen, können sie es auch nicht ahnden. So erlauben einige Eltern ihren Kindern ohne Einschränkungen extensives Fernsehen, achten nicht auf die vollständige Bearbeitung der Hausaufgaben, lassen sie rauchen und verhindern nicht die Anwendung von Gewalt gegenüber Gleichaltrigen. Wenn Eltern diese Verhaltensweisen also nicht als deviant einstufen, werden sie diese auch nicht ahnden.[780] Dieses ist für die Autoren auch der Grund dafür, dass die Kriminalitätsrate von Kindern aus einem kriminellen Elternhaus ebenfalls erhöht ist. Eltern mit mangelnder Self-Control fehlt die Möglichkeit, ihren Kindern adäquat Self-Control zu vermitteln.[781] Hierbei stützen die Autoren ihre Erkenntnisse auf Forschungsarbeiten von Donald West und David Farrington.[782] Auch wenn diese Autoren genetische Voraussetzungen für Delinquenz ablehnen, so akzeptieren sie dennoch, dass abweichendes Verhalten von Generation zu Generation offensichtlich weitergegeben wird. Dieses sehen sie vor allem in der fehlenden Möglichkeit delinquenter Eltern, abweichendes Verhalten ihrer Kinder zu erkennen und ihnen eine angemessene Sozialisation mitzugeben.[783] Eltern, die selbst einen Mangel an Selbstkontrolle aufweisen, werden nicht in der Lage sein, ihren Kindern Selbstkontrolle zu vermitteln.

Und drittens müssen die Eltern auftretendes deviantes Verhalten in angemessener Weise ahnden. Eine effektive Bestrafung ist nach Gottfredson und Hirschi die logische Konsequenz, die auf ein kindliches Fehlverhalten folgen muss. Sie vertreten die Auffassung, dass im Fall einer

[778] Glueck/Glueck 1930, S.1950 ff.
[779] McCord 1979, S.1477 ff.
[780] Gottfredson/Hirschi 1990, S. 99, 101.
[781] Gottfredson/Hirschi 1990, S. 100.
[782] West/Farrington 1993, S.109 ff.
[783] Gottfredson/Hirschi 1990, S. 100.

Bestrafung negativer Verhaltensformen spätere Delinquenz unwahrscheinlicher werde. Welche Bestrafung für welches Fehlverhalten als effektiv zu bewerten ist, wird von den Autoren leider nicht beschrieben. Als einzigen Hinweis nennen sie Erkenntnisse von Glueck/Glueck und McCord/McCord, die zu dem Ergebnis kommen, dass Eltern zu leicht oder zu hart bestrafen.[784] Für Gottfredson und Hirschi sollen Sanktionen nicht zu hart, aber auch nicht zu weich, sondern „angemessen" sein, ohne dass sie aber Angemessenheit konkret definieren.

Es lässt sich festhalten, dass die General Theory of Crime die Ursachen für die Entstehung von High oder Low Self-Control in der primären Sozialisation verortet. Die Sorge um das Kind, seine Beaufsichtigung, das Erkennen und das effektive Bestrafen abweichenden Verhaltens führt zur Herausbildung von High Self-Control. Dies hat zur Folge, dass grundsätzlich eine Bereitschaft entsteht, auf schnelle Formen der Bedürfnisbefriedigung zu verzichten und langfristige Konsequenzen mit in die Handlungsentscheidung einzubeziehen. Sei einmal die Neigung herausgebildet, eher die Befriedigung von kurzfristigen Bedürfnissen vorzuziehen, und im „Hier und Jetzt" zu leben, so führe diese Tendenz später zu einer höheren Wahrscheinlichkeit, dass delinquente und analoge Verhaltensweisen begangen werden. Aus der Sicht von Gottfredson und Hirschi ist Verbrechen keine automatische Konsequenz von Low Self-Control, sondern diese erhöht lediglich die Wahrscheinlichkeit einer Tatbegehung.[785]

Crime Opportunity

Kriminalität ist nach Gottfredson und Hirschi nicht notwendige Folge von geringer Selbstkontrolle, diese ist jedoch eine notwendige Voraussetzung für Delinquenz. Hinzu kommen müssen vor allem situative Variablen: Crime Opportunities. Gottfredson und Hirschi sehen Self-Control und Crime Opportunity grundsätzlich als voneinander nicht unabhängige Variablen an. Gelegenheiten definieren die Autoren hierbei in Anlehnung an die Routine-Activity Theorie (RA-Theorie) von Cohen und Felson:[786]

„To begin, we take the conditions necessary for crimes in general as commonly stated in opportunity theory. For example, in the version advanced by Lawrence Cohen und Marcus Felson (1979), crime requires a motivated offender, the absence of a capable guardian, and a suitable target. Extention or modification of definitions of crime must beginn with one or an-

[784] Ebd.
[785] Gottfredson/Hirschi 1990, S. 91.
[786] Gottfredson/Hirschi 1990, S. 22 ff.; Gottfredson/Hirschi 1994, S. 5, 166 ff.; Eifler 1997, S. 15 ff.; Cohen/Felson 1979, 588 ff.

other of these three elements. Normally, one would think that theories interested in the offender would concentrate on the first element. Indeed most theories of criminality take the second and third elements irrelevant and develop accounts of offender motivation. In fact, in our view, this is the fundamental mistake of modern theory. If we begin to construct our picture of the offender after first understanding the role of guardians and targets, he does not resemble the picture painted by current theories of criminality."[787]

Im Zentrum der Routine-Activity-Theorie steht, dass das Viktimisierungsrisiko mit den alltäglichen Mustern der Lebensführung von Personen zusammenhängt. Der Begriff Routineaktivitäten charakterisiert dabei diejenigen Handlungen, die Personen regelmäßig zum Zwecke der Existenzsicherung ausüben.[788] Die RA-Theorie geht von alltäglichen Lebensführungsarten bestimmter Bevölkerungsgruppen aus, die mit dem Kriminalitätsaufkommen in Verbindung gebracht werden. Routineaktivitäten der Arbeit, des Spiels und der Freizeit ergeben durch ihre raumzeitliche Verteilung unterschiedliche Wahrscheinlichkeiten für bestimmte Formen des strafrechtlich relevanten Verhaltens zu bestimmten Zeiten an bestimmten Orten.[789] Sie zeigt, dass Kriminalität nicht mit biologischen, psychologischen oder ökonomischen Faktoren zusammenhängt, sondern allein mit der Situationsveränderung, weshalb sich Cohen und Felson hauptsächlich mit Veränderungen in der Gesellschaft und ihrer Desorganisation beschäftigen.[790]

Die Routine-Activity-Theorie verknüpft drei Elemente: einen potenziellen Täter (likely offender), ein Ziel bzw. Objekt (suitable target) und die Abwesenheit von Kontrollen und Kontrolleuren (guardian).[791] Fehlt eines dieser Elemente, kommt es nach Cohen und Felson nicht zur Straftat.[792] Wenn alle drei Elemente anwesend sind, dann erhöhe sich die Wahrscheinlichkeit für eine Verbrechensbegehung. Sie argumentieren, dass die Kriminalitätsrate zur Anzahl der Zielobjekte und der Abwesenheit von Kontrollpersonen steige.[793] In Übereinstimmung mit der Routine-Activity Theorie von Cohen und Felson betrachten Gottfredson und Hirschi eine Gelegenheit als eine Situation, in der ein motivierter Täter die Möglichkeit hat, durch kriminelles oder äquivalentes Verhalten kurzfristige Bedürfnisse zu befriedigen.[794] Gottfredson und

[787] Gottfredson/Hirschi 1990, S.24.
[788] Eifler 1999, S. 3.
[789] Eisenberg 2005, S. 68.
[790] http://home.attbi.com/~ddemelo/crime/crimetheory.html (zuletzt eingesehen am 15.11.2004).
[791] Cohen/Felson 1979, S. 589; Karstedt/Greve 1996, S. 180.
[792] Eisenberg 2005, S. 68.
[793] http://www.socsci.umn.edu/~uggen/mark.txt (zuletzt eingesehen am 15.11.2004).
[794] Eifler 1998, S. 96 f.

Hirschi sehen die Verfügbarkeit von Zielobjekten und die Abwesenheit von Kontrollinstanzen als notwendige Voraussetzung zur Kriminalitätsentstehung. Die Entstehung der Motivation eines potenziellen Täters definieren Gottfredson und Hirschi jedoch anders als Cohen und Felson.

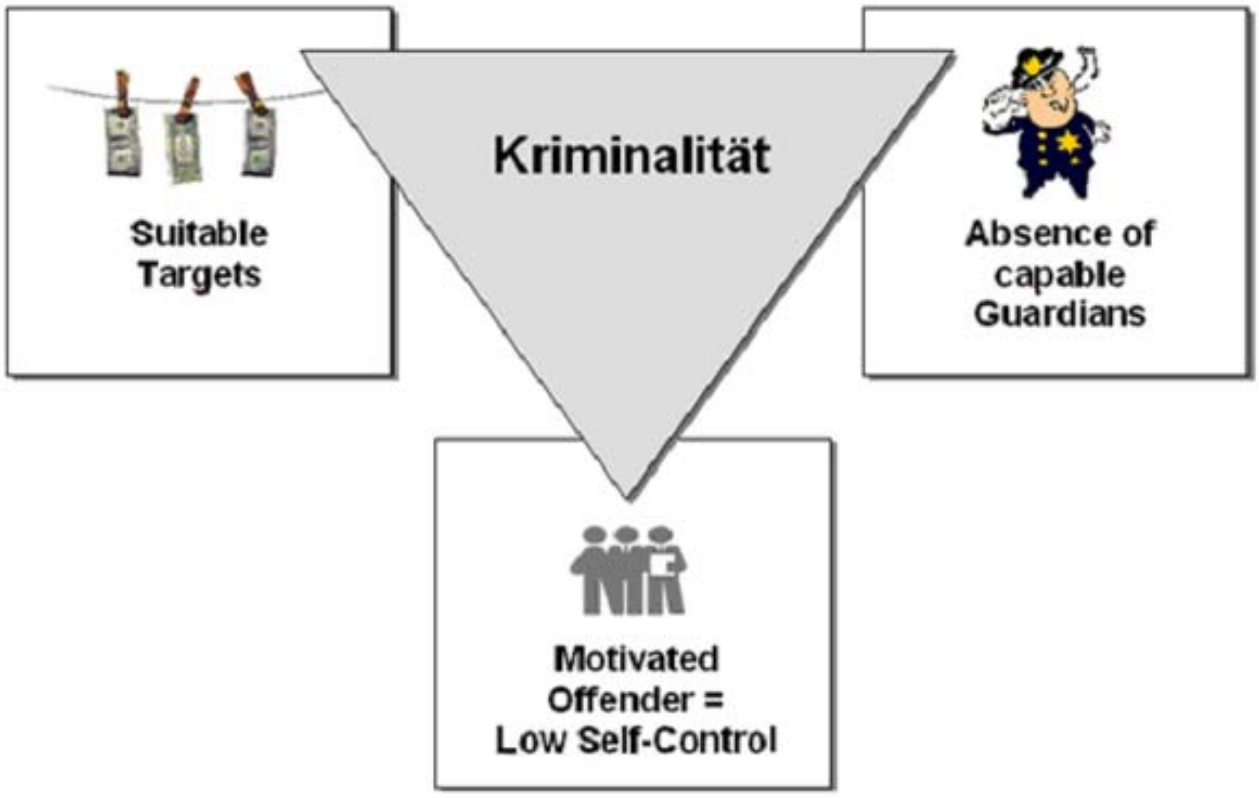
Die Motivation des Täters entsteht nach Cohen und Felson durch das Erleben von Deprivation, die wiederum durch Arbeitslosigkeit, Drogenkonsum, Verarmung, niedrige Bildung, kriminelle Familien und Protest gegen die Gesellschaft entstehe.[795] Gottfredson und Hirschi übernehmen Deprivation nicht als Entstehungsgrund für die Delinquenz des Täters. Sie sehen Arbeitslosigkeit, Drogenkonsum und niedrigen Bildungsstand als Ausläufer von mangelnden individuellen Eigenschaften und versuchen die Stärke der Motivation für Delinquenz gerade nicht mit externen Faktoren und der damit zum Teil erlebten Deprivation zu erklären. Die Self-Control Theory sieht gegenüber der Routine-Activity Theorie einen Akteur als dann motiviert, wenn er eine geringe Ausprägung in Bezug auf das Merkmal Self-Control aufweist.[796] Die Motivation des Täters hängt von der Stärke von Self-Control ab. Die Motivation, kriminellen oder analogen Verhaltensweisen nachzugehen, ist somit umso höher, je schwächer das Merkmal Self-Control ausgebildet ist.

Die Self-Control Theory sieht drei wesentliche Elemente für die Entstehung von Kriminalität an:

1. Low Self-Control
2. ein attraktives Ziel
3. die Abwesenheit von Kontrollinstanzen.

[795] Clarke/Felson 1993, S. 21.
[796] Eifler 1998, S. 96.

Grafische Darstellung der Self-Control Theory:



Quelle: eigene Darstellung

Ziel dieser Arbeit soll nicht allein die kritisch-theoretische Auseinandersetzung mit einer Theorie sein, sondern vor allem die Betrachtung der Computerkriminalität, im Speziellen der Hackerszene, und der Versuch einer Erklärung hierfür. Trotzdem sollen einige ausgewählte und häufig zitierte Kritikpunkte an dieser Stelle erwähnt werden.

Die Self-Control Theory hat seit ihrer Veröffentlichung einen erheblichen Nachhall in der kriminologischen Diskussion erfahren.[797] Gegenstand der Forschungen sind allerdings zumeist nicht Untersuchungen des Ansatzes insgesamt; vielmehr werden Teilaspekte in den Mittelpunkt der jeweiligen Untersuchung gestellt. Neben kriminellen Verhaltensweisen untersuchten viele Studien auch unvorsichtige Verhaltensweisen wie das Rauchen oder den Alkoholkonsum. Als ein wichtiges Ergebnis stellt sich in diesem Zusammenhang die Erkenntnis dar, dass die Annahme einer direkten Beziehung zwischen Self-Control und verschiedenen Formen abweichenden und analogen Verhaltensweisen im Allgemeinen Unterstützung gefunden hat.

[797] Arneklev u.a. 1993; Bartusch u.a. 1997; Lilly u.a. 1995; Paternoster/Brame 1997; Pratt/Cullen 2000; Paternoster/Brame 2000.

Die am meisten zitierte und gewichtigste Kritik ist wohl der Vorwurf der Tautologie,[798] da die Variable Low Self-Control nicht unabhängig von dem Verhalten erhoben werde, das sie vorhersagen soll:

"Low self-control explains both the stability and the versatility of crime. The testability of this explanation is put into question, however, by the fact that G&H do not define self-control separately from the propensity to commit crimes. G&H use 'low self-control' and 'high self-control' simply as labels for this differential propensity to commit crime. (...) In the past they have attached a different label to it – criminality. But they now reject criminality and other terms such as conscience and antisocial personality in favor of self-control (although they continue to use criminality as synonymous with low self-control). Thus, it would appear to be tautological to explain the propensity to commit crime by low self-control. They are one and the same, and such assertions about them are true by definition. The assertion means that low self-control causes low self-control."[799]

Ein Vorwurf, der von Gottfredson und Hirschi überraschenderweise als Kompliment gesehen wird. Aus ihrer Sicht ist der Vorwurf der Tautologie das Resultat einer folgerichtigen und konsequenten Erklärung:

„Even more curious is the charge that our theory is tautological (Akers 1991). In our view, the charge of tautology is in fact a compliment, an assertion that we followed the path of logic in producing an internally consistent result. Indeed, this is what we set out to do. We started with a conception of crime, and from it attempted to derive a conception of the offender. As a result, there should be strict definitional consistency between our image of the actor and our image of the act. What distinguishes our theory from many criminological theories is that we begin with the act, whereas they normally begin with the actor. Theories that start from the causes of crime – for example, economic deprivation – eventually define crime as a response to the causes they invoke. Thus, a theory that sees economic deprivation as the cause of crime will by definition see crime as an attempt to remedy economic deprivation, making the connection between cause and effect tautological. What makes our theory peculiarly vulnerable to complaints about tautology is that we explicitly show the logical connections between our conception of the actor and the act, whereas many theorists leave this task to those interpreting or testing their theory, but again we are not impressed that we are unusual in this regard. One more example: Sutherland's theory of differential association says that offenders have

[798] Geis 2000, S. 39.
[799] Akers 1991, S. 203 ff.

peculiar skills and attitudes toward crime learned from their subcultures. Crime is thus a reflection of those skills and attitudes. In this theory too the connection between the image of the offender and the image of crime (both require particular skills and attitudes) is tautological."[800]

Auch wenn Gottfredson und Hirschi den Vorwurf der Tautologie reduziert haben, folgen einige andere Autoren ihren Schlussfolgerungen bis heute nicht. Um dem Vorwurf der Tautologie trotzdem zu begegnen, suchten die Autoren nach Möglichkeiten, Self-Control unabhängig von dem zu erklärenden Verhalten zu begreifen. Einige Autoren erfassen deshalb Self-Control anhand von Skalen, die in Anlehnung an die im Rahmen der Theorie formulierte Definition dieses Attributs gestaltet sind.[801] Zu diesem Zweck wurden Items formuliert, die jeweils einzelne Aspekte des Merkmals Self-Control abbilden sollten. Diese Items werden zumeist in sechs Komponenten eingeteilt: „Impulsivity, Simple Task, Risk-Seeking, Physical Activities, Self-Centered und Temper".[802] Dadurch wurde eine grundsätzlich unabhängige Art der Erfassung von Self-Control und dem in Frage stehenden Verhalten erreicht, wodurch das Problem der Tautologie entkräftet wurde. Jedoch entstand in diesem Zusammenhang ein neues Problem. Es stellte sich die Frage, ob sich die sechs verschiedenen Komponenten zu einem eindimensonalen Konstrukt zusammenfassen lassen oder ob sie eher ein mehrdimensionales Konstrukt von Self-Control darstellen. Da diese Erwägungen rein theoretischer Art und in dieser Arbeit ohne Bedeutung sind, wird auf weitere Erwägungen hierzu verzichtet.

Die Annahme, dass Self-Control hinsichtlich seiner Ausprägung auf strukturelle und prozessuale Aspekte der primären Sozialisation zurückzuführen ist und diese, einmal entstanden, über die weitere Lebensspanne stabil bleiben, hat ebenfalls Befürwortung und Kritik gleichermaßen hervorgerufen. Auch hier zeigen die Ergebnisse vorliegender Studien ein uneinheitliches Bild.[803] Einige Autoren befürworten Gottfredson und Hirschis Gedanken, andere sehen zwar Kontinuitäten im kindlichen Problemverhalten und im abweichenden Verhalten im Erwachsenenalter, jedoch erkennen sie auch, dass Verhaltensauffälligkeiten im Kindesalter auf andere Faktoren zurückzuführen sind als Verhaltensauffälligkeiten derselben Personen im Erwachsenenalter.

[800] Gottfredson/Hirschi 1994, S. 8.
[801] Arneklev/Grasmick/Bursit 1999; La Grange/Silverman 1999; Bartusch u.a. 1997; Polakowsky 1994.
[802] Arneklev/Grasmick/Bursit 1999, S. 315 ff.
[803] Geis 2000; Burton u.a. 1999; Bartusch u.a. 1997; Evans u.a. 1997.

Daneben wird an der Self-Control Theory kritisiert, sie sei nicht wertfrei, sondern Ausdruck einer konservativen Gesinnung, die zudem die Verantwortung für soziale Notlagen den von diesen Notlagen betroffenen Personen zuschreibt.[804] Eine große Leistung der Self-Control Theory ist jedoch die Rückbesinnung zur Analyse der Motive für Kriminalität.[805] Allerdings muss ebenfalls zur Entlastung von Gottfredson und Hirschi erwähnt werden, dass die meisten empirischen Studien sich darauf beschränken, Self-Control zu analysieren, dabei aber die Gelegenheiten außen vor lassen. Gottfredson und Hirschi sehen Gelegenheiten aber als einen entscheidenden Faktor an, der in Wechselwirkung zu Self-Control steht. Studien, die einen wichtigen Teilaspekt der Self-Control Theory unberücksichtigt lassen, verfälschen das Ergebnis und spiegeln nicht unbedingt den Wahrheitsgehalt dieser Theorie wider:
„Not only self-control, but also opportunity to engage in crime, was an important element in the general theory. Most tests of the general theory did not include a measure of criminal opportunity."[806]

Insgesamt lässt sich feststellen, dass viele Befürworter, aber auch viele Gegner dieser neuen Theorie existieren und somit ein sehr uneinheitliches Bild über die Self-Control Theory besteht.

4.1.3 Gemeinsamkeiten und Unterschiede der Self-Control Theory und der Social Bond Theory

Einige Autoren sind der Meinung, dass die Self-Control Theory sich signifikant von der Social Bond Theory unterscheide. Dies mag im Ansatz stimmen, da beide Theorien unterschiedliche Ansatzpunkte aufweisen. Jedoch muss auch gezeigt werden, dass einige Gemeinsamkeiten bestehen, die verdeutlichen, aus welchen Grundgedanken die Erkenntnisse stammen und das Verständnis der Self-Control Theory damit erleichtern.

Die General Theory of Crime hat mit der Theorie der sozialen Bindungen einige Gemeinsamkeiten, besitzt aber auch wesentliche neue und von ihr abweichende Gedanken. Beide Theorien sehen Sozialisation als einen wichtigen Aspekt zur Erklärung von Kriminalität an und setzen ihre Schwerpunkte in den Bereich der elterlichen und schulischen Erziehung.[807]

[804] Lamnek 1997, S. 162 ff.
[805] Fattah 1997, S. 267 f.
[806] Burton u.a. 1999, S. 48 f.
[807] Polakowsky 1994, S. 43.

Gottfredson und Hirschi führen zudem aus, dass Self-Control soziale Konsequenzen mit sich führt, die sich u.a. auch darin äußern, wie Menschen soziale Bindungen zu anderen eingehen.[808]

Weiterhin entspricht der Bindungsebene attachment, dass Menschen mit hoher Selbstkontrolle von der Begehung krimineller Handlungen deshalb abgehalten werden, weil sie es als eine Verpflichtung ansehen, Handlungen zu unterlassen, die ihren Bezugspersonen wie Familie und Freunde missfallen könnten.[809] Das Gegenstück zu der „Hier-und-Jetzt"-Orientierung, die mit geringer Selbstkontrolle einhergeht, ist eine zielgerichtete und an den Folgen des eigenen Handelns orientierte Lebensplanung, wie sie etwa im commitment zum Ausdruck kommt.[810]

Unterschiedlich sind jedoch bei beiden Theorien die Ausgangspunkte, mit denen Kriminalität erklärt wird. Die Theorie der sozialen Bindungen spricht von vier Elementen, aus denen sich ergibt, dass eine Person sich sozial konform verhält. Ausgangspunkt der General Theory of Crime ist allein Self-Control. Erst durch die Ausprägung von Self-Control ergibt sich, ob eine Person soziale Bindungen eingehen kann und ob sie längerfristige Ziele in ihre Lebensplanung mit einbezieht.[811] Man könnte somit sagen, dass die General Theory of Crime abstrakter gestaltet ist als die Theorie der sozialen Bindungen.[812] Man könnte sie jedoch auch in vielen Bereichen als Kehrseite der anderen sehen. Nach der Theorie der sozialen Bindungen beeinflussen sich Peers[813] durch die Art der Bindungen und die Art der Beschäftigung gegenseitig. Nach Gottfredson und Hirschi finden sich Jugendliche mit ähnlicher Ausprägung von Self-Control in solchen Gruppen. Weiterhin bezieht die General Theorie of Crime nicht nur kriminelle Handlungen ein, sondern versucht mit Self-Control jegliche Art, kriminelle und analoge, zu erklären. Unter Hinzunahme von Gelegenheitsstrukturen bringt die General Theory of Crime zudem einen ganz neuen Aspekt hinein, der in der Theorie der sozialen Bindungen nicht enthalten ist.

---

[808] Evans u.a. 1997, S. 476; Gottfredson/ Hirschi 1990, S. 154 ff.
[809] Göppinger 1997, S. 114.
[810] Ebd.
[811] Evans u.a. 1997, S. 486.
[812] Göppinger 1997, S. 114.
[813] Peers ist ein Fachbegriff aus der Soziologie und Pädagogik und geht zurück auf Charles H. Cooley (1864-1929), der das Konzept der Primärgruppen entwickelte. Peers übernehmen bei Kindern und Jugendlichen wichtige Sozialisationsfunktionen. Als Peers gelten dabei Personen entsprechenden Alters, vorwiegend auch ähnlicher sozialer Herkunft und gleichen Geschlechts. Charles H. Cooley beobachtete, dass Kinder und Jugendliche sich stärker an Menschen ähnlichen Alters orientieren, als an den eigenen Eltern und dass auch später die Ansichten eines Menschen häufig von den Menschen der unmittelbaren Umgebung geprägt werden.

Die Theorie der sozialen Bindungen erklärt Kriminalität mit der Schwächung oder dem Bruch der Bindungen, die ein Mensch zur Gesellschaft und ihren Gruppen besitzt.[814] Obwohl Hirschi sich von der Social Bond Theory abwendet, indem er erklärt: „Causal theories must be motivated theories".[815] Die Social Bond Theory hat durch die Veröffentlichung der Self-Control Theory an Wert nicht verloren. Einige Autoren sind sogar der Meinung, dass das Prinzip Low Self-Control nicht weit entfernt von den ursprünglichen Annahmen der Social Bond Theory sei. Geringe Selbstkontrolle muss danach gerade als die Kehrseite derjenigen Bindungen verstanden werden, die mit einem sozialen konformen Lebensstil einhergehen.[816] Somit lässt sich fest halten, dass die General Theory of Crime auf den Gedanken der Theorie der sozialen Bindungen aufbaut, sich jedoch als vollständig neue Theorie mit neuem Ansatz und neuen Grundelementen darstellt.

4.2 Ein Erklärungsversuch anhand der Self-Control Theory

Im Folgenden wird versucht, anhand der Self-Control Theory mögliche Ursachen und Erklärungen für die Entstehung von Computerkriminalität zu finden. Hierbei werden nicht alle Aspekte gleich gewichtet, vielmehr werden einzelne mehr oder weniger wichtige Teilaspekte herausgegriffen und analysiert. Dabei werden auch konzeptionelle und inhaltliche Probleme der Self-Control Theory behandelt und analysiert.

Self-Control

Self-Control wird von Gottfredson und Hirschi als ein Konstrukt verstanden, welches – in den ersten Jahren entstanden – stabil über die weitere Lebensphase bleibt und in dem das Alter als ein in einer Kriminalitätstheorie zu berücksichtigender Faktor entfällt:
„The major 'cause' of low self-control thus appears to be ineffective child-rearing. Put in positive terms, several conditions appear necessary to produce a socialised child."[817] „The fact most obviously relevant to the family is the stability of differences in the likelihood of criminal and deviant behavior over the life course. These stable differences appear to be established as early as ages six to eight. "[818] „The evidence suggests to us that variation in self-

[814] Schneider 2001, S. 55 f.
[815] Fattah 1997, S.276.
[816] Göppinger 1997, S. 113.
[817] Gottfredson/Hirschi 1990, S. 96.
[818] Gottfredson/Hirschi 1994, S. 52.

control is established early in life, and the differences between individuals remain reasonably constant over the life course. “[819]

An diesem Konzept der Stabilität von Self-Control durch das ganze Leben hindurch haben Gottfredson und Hirschi unter anderem von Bartusch Kritik erfahren: „Gottfredson und Hirschi (1990) do not argue that age is a trivial element in the explanation of crime. Quite the contrary: They maintain that the age effect is so robust and so powerful that no social factor can account for it. (...) It is Gottfredson and Hirschi´s argument for the immunity of theory to consideration of age, and their assertion that the causes of crime are the same at every age, that leads to our claim that age is superfluous in their theory.”[820] „Moreover, we found that these childhood and adolescent factors related in ways predicted by Moffitt's developmental theory to four correlates of antisocial behavior: Childhood antisocial behavior was related more strongly than adolescent antisocial behavior to low verbal ability, hyperactivity, and negative/impulsive personality, whereas adolescent antisocial behavior was related more strongly than childhood antisocial behavior to peer delinquency. The two underlying latent factors also showed the predicted differential relations to later criminal convictions: Childhood antisocial behavior was significantly more strongly associated with convictions for violence, while adolescent antisocial behavior was significantly more strongly associated with convictions for nonviolent offenses.”[821]

Die Autoren können nicht die Annahme von Gottfredson und Hirschi bestätigen, dass das Alter ein nicht zu berücksichtigender Faktor sei und dass Self-Control durch das Alter nicht beeinflusst werde.

In diesem Zusammenhang stellt sich die Frage, ob diese Kritik auch in Bezug auf Hacker bestätigt werden kann und ob sich diese Annahme auch im Hinblick auf Hacker, die sich in Systeme fremder Unternehmen gehackt haben und danach von denselben Unternehmen als Angestellte übernommen wurden, gelten kann. Dieselbe Frage stellt sich bei Virenkonstrukteuren, die mit eingebauten Bewerbungen im Virenquellcode von Unternehmen angestellt werden. Außerdem stellt sich in diesem Zusammenhang die Frage, ob diese Hacker nach ihrer Einstellung weiterhin hacken und Viren bauen. Würde man annehmen, dass diese Hacker damit aufhörten, dann würde sich die Frage stellen, warum? Waren diese Hacker früher kriminell, ist

[819] Gottfredson/Hirschi 1994, S. 2.
[820] Bartusch u.a. 1997, S. 15.
[821] Bartusch u.a. 1997, S. 16f.

dies ein Anzeichen dafür, dass sie Low Self-Control haben. Dieses bleibt nach Gottfredson und Hirschi aber lebenslang relativ stabil. Der zweite Ansatz von Gottfredson und Hirschi, dass auch Gelegenheiten Einfluss auf kriminelle Handlungen haben, hat hier keinen Bestand, da sich die Gelegenheiten für diese Hacker nicht durch deren Angestelltenverhältnis wesentlich verändert haben. Eine Ausnahme könnte allenfalls der reduzierte Freizeitfaktor sein, wenn die Hacker zuvor arbeitslos waren. Die eben aufgezeigte Kritik wird von Kevin Mitniks Aussage bestätigt, der früher ein krimineller jugendlicher Hacker war und mittlerweile auf diese kriminellen Handlungen verzichtet: „Meine Neugier hat mich zu den Verbrechen motiviert. Ich wollte so viel wie möglich darüber erfahren, wie Telefonnetze arbeiten und wie es sich mit der Computersicherheit verhält. Ich wurde von dem Kind, das Zaubertricks liebte, zum weltweit berüchtigten Hacker – von Regierungen und Unternehmen gefürchtet! Wenn ich an mein Leben in den vergangenen dreißig Jahren zurückdenke, muss ich mir eingestehen, dass ich durch meinen Wunsch, Technologien zu begreifen, mein Bedürfnis nach guten intellektuellen Herausforderungen und meine Neugier einige sehr schlechte Entscheidungen getroffen habe. Mittlerweile bin ich ein neuer Mensch geworden. Ich nutze meine Talente und das umfassende Wissen, das ich über Informationssicherheit und Taktiken des Social Engineering angesammelt habe, um Regierungen, Firmen und Einzelpersonen dabei zu helfen, Bedrohungen ihrer Informationssicherheit zu erkennen, zu vermeiden und zu begegnen. In diesem Buch kann ich auf eine weitere Art und Weise meine Erfahrungen für andere nützlich machen, die sich gegen die weltweiten Aktivitäten bösartiger Informationsdiebe schützen wollen."

Im Zusammenhang mit der These seitens Gottfredson und Hirschi, dass Personen mit einem niedrigen Maß an Self-Control eine Neigung besitzen sofortigen Bedürfnisen nachzugehen, könnte der schnelle und berüchtigte Ruhm durch Virenkonstruktionen eine Rolle spielen, der sich als ein Hinweis auf Low Self-Control darstellen würde. Die im ersten Teil der Arbeit aufgezeigten Virengruppen zeigen den Fortschritt in den Fähigkeiten von Virenprogrammierern. Jede neue Virengruppe hat unterschiedliche Aufbauarten und Eigenschaften, die zeigen, dass diese speziell von erfahrenen Programmierern erstellt werden mussten. Script-Kiddies, die zumeist Virenbaukästen benutzen, müssen dagegen auf vorhandene und bekannte Virenarten zurückgreifen und sich anhand der von Virusbaukästen vorgegebenen veränderbaren Eigenschaften orientieren. Somit kann vermutet werden, dass Script-Kiddies eher Low Self-Control besitzen, wogegen Hacker, die neue Virencodes erstellen, eher High Self-Control besitzen. Die Bedürfnisbefriedigung liegt bei beiden Gruppen darin, dass der Virus Erfolg hat,

d.h. dass er sich möglichst weit verbreitet. Viren verursachen zum Teil einen erheblichen Schaden, und Hacker können deswegen wegen Datenveränderung oder -sabotage bestraft werden. Gottfredson und Hirschi gehen aber davon aus, dass alle Kriminellen mit Low Self-Control ausgestattet sind. Dies würde auf Script-Kiddies zutreffen, da sie die schnelle und einfache Variante der Bedürfnisbefriedigung wählen. Sie benötigen nur einen geringen Aufwand, um zum Erfolg zu gelangen. Hacker dagegen müssen langwierig programmieren, was eher für High Self-Control spricht. Dies widerspricht jedoch der Annahme von Gottfredson und Hirschi, da nach deren Meinung solche Personen nicht kriminell werden könnten.

Im Gegensatz zur Virenkonstruktion spricht der Ruhm eines Hackers in der Hackerszene, der sich durch neue Hacks, neue Programme oder neue Cracks einen Namen erst langwierig und teilweise mühselig erarbeiten muss, eher dafür, dass dieser mit High Self-Control ausgestattet ist.

Für Gottfredson und Hirschi stellt Low Self-Control die Motivation eines kriminellen Täters dar. Der Ansatz der Deprivation als Motivationsgedanke von Cohen und Felson könnte hier jedoch ebenfalls hilfreich sein. „Das Konzept der relativen Deprivation bezieht sich auf die Diskrepanz zwischen gesellschaftlichen Bedürfnissen und der gesellschaftlichen Befriedigung dieser Bedürfnisse.“[822] Gerade die Definition von Ted Robert Gurr scheint ein geeigneter Erklärungsansatz im Bereich der Hackerszene darzustellen: „Ted Robert Gurr definiert ´relative Deprivation´ insofern ganz ähnlich als die von den Handelnden wahrgenommene Diskrepanz zwischen ihren Werterwartungen und ihren Wertansprüchen. Werterwartungen nennt er dabei die Güter und Lebensumstände, von denen die Menschen annehmen, dass sie ihnen rechtmäßig zustehen; Wertansprüche sind in seiner Terminologie die Güter und Bedingungen, von denen sie glauben, dass sie sie erreichen und beibehalten können.“[823]
So könnten sich Hacker im Zustand einer relativen Deprivation befinden. Hacker sehen sich in Bezug auf die Zurückhaltung von Daten und sonstigen Informationen durch den Staat oder private Unternehmen beeinträchtigt. Sie beanspruchen die „Freiheit von Informationen“ und sind in ihrer Erwartung enttäuscht. Die Open-Source-Bewegung ist hierfür ein nichtkriminelles Paradebeispiel einer solchen Bewegung, die dieser Deprivation entgegenzuwirken versucht. Andere wiederum dringen in Systeme ein, um dort Informationen auszuspähen. Daneben sehen Gottfredson und Hirschi aufregendes und risikobehaftetes Verhalten als ein Anzeichen für Low Self-Control: „Criminal acts are exciting, risky, or thrilling. They involve

[822] Scheerer 1988, S.91.
[823] Ebd.

stealth, danger, speed, agility, deception, or power. People lacking self-control therefore tend to be adventuresome, active, and physical. Those with high levels of self-control tend to be cautious, cognitive, and verbal."[824] Die von einigen Hackern beschriebenen Thrill-Erlebnisse oder Kicks sprechen wiederum für ein geringes Maß an Self-Control, da Abenteuerlust, Gefährlichkeit und Heimlichkeit nach Gottfredson und Hirschi ein Anzeichen für Low Self-Control darstellen.

Das Cracken von Kreditkartennummern für kostenlose Telefonate, der Betrug beim Online-Banking oder die Weitergabe von ausgespähten Source-Codes und anderen Betriebsgeheimnissen sprechen für Low Self-Control, da Gottfredson und Hirschi Geld verdienen, ohne zu arbeiten, ebenfalls als ein Indiz für Low Self-Control ansehen. Betrachtet man die politisch motivierten Hacker, so dienen der Computer und die mit ihm verbundenen Aufklärungsversuche dieser Hacker dazu, langfristige Ziele zu erreichen, die der gesamten Gesellschaft nutzen. Durch den CCC veranstaltete Kongresse zeigen mit ihren computertechnischen und gesellschaftlichen Themen ein Engagement, das nicht ausschließlich als kurzfristige Bedürfnisbefriedigung angesehen werden kann. Auch die dauerhaften Bestrebungen, durch andere Veröffentlichungen einer eigenen generellen Kriminalisierung entgegenzuwirken, zeigen, dass zumindest Teile der Hackerszene auch langfristige Ziele verfolgen. Gottfredson und Hirschi setzen voraus, dass alle Handlungen, kriminelle und nichtkriminelle, denselben Neigungen unterliegen. Somit wären diese von politisch motivierten Hackern angestrebten langfristigen Ziele ein Indiz für ein höheres Maß an Self-Control. Selbst das Eindringen in fremde Systeme zum Zwecke der Bekanntgabe an die jeweiligen Unternehmen, um dadurch mögliche Schäden zu vermeiden, könnte ein Hinweis auf High Self-Control darstellen, da hierdurch das Ziel verfolgt wird, Unternehmen, und damit die Gesellschaft auch, langfristig für die Zukunft vor Übergriffen zu schützen. Dieser auf Unternehmen oder staatliche und andere gesellschaftliche Institutionen bezogene datenschutzrechtliche Aspekt ist ein zentrales Handlungsmotiv politisch orientierter Hacker.

Nicht alle Hacker müssten demnach aufgrund ihrer Handlungen ein geringes Maß an Self-Control besitzen. Low Self-Control ist für das Entstehen von Kriminalität jedoch nicht der einzige Faktor. Gelegenheiten spielen nach Gottfredson und Hirschi ebenfalls eine gewichtige Rolle. Programmierer, nichtkriminelle Hacker und kriminelle Hacker haben aber grundsätzlich dieselben Gelegenheiten. Sie sind mit einem ähnlichen Wissensstand ausgestattet, mit

[824] Gottfredson/Hirschi 1990, S. 89.

dem sie auf spezielle computertechnische Gelegenheiten reagieren können, und haben vergleichbare Zugriffsmöglichkeiten auf Computer und das Internet. Man müsste im Sinn der Self-Control Theory also davon ausgehen dürfen, dass z.B. nichtkriminelle Programmier mit einem hohen Maß an Self-Control und kriminelle Hacker mit einem geringen Maß an Self-Control ausgestattet sind.

Um diese Aussage zu überprüfen, muss zunächst erläutert werden, wie Gottfredson und Hirschi die Beziehung von kriminellen und analogen Handlungen zueinander in Beziehung stellen: „Our image of the 'offender' suggests that crime is not an automatic or necessary consequence of low self-control. It suggests that many noncriminal acts analogous to crime (such as accidents, smoking, and alcohol use) are also manifestations of low self-control. Our image therefore implies that no specific act, type of crime, or form of deviance is uniquely required by the absence of self-control. Because both crime and analogous behaviors stem from low self-control (that is, both are manifestations of low self-control), they will all be engaged in at a relatively high rate by people with low self-control. Within the domain of crime, then, there will be much versatility among offenders in the criminal acts in which they engage.“[825]

Gottfredson und Hirschi sehen kriminelle Handlungen als eine Untermenge von allgemeinen Verhaltensweisen, die Personen trotz der langfristigen negativen Konsequenzen begehen. Nach Gottfredson und Hirschi begehen Kriminelle eine Vielzahl von unterschiedlichen Taten. Sie spezialisieren sich nicht auf bestimmte kriminelle Handlungen, sondern haben ein breit gefächertes Handlungsmuster.[826] Aus dieser Erkenntnis heraus sehen Gottfredson und Hirschi nur einen Grund, Low Self-Control, für abweichende und analoge Handlungen. Sie lehnen das „Vielseitigkeitskonstrukt“ ab, nachdem verschiedene Formen von Delinquenz unterschiedliche Ursachen haben.[827] Diese Ideen bezeichnen sie im Rahmen ihrer General Theory of Crime als „Versatility“. Sie stützen ihre Behauptung auf Ergebnisse verschiedener Forschungsarbeiten, bei denen sich Personen in der Regel nicht auf eine Art abweichenden Verhaltens spezialisieren, sondern eher breit gefächerte abweichende Verhaltensweisen zeigen.[828] Eine Person begeht somit ihrer Ansicht nach eine Vielzahl von abweichenden Verhaltensweisen. Diese Verhaltensweisen stellen Gottfredson und Hirschi nicht kriminellen analogen Verhaltensweisen wie Unfällen, Rauchen und Alkoholkonsum gleich.[829] Sie sehen in kriminellen und

[825] Gottfredson/Hirschi 1990, S. 91.
[826] Gottfredson/Hirschi 1990, S. 91; Gottfredson/Hirschi 1994, S. 173 ff.; Hirschi/Gottfredson 2000, S. 64 f.
[827] Schneider 2001, S. 57.
[828] Gottfredson/Hirschi 1990, S. 91; Gottfredson/Hirschi 1994, S. 173 ff.
[829] Arneklev/Grasmick/Bursit 1999, S. 307, 328; Burton u.a. 1999, S. 46, 51; Gottfredson/Hirschi 1990, S. 91.

analogen nichtkriminellen Verhaltensweisen die Manifestation einer gemeinsamen Ursache: Low Self-Control. Fehlt es Personen an Self-Control, neigen sie dazu eher ihre Bedürfnisse krimineller sowie nicht krimineller Art zu befriedigen, ohne die langfristigen Konsequenzen ausreichend mit einzubeziehen. Self-Control ist in der General Theorie of Crime somit ein ausschlaggebender Faktor für Abweichung und Konformität und kann zur Erklärung aller Verhaltensformen herangezogen werden. Somit ließe sich anhand analoger Handlungen ebenfalls feststellen, mit welchem Maß an Self-Control bestimmte Hacker ausgestattet sind.

Um Self-Control besser verständlich zu machen, nennen Gottfredson und Hirschi mehrere Elemente von Self-Control, welche sie nicht als Ursache, sondern vielmehr als Folge von mangelnder Selbstkontrolle sehen. Diese Folgen ergeben sich nach Meinung der Autoren aus den Eigenarten krimineller Handlungen und sind im Folgenden bei der Erklärung von Self-Control von großer Bedeutung.[830]

Nach Gottfredson und Hirschi sind kriminelle Handlungen aufregend und gefährlich. Sie beinhalten Heimlichkeit, Gefährlichkeit, Schnelligkeit, Beweglichkeit und Kraft. Menschen, denen es an Self-Control fehle, neigen deshalb dazu, abenteuerlustig und physisch aktiv zu sein. Personen mit High Self-Control dagegen seien eher vorsichtig, kognitiv und verbal.

Etwas Verbotenes und Heimliches zu tun, haben Wetzstein u.a vor allem im Bereich der Virenkonstruktion und ihrer Verbreitung gesehen. Sie beschrieben es als den „Reiz mit dem Feuer“ und dem „Reiz ein Verbrechen zu begehen“. Die Abenteuerlust ist auch bei Hackern verbreitet und wurde von Eckert u.a. als Thrill-Erlebnisse, emotionale Kicks und Sensations-Seekers beschrieben. „Erst die Kicks und Thrills beim Öffnen eines fremden Computers bringen wieder Abwechslung, Spannung oder Euphorie.“[831] Der Computer und das Internet bieten Hackern viele Möglichkeiten, diese Gefühle auszuleben. Der Vergleich Roland Girtlers von Hackern mit Entdeckern, die mit ihren Schiffen auslaufen, um unbekannte Orte aufzuspüren, macht sich gerade in dem sich ständig ausdehnenden Internet bemerkbar.

Als weitere Folgen mangelnder Self-Control nennen Gottfredson und Hirschi folgende Eigenschaften: „Criminal acts provide easy or simple gratification of desires. They provide money without work, sex without courtship, revenge without court delays. People lacking self control also tend to lack diligence, tenacity, or persistence in a course of action. (...) Crimes require

[830] Gottfredson/Hirschi 1990, S. 89.
[831] Eckert u.a. 1991, S. 165.

little skill or planning. The cognitive requirements for most crimes are minimal. It follows that people lacking self-control need not possess or value cognitive or academic skills. The manual skills required for most crimes are minimal. It follows that people lacking self-control need not possess manual skills that require training or apprenticeship."[832]

Mit kriminellen Handlungen soll nach Gottfredson und Hirschi eine einfache und leichte Genugtuung der eigenen Wünsche möglich sein. Diese Menschen wünschen sich Geld, ohne zu arbeiten, oder Rache ohne die Verzögerung, die eine gerichtliche Auseinandersetzung mit sich bringen würde. Menschen mit fehlender Self-Control neigten auch zu fehlendem Fleiß und fehlender Beharrlichkeit im Verlauf ihrer Handlungen. Ein Verbrechen benötigt nach Gottfredson und Hirschi wenig Fachkenntnisse oder Planung. Die kognitiven Bedingungen für die meisten Verbrechensarten sind minimal. Ebenso sind die Anforderungen an die manuellen Fähigkeiten für die meisten Verbrechensarten minimal. Somit benötigten Kriminelle in der Regel kein Training oder eine Lehre für ihr normabweichendes Verhalten.

Hacker zerstören fremden Daten, fremde Rechner oder ganze Netzwerke, um ihre persönliche Frustration zu kanalisieren. Rache wurde zudem als mögliches Motiv von Hackern im vorherigen Kapitel an dem Beispiel des 13-jährigen Jugendlichen mit dem Nickname „Wicked" beschrieben, der die Firmenserver des Systemadministrators Steve Gibson mit DDoS-Attacken angriff. Dies würde demgemäß ein Anzeichen für Low Self-Control darstellen. Gottfredson und Hirschi nennen in diesem Zusammenhang aber die geringe Planung und die geringen Fachkenntnisse von Personen mit Low Self-Control.

„It also suggests, consistent with the idea of self-control, that individuals will tend to engage in (or avoid) a wide variety of criminal and analogous behaviors – that they will not specialize in some to the exclusion of others, nor will they 'escalate' into more serious or skillful criminal behavior over time."[833]

Um zu widerlegen, dass Hacker Low Self-Control besitzen, vielmehr eher High Self-Control, oder dass geringe Planung oder geringe Fachkenntnisse kein Anzeichen von Low Self-Control sind, werden die folgenden Aussagen über den Werdegang von Hackern, deren Vorgehensweisen und Auszüge aus den Berichten von Kevin Mitnick herangezogen.

[832] Gottfredson/Hirschi 1990, S. 89.
[833] Gottfredson/Hirschi 1994, S. 2.

Die aufklärerischen und kritisch-kreativen Hacker, die zum Teil als die echten Hacker bezeichnet werden, sehen den Schwerpunkt ihrer Tätigkeit im reinen Programmieren und der Verbesserung von Programmen, sei es auch von Programmen wie Firewalls oder Betriebssystemen. Das Lösen von Programmfehlern stellt einen wesentlichen Arbeitsbereich dieser Hacker dar. In diesem Zusammenhang leistet gerade die Open-Source-Gemeinde einen wesentlichen Beitrag. Kriminelle und nichtkriminelle Handlungsweisen werden von Gottfredson und Hirschi gleichgestellt und gelten somit in gleicher Weise als Folge von High oder Low Self-Control. Die Mitglieder der Open-Source-Gemeinde und ihre Handlungen können nicht als kriminell betrachtet werden. Sie sind zum Teil über Jahre angelegt und könnten somit einen Beweis dafür liefern, dass Personen mit langfristigen Neigungen als Indiz für High Self-Control nicht zu kriminellen Handlungen neigen.

Nicht alle Hacker, die sich mit dem Programmieren beschäftigen und dafür langfristige Vorgehensweisen, zum Teil über Jahre benötigen, um Programmiersprachen, Betriebssysteme, Netzwerksysteme und Sicherheitsprogramme zu erlernen, sind jedoch kriminell. Der Kölner CCC zeigt Interessierten, wie sie zu einem Hacker werden. Damit meint der Kölner CCC diejenigen Hacker, die in Systeme eindringen und Daten ausspähen. Nicht gemeint sind Handlungen wie Virenkonstruktionen von Script-Kiddies oder das Softwarecracken:
„Besorg' dir einen echten IP-Zugang. Wenn du im Internet hacken willst, benötigst du einen direkten Zugang zum Netz. Den bekommst du in der Regel per PPP. SLIP, Raw IP über ISDN oder X.25 würden es auch tun, (…). Installiere Unix auf deinem System. (…) Arbeite dich durch die Kernel-Docs/FAQ/HOWTO. (…). Der Zeitpunkt, programmieren zu lernen, ist jetzt gekommen. Besorg' dir ein paar Bücher über C, C++, Perl, Unix-Programmierung usw. Lese sie. Lese sie weitere Male, weil das meiste, was du im ersten Durchgang gelesen hast, dich verwirrt hat. Nun spiel' auf deinem System mit Perl, C und C++ herum, bis du programmieren kannst. Übe einige Zeit, bis du zumindest einigermaßen gut bist. Danach übe weitere ein bis zwei Jahre. Als nächstes besorgst du dir alle RfCs und arbeitest sie gewissenhaft durch. (…) Erkunde das Netz. Probiere herum. Suche Sicherheitslücken. Lese viel Source Code. Programmier einige Hacker-Tools. Nun bist du ein echter Hacker-Anwärter.“[834]

Wenn Hacker nun dieses hohe Fachwissen besitzen, gehen sie nicht planlos an Systeme heran, um diese zu hacken, sondern haben spezielle Vorgehensweisen.[835] Hacker bedienen sich ver-

[834] http://koeln.ccc.de/prozesse/writing/artikel/hacker-werden.html (zuletzt eingesehen am 17.12.2004).
[835] Auch wenn nicht immer eine spezielle Reihenfolge eingehalten wird, so sind die verschiedenen Vorgehensweisen zumindest immer auf irgendeine Weise ein Teil des Hackens.

schiedener Methoden, um Daten auszuspähen und zu manipulieren. Neben rein zerstörerischen Akten wie das Konstruieren von Viren und Würmern haben Hacker und Cracker spezielle Vorgehensweisen, mit denen sie die gewünschten Informationen erhalten. Dabei ist die folgende Reihenfolge nicht zwingend, sie wird jedoch bei Übergriffen als der effektivste Weg angesehen.

In der ersten Phase beschäftigen sich Hacker und Cracker mit dem Footprinting. Das Footprinting wird als ein wichtiger Teil des Angriffs bezeichnet und beinhaltet jede Form der Informationsbeschaffung. Dabei liegt der Schwerpunkt auf dem Sammeln systemrelevanter Informationen über das Ziel, um dadurch ein Profil zu erstellen. Hierbei nutzen Hacker Suchmaschinen oder das Usenet[836], um an Information wie Standorte, verbundene Firmen oder Organisationen, Nachrichten zu Fusionen, Kontaktnamen und deren E-Mail-Adresse oder Telefonnummer oder sogar Richtlinien zur Sicherheit zu gelangen.[837] Daneben gelangen Hacker auch durch das Social Engineering an wichtige Informationen. Diese Form des Generierens von Informationen hat wenig mit technischem Know-How zu tun. Social Engineering nutzt Techniken der Beeinflussung und Überredungskunst, falsche Tatsachen vorzutäuschen, um dergestalt an Informationen zu gelangen.[838] Kevin Mitnick ist ein Hacker, der mit dem Social Engineering einen großen Bekanntheitsgrad erlangt hat, indem er sich z.B. als Außendienstmitarbeiter, Lieferant, Kunde, Autoritätsperson oder Hilfsperson ausgab und dergestalt in die Räumlichkeiten eines Unternehmens gelangte.[839] Neben dem Social Engineering bezeichnet das Trashing Handlungen, bei dem ein Angreifer den Müll eines Unternehmens durchsucht, um dort an verwertbare Informationen über Benutzer- und Computerdaten zu gelangen.[840]

Nachdem wichtige Informationen gesammelt wurden, beginnt in der zweiten Phase der technische Bereich. Zunächst werden Netzwerke mit Netzwerk- und Port-Scannern gescannt, um in Erfahrung zu bringen, was für Rechner zur Zeit aktiv sind.[841] Als Informationen erhält man

[836] Z.B. mit groups.google.com kann man nach Meldungen im Usenet suchen.
[837] http://www.it-secure-x.de/index.php?option=com_glossary&func=display&letter=F&Itemid=40&catid=68&page=1 (zuletzt eingesehen am 17.12.2004).
[838] http://de.wikipedia.org/wiki/Social_Engineering (zuletzt eingesehen am 17.12.2004).
[839] Schönstein 2002, S 126 ff.; Mitnick/Simon 2003.
[840] http://www.it-secure-x.de/index.php?option=com_glossary&catid=68&func=display&search=Social+Engineering (zuletzt eingesehen am 17.12.2004).
[841] Hierfür werden z.B. Tools wie Nmap (Network Mapper) benutzt.

unter anderem Computernamen und die IP-Adressen. Mit Sniffern[842] wird der Datenverkehr eines Netzwerks empfangen und dargestellt. Als nächstes sucht der Hacker nach Exploits. Das sind Programme, die von Hackern ausgeführt werden und Schwachstellen in der Systemsicherheit ausnutzen. Nur indem der Hacker die Schwachstellen in einem Betriebssystemdienst ausnutzt, gelangt er in das System. Viele Exploits tauchen zum Beispiel in den neuen Microsoft Betriebssystemen Windows 2000 / XP auf. Softwareunternehmen veröffentlichen regelmäßig Sicherheitspatches, welche die Schwachstelle ausbessern. Jedoch installieren nur die wenigsten Nutzer solche Sicherheitspatches.[843]

Erst in der dritten Phase nutzt der Hacker seine Erkenntnisse, um Angriffe zu starten. Dabei versucht er z.B. im System die Zugangskontrolle zu erlangen, Passwortangriffe oder DoS-Attacken zu starten. In der vierten Phase versucht der Angreifer, sich den Zugang für spätere Manipulationen zu erhalten. Dafür werden meist Trojanische Pferde oder Root-Kids eingesetzt. In der letzten Phase versucht der Hacker, seine Spuren zu verwischen. Dies geschieht durch das Tunneling, Manipulation der Log-Dateien oder durch die Erstellung unsichtbarer Dateien.

Der Werdegang und die Vorgehensweise von Hackern verdeutlichen, dass Hacker über hohe Fachkenntnisse verfügen müssen, um sich Hacker nennen zu können. Auch wenn sich Hacker nicht zwangsläufig an die eben dargestellte Reihenfolge halten, so müssen sie zumindest gut mit Programmiersprachen und Netzwerksystemen umgehen können. Viele Hacker stammen zudem aus der Sparte der Programmierer, so dass sogar akademisches Fachwissen vorhanden ist. Von geringen Fachkenntnissen kann hier somit nicht gesprochen werden. Im Gegensatz zur Annahme von Gottfredson und Hirschi sind Hacker eher fleißig und verfügen über hohe Ausdauerfähigkeit. Zudem benötigt ein Angriff auf ein Computersystem einen sehr hohen Grad an Planung und Vorbereitung. Somit kann in keiner Weise von mangelnden kognitiven Eigenschaften gesprochen werden.

Bei anderen Hackern wie den Script-Kiddies trifft die Annahme von Gottfredson und Hirschi schon eher zu. Wie im zweiten Teil der Arbeit dargestellt, handelt es sich bei Script-Kiddies zumeist um Kinder und Jugendliche. Sie sind nicht daran interessiert, komplizierte Programmiersprachen zu erlernen, bis sie Viren erstellen können. Vielmehr möchten sie schnell und

[842] Engl. „to sniff“ für riechen, schnüffeln
[843] http://de.wikipedia.org/wiki/Exploit (zuletzt eingesehen am 17.12.2004); weitere Informationen unter: http://www.sans.org/top20/

mit geringem Aufwand Viren generieren. Es geht ihnen um den schnellen Erfolg, also darum zu sehen, ob und wie gut sich der eigene Virus verbreitet. Hierfür eignen sich die im zweiten Teil besprochenen Virenbaukästen. Spielerisch und mit wenig Programmierkenntnissen können so Viren erstellt werden. Script-Kiddies scheinen eher in das Bild des Kriminellen zu passen, der weniger kognitiv arbeitet und sehr auf die sofortige Bedürfnisbefriedigung aus ist: „Wer lernen will, wie man Viren schreibt, findet Tipps auf vielen Websites sogar Programme, die Viren erstellen, oder fertige Virenskripte, an denen man sich prächtig fortbilden kann, die aber auch jeder Halblaie herunterladen und leicht abgeändert auf die Reise schicken könnte. Solche Leute gelten in der Szene als `Script-Kiddies´ und stehen auf der niedrigsten Stufe der `VXer´-Hierarchie.“[844] VXer nennen sich hierbei die Mitglieder der Szene der Virenprogrammierer, die sich zum Teil auch als eine Parallelgruppe zur Hackerszene verstehen und nicht als ein Teil der Hacker-Szene selbst. Dabei schreiben Script-Kiddies nicht nur Viren, sondern versuchen sich auch am klassischen Hacken, bei dem sie wiederum vorgefertigte Programme benutzen, um in Systeme möglichst schnell und ohne viel Aufwand einzudringen.

Auch wenn diese Aussagen zum Teil auf viele Script-Kiddies zutreffen mögen, so scheint doch eine strenge Unterscheidung von Script-Kiddies und Virenprogrammierern notwendig. Dies kann durch Aussagen in einem Interview des Sasser-Virus-Erstellers Sven J. noch einmal verdeutlicht werden. Auch wenn Sven J. noch ein Jugendlicher ist, scheint er nicht in das Bild des Script-Kiddies zu passen, sondern eher in das Bild eines guten Virenprogrammierers: „Sven genießt das Warten und die Einsamkeit. Er besucht die Berufsfachschule für Informatik in Rotenburg. (…) Sven ist schüchtern. Reden ist seine Sache nicht. Er hat nur wenige Freunde, geht ungern auf Partys, trinkt keinen Alkohol. (…) Über den Wurm aber hat er geredet – und nicht nur mit der Hand voll Kumpels in der Schule. Bald wusste jeder in der Klasse, dass Sven an einem Computerwurm sitzt. Die Geschwister waren eingeweiht, nur die Eltern hatten keine Ahnung. Die es wussten, fanden die Idee gut. ´Die haben mir sogar gesagt`, erinnert Sven sich, ´dass ich etwas hinzufügen soll, das Schaden macht. Aber das wollte ich nie.` Ihm reicht der Wurm selbst. Er will besser sein als andere Virenprogrammierer. Nicht böser. (…) Bis zu zehn Stunden am Tag saß er vor dem PC.“[845] „Besonders am 3. März. Er chattet gerade mit seinen Kumpels, da sieht er in der ARD, wie das Nachtmagazin über ´Netsky`[846] berichtet. Sein Wurm im Fernsehen! ´Das war cool`, sagt Sven heute – aber er sagt es, als sei

[844] Stillich/Liedtke 2004, S. 2.
[845] Stillich/Liedtke 2004, S. 1.
[846] Netsky war der erste von Sven J. programmierte Virus mit dem er in Erscheinung getreten ist. Hierauf folgte der Sasser-Virus.

das die gute alte Zeit gewesen, in der er sich sicher gefühlt hat, als ich nur manchmal nachts wach geworden bin und dachte, das könnte Stress geben."[847]

Auch hier zeigt sich wieder das Bedürfnis nach Anerkennung. Jedoch scheint Sven J. nicht in das Bild eines typisch Kriminellen im Sinne der Theorie von Gottfredson und Hirschi zu passen: „People lacking self-control therefore tend to be adventuresome, active, and physical. Those with high levels of self-control tend to be cautious, cognitive, and verbal."[848] „The correlation between the use of drugs, alcohol, or tabacco and the commission of delinquent and criminal acts is well established."[849]

Sven J. ist nicht physisch orientiert, sondern beschäftigt sich eher kognitiv. Er ist kein körperlich aktiver Mensch, sondern eher schüchtern. Auch die Korrelation von Alkohol und Kriminalität trifft auf Sven J. nicht zu. Die Korrelationen zwischen Alkohol- und Tabakkonsum zu Low Self-Control wurden im Übrigen aufgrund von empirischen Studien bezweifelt.[850]

Durch die eben gemachten Ausführungen, auch in Verbindungen mit den Aussagen von Sven J., scheint entweder die Annahme, dass Kriminelle über wenig kognitive Fähigkeiten und wenig Ausdauer verfügen, falsch oder aber, dass der Grad dieser Fähigkeiten kein ausschlaggebendes Anzeichen für den Grad von Self-Control ist. Damit verbunden scheint somit auch die zentrale Aussage der Self-Control-Theorie, dass Kriminelle die Neigung haben, kurzfristigen Bedürfnissen zu erliegen und langfristige Ziele ausblenden, widerlegt oder zumindest angreifbar geworden. Es besteht weiterhin die Möglichkeit, dass neben Self-Control weitere Faktoren für die Kriminalitätsentstehung eine Rolle spielen. Britt führt hierzu Folgendes aus:

„Third, we tried to formally describe – through the use of our Simulation evidence – why we think the estimator we used in our original paper is useful for investigating the strength of the association between crime and analogous behaviors before and after conditioning on self-control. The Simulation evidence shows that when self-control is the only variable that affects variation in crime and analogous behaviors, our correlation parameter vanishes once we condition both outcomes on self-control. Our analysis of the Cambridge data showed that the correlation parameter did not vanish after we conditioned both outcomes on self-control. As we discussed in that paper, there are several reasons this result could have occurred. In our

[847] Stillich/Liedtke 2004, S. 2.
[848] Gottfredson/Hirschi 1990, S. 89.
[849] Gottfredson/Hirschi 1990, S. 40.
[850] Eifler 1998; Eifler 1997.

discussed in that paper, there are several reasons this result could have occurred. In our original paper, we drew our own conclusion. Others may think (perhaps for very good reasons) that we have mismeasured self-control or that we have misinterpreted Gottfredson and Hirschi's theory. Nevertheless, for the reasons expressed in our paper, we continue to believe that it is likely that other variables – in addition to self-control – will be necessary to explain this association."[851]

Attraktive Ziele

Neben Low Self-Control müssen den Tätern attraktive Zielobjekte oder -subjekte zur Verfügung stehen. Gottfredson und Hirschi sprechen im Bereich der Gelegenheiten kaum Details an: „Unfortunately, compared to their discussion of self-control and consequences, Gottfredson and Hirschi say relatively little about crime opportunity. Although, like levels of self-control, opportunity is expected to vary across individuals, possible sources of such variance are not described in detail."[852] Gottfredson und Hirschi beziehen sich, wie gezeigt, vor allem auf Cohen und Felson, so dass im Folgenden Gelegenheiten vor allem in Bezug auf die Forschungsarbeit interpretiert werden.

„Target suitability is likely to reflect such things as value (i.e., the material or symbolic desirability of a personal or property target for offenders), physical visibility, access, and the inertia of a target against illegal treatment by offenders (including the weight, size, and attached or locked features of property inhibiting its illegal removal and the physical capacity of personal victims to resist attackers with or without weapons). Routine production activities probably affect the suitability of consumer goods for illegal removal by determining their value and weight. Daily activities may affect the location of property and personal targets in visible and accessible places at particular times. These activities also may cause people to have on hand objects that can be used as weapons for criminal acts or self-protection or to be preoccupied with tasks which reduce their capacity to discourage or resist offenders."[853]

Dass hierbei das Internet und der Computer dem Hacker eine Vielfalt an suitable targets bieten, verdeutlicht die folgende Aussage von Sabine Helmers und Peter Grabosky: „Der Informationsraum des Internet ist im Vergleich zu anderen Netzen in seiner Größe und Vielfältig-

[851] Britt 2000, S. 980.
[852] Grasmick u.a. 1993, S. 10.
[853] Cohen/Felson 1979, S. 591.

keit einzigartig. Die dargebotenen Informationsangebote sind kostenlos abrufbar; sie werden in Eigenregie von den anbietenden Institutionen – anfänglich in der Mehrheit Forschungsinstitute und später zunehmend auch private Organisationen – sowie von Einzelpersonen erstellt. In den Datenmassen finden sich Informationen zu jedem erdenklichen Thema."[854] Eine weiterführende und ergänzende Wirkung hat die Aussage von Grabowsky: „While motives tend not to change, the variety and number of opportunities for cyber crime are proliferating. The exponential growth in Connectivity of Computing and Communications creates parallel opportunities for prospective offenders and parallel risks for prospective victims. As the Internet becomes increasingly a medium of commerce, it will become increasingly a medium of fraud."[855]

So kann gerade das Internet mit seinen hochwertigen Spielen, Film- und Musikangeboten, Softwareprodukten und der leichten Transportierbarkeit in Form von digitalen Kopien verglichen werden mit Selbstbedienungsläden für Konsumgüter. Auch hier hat sich damals ein Strukturwandel vom Thekenverkauf zu Selbstbedienungsläden vollzogen, der zu einer gesteigerten Diebstahlsrate führte. Hackern stellt das Internet eine überwältigende Menge an attraktiven Objekten zur Verfügung: „Im RA-Ansatz spielt die Kontrolle durch formelle Institutionen eine geringere Rolle und die Kriminalilätsentwicklung wird statt dessen mit allgemeinen gesellschaftlichen Entwicklungen und Modernisierungsprozessen verknüpft, die die informellen Kontrollen tangieren; entscheidend sind daher neben der Zunahme attraktiver Objekte vor allem Verschiebungen zwischen formeller und informeller Kontrolle. Die Externalisierung von Kosten für Kontrollen, die durch den Abbau der von Felson so genannten natürlichen sozialen Kontrollen' und deren Verlagerung hin zu rechtsförmigen Kontrollen forciert wurde, hat sich vor allem als konsequente ökonomische Strategie des Einzelhandels und der Nahverkehrsbetriebe gezeigt."[856]

Die Entwicklung des Computers und des Internets stellen einen gewichtigen Modernisierungsprozess dar. Mussten bislang tatsächliche Schranken wie Türen und Schlösser, Wachpersonal und Ausweiskontrollen überwunden werden, um an interne Daten und Geheimnisse einer Organisationen zu gelangen, so kann dies mittlerweile von jedem Ort aus geschehen, der mit einem Computer und einem Internetzugang ausgestattet ist. Hierdurch ist eine Vielzahl natürlicher sozialer Kontrollen weggefallen.

[854] Helmers 1995, S. 39.
[855] Grabosky 2001, S. 47.
[856] Karstedt/Greve 1996, S. 180.

Cohen und Felson beschreiben suitable targets hierbei zudem nicht allgemein, sondern sehen verschiedene Voraussetzungen dafür, wann Zielobjekte für Täter als attraktiv wahrgenommen werden. Dabei kann der Schwerpunkt auf folgende vier Hauptpunkte gelegt werden, die zur Attraktivität der Zielobjekte beitragen:

„Four main elements influence a target's risk of criminal attack, as summed by the acronym VIVA: Value, Inertia, Visibility, Access. All four of these dimensions are considered from an offender's viewpoint. Offenders will only be interested in targets that they value, for whatever reason. Thus the latest popular CD hit will be stolen more from record stores than a Beethoven CD of roughly equal monetary value, since most offenders would like to have the former but not the latter. Inertia is simply the weight of the item. Thus small electronic goods are stolen more than weighty items, unless these latter are wheeled or motorised to overcome their weight. Visibility refers to the exposure of theft targets to offenders, as when someone flashes money in public or puts valuable goods by the window. Access refers to street patterns, placement of goods near the door, or other features of everyday life making it easy for offenders to get to targets."[857]

Auf deutsch zusammengefasst: Vier Hauptelemente beeinflussen die Gefahr für ein Objekt oder Subjekt, zum Ziel eines kriminellen Angriffs zu werden: der Wert, die Trägheit, die Sichtbarkeit und die Zugriffsmöglichkeit. Dabei ist die Sichtweise der Täter von Bedeutung, die nur an den Zielen interessiert sind, die für sie einen Wert haben. Mit Trägheit ist das Gewicht des Zielobjekts gemeint. Sichtbarkeit meint, wie deutlich Zielobjekte für den Täter erkennbar sind. Die Zugriffsmöglichkeit oder der Zugang bezieht die allgemeinen Muster der Platzierung der Zielobjekte ein.

Der Wert eines Ziels kann bei Hackern unterschiedlich bewertet werden. Allein der materielle Wert kann hierbei schon von Bedeutung sein. So zeigte sich in der Studie zum Account-Missbrauch, dass ein wesentlicher Wert des Zugangscodes darin lag, kostenlos surfen zu können. In ähnlicher Weise müssen die Tauschhandlungen hinsichtlich Musikstücken, Filmen oder Software auf Tauschbörsen beurteilt werden. Sie haben zunächst den Wert, den die Täter auf legalem Wege hätten bezahlen müssen. Jedoch sehen einigen Hacker den Wert auch darin, dass sie mehr Files (Musik, Filme, Software) als die anderen haben. Gerade bei den Software-

[857] http://www.homestead.com/rouncefield/files/a_soc_dev_22.htm (zuletzt eingesehen am 15.12.2004).

crackern wurde gezeigt, dass bei ihnen weniger der materielle Wert eine Rolle spielt, als darin, die Software als erster geknackt zu haben. Somit liegt hier der Wert im Prestige, das aus den einzelnen Handlungen erwächst. In ähnlicher Form können die Handlungen von einzelnen Hackern bewertet werden, die in Systeme eindringen und diese ausspähen. Hier liegt der Wert ebenfalls darin, in der Szene einen Prestigegewinn zu erhalten. Jedoch bestand ein Wert dieser Hacks auch darin, ein Duell gegen die Systemadminstratoren zu gewinnen. Dabei geht es den Tätern nicht ausschließlich um den Sieg gegen eine Person, sondern auch um den Sieg gegen ein vermeintlich gut gesichertes System. Für einige Hacker scheint ein Wert darin zu liegen, sich einfach mit der Materie des Programmierens auseinander zu setzen und die Programme zu verbessern. Ihr Erfolg liegt offensichtlich darin, dass ein Programmcode nach seiner Bearbeitung besser funktioniert als vorher.

Die Größe und das Gewicht (Inertia=Trägheit) ist bei der Beurteilung eines Ziels ebenfalls von Bedeutung. Cohen und Felson gingen davon aus, dass Objekte, die sehr schwer oder sehr groß sind, weniger häufig gestohlen werden als Objekte, die eher klein und leicht ausfallen. Dieser praktische Gedanke verdeutlicht die Problematik der Digitalisierung. Digitalisierte Daten, in welcher Form auch immer, besitzen quasi kein Gewicht mehr und haben auch nur eine rein logische Größe, die in Bytes angegeben wird. Erst wenn die Daten auf ein Medium (Diskette oder CD-ROM) gespeichert werden, erhalten sie eine tatsächliche Größe. Werden Daten jedoch über das Internet kopiert oder verändert, so sind die Größe und das Gewicht dieser Daten gleich null.

Visibility beschreibt die Sichtbarkeit oder die Erreichbarkeit eines Ziels. Hier spielt wiederum das Internet eine entscheidende Rolle. Tauschbörsen ermöglichen es jedem Nutzer auf der Welt, zahlreiche Daten zu erhalten, auch wenn diese Daten den Anbietern gar nicht gehören. Wurde bislang eine Raubkopie auf VHS überspielt, so blieb sie bislang im Umkreis des Raubkopierers, zumeist in seiner Wohnung oder seinem Haus und war für Personen außerhalb des sozialen Umfelds nicht erreichbar und nicht sichtbar. Im Zuge der Tauschbörsen wurden Daten digital auf Computern gespeichert und konnten durch Freigaben an alle mit dem Internet angeschlossenen Nutzer zur Verfügung gestellt werden. In ähnlicher Weise muss die Erreichbarkeit von Unternehmen beschrieben werden. Viele Großunternehmen sind mittlerweile mit Niederlassungen auf allen Kontinenten vertreten. Bislang war es Außenstehenden nur schwer möglich, diese zu erreichen, z.B. durch den Aufwand, in ein fremdes Land zu reisen, um so die Niederlassung betreten zu können. Zudem war es auch recht schwer herauszufinden

wo die gewünschten Informationen zu finden waren. Heutzutage können mit Hilfe von Suchprogrammen wie Google wichtige Informationen eingeholt werden, ohne dass man sich aus den eigenen vier Wänden begeben müsste.

Neben dem Wert, der Trägheit und der Erreichbarkeit ist die Zugriffsmöglichkeit weiterhin von entscheidender Bedeutung. Nach Cohen und Felson verstärkt eine erleichterte Zugriffsmöglichkeit die Wahrscheinlichkeit krimineller Handlungen. Grundsätzlich sind Daten für jeden frei lesbar. Dabei können sie frei auf einem Computer gespeichert sein oder aber auf dem Weg durch das Netz abgefangen werden. Daten werden deshalb zunehmend durch unterschiedliche Formen vor dem Zugriff von Fremden geschützt. Es entstehen immer mehr Sicherheitsstandards und -verfahren, wie Antivirenprogramme, Firewalls und kryptografische Verschlüsselungsverfahren. Fehlen solche Sicherheitsstandards oder sind sie nur ungenügend, so erhöht dies nach Cohen und Felson die Wahrscheinlichkeit einer kriminellen Handlung. Wie die Untersuchungen des Computersicherheitsinstituts Computer Security Institute (CSI) in Zusammenarbeit mit dem FBI gezeigt haben, hatten in den Jahren 1999-2004 30-42 Prozent der Unternehmen keine Kenntnis darüber, wie viele Vorfälle im Bereich der Übergriffe von außen stattfanden. Wenn Firewalls und ähnliche Programme eingesetzt werden, können Unternehmen zumindest an den Log-Dateien nachvollziehen, welche und wie viele Übergriffe stattfanden. Es scheint, dass diese hohe Anzahl an Unternehmen bislang keine oder zumindest ungenügende Sicherheitsvorkehrungen getroffen haben. Eine ähnliche oder noch gravierendere Situation kann bei privaten Computern vermutet werden. Somit verstärken ungeschützte Daten und ungeschützter Datentransfer die Wahrscheinlichkeit krimineller Handlungen. Dies mag vor allem für jüngere und noch relativ unerfahrene Hacker der Fall sein.

In diesem Zusammenhang soll die Aussage von Karstedt und Greve zitert werden, die diese Problematik noch einmal verdeutlicht: „So stellen die Ausstattung von Haushalten mit hochwertigen, aber leicht zu transportierenden Konsumgütern ebenso wie die Selbstbedienungsläden Jugendlichen eine überwältigende Menge an attraktiven Objekten zur Verfügung, die aufgrund überwiegend außerhäuslicher Berufstätigkeit bzw. der Verringerung des Bedienungspersonals praktisch nicht bewacht und kontrolliert werden.“[858]

Dabei handelt es sich bei den leicht zu transportierenden Konsumgütern um die Daten auf den Rechnern, die häufig ungesichert mit dem Internet verbunden sind.

[858] Karstedt/Greve 1996, S. 180.

Allerdings stellt sich die Frage, ob eine erschwerte Zugriffsmöglichkeit auch bei Hackern kriminelle Handlungen verringert. Interessanterweise geben einige Hacker als Motiv an, dass gerade der intellektuelle Wettkampf gegen gesicherte Systeme den Reiz des Hackens ausmacht. Sie sprechen von Langeweile, wenn sie keine Herausforderung haben. Dies wird unter anderem durch folgende Aussage Kevin Mitnicks deutlich: „My motivation was the quest for knowledge, the intellectual challenge (...) My hacking involved pretty much exploring computer systems and obtaining access to the source code of telecommunication systems and computer operating systems, because my goal was to learn all I can about security vulnerabilities within these systems...“[859]

Auch die Aussagen zweier 18- und 19-jähriger Hacker verdeutlicht diese Problematik:
„Anfangs ist man nur tagelang frustriert, weil man nicht reinkommt. Aber wenn man es dann geschafft hat, wenn man sich überlegt, dass man schlauer ist oder mehr Glück hat als derjenige, der versucht, das System vor solchen Leuten wie mir zu schützen, dann ist das schon eine phantastische Sache. Ich meine, dass muss man sich einmal überlegen: Ich gegen den cleversten Experten und gewinne (...). Manchmal gibt es Netze, da braucht man lange, um reinzukommen, manchmal geht es sehr schlecht; aber das ist es ja gerade, was mich anmacht. Wenn ich genug Zeit habe und noch ein paar Kumpels bei mir sind, die mir helfen, knacke ich fast alles.“[860]

Somit sind gerade ungesicherte Systeme vor solchen Hackern[861] sicher, da diese nicht an dem Ausspähen der sich auf den Computern befindlichen Daten interessiert sind. Diese Hacker sind vielmehr daran interessiert, das Sicherheitssystem kennen zu lernen und es zu umgehen, d.h. ihre eigenen Fähigkeiten mit denen des Systems und des jeweiligen Administrators zu messen. Erst diese Herausforderung motiviert diese Hacker, in Systeme einzudringen. Somit scheint es, dass im Bereich der Computerkriminalität die Annahme, dass eine geringe Zugriffsmöglichkeit die Wahrscheinlichkeit krimineller Handlungen verringert, für einige Hacker nicht zutrifft und sich gerade ins Gegenteil verkehrt. Je weniger Zugriffsmöglichkeiten durch verstärkte Sicherheitsvorkehrungen vorhanden sind, desto reizvoller sind diese Ziele

[859] http://www.pbs.org/wgbh/pages/frontline/shows/hackers/whoare/testimony.html (zuletzt eingesehen am 19.09.04).
[860] Eckert u.a. 1991, S. 168ff.
[861] Dabei muss es sich um Hacker mit einem besonders hohen computertechnischen Wissensstand handeln, da sie im Wettkampf mit dem System und dem Administrator relativ schnell handeln und über einen umfassenden Kenntnisstand im Bereich der Computertechnik verfügen müssen.

für einige Hacker. Mit anderen Worten: Je komplizierter das System gesichert ist, desto interessanter wird es anscheinend für einige Hacker. Dies gilt jedoch nur, wenn man die Daten als die eigentlichen Objekte ansieht, an die Hacker gelangen wollen. Um an diese Daten gelangen zu können, müssen sie komplizierte Sicherheitssysteme überwinden. Je komplizierter das System allerdings ausgestattet ist, umso eher besteht die Wahrscheinlichkeit, dass sich Hacker an dieser Aufgabe zu schaffen machen. Es stellt sich jedoch für diese Gruppe von Hackern, die ihre Motivation aus dem intellektuellen Wettkampf ziehen, die Frage, ob die Daten überhaupt das eigentliche Zielobjekt darstellen. Es scheint vielmehr, als ob nicht die Daten, sondern Firewalls, Passwörter und andere Sicherheitsvorkehrungen das eigentliche Zielobjekt darstellen. Dies ist vergleichbar mit einem Dieb, dessen Ziel es nicht ist, Gegenstände aus einem Haus zu entwenden, sondern für den die Herausforderung in dem Öffnen von Haustüren besteht. Betrachtet man Firewalls und andere Sicherheitsvorkehrungen als das eigentliche Zielobjekt, dann sind diese wiederum über das Internet leicht erreichbar. Somit würde aus dieser Sichtweise die Annahme, dass Kriminalität erhöht wird, wenn eine leichte Zugriffsmöglichkeit auf die Zielobjekte vorherrscht, wieder hergestellt.

Kontrollinstanzen

Neben dem lohnenden Ziel müssen Kontrollinstanzen fehlen, die geeignet sind, die Tat zu verhindern. Dabei muss es sich nicht zwangsläufig um Polizisten, Sicherheitspersonal oder andere Aufsichtspersonen handeln. Tatsächlich hat sich in Forschungsergebnissen gezeigt, dass die Anwesenheit von Nachbarn, Freunden oder des Eigentümers des möglichen Zielobjekts die Wahrscheinlichkeit der Tatbegehung stark verringert.[862] Zudem muss es sich bei den Kontrollen keineswegs ausschließlich um Personen handeln. Auch Alarmsysteme, Barrieren oder Beleuchtungen können geeignet sein, Wächterfunktionen zu übernehmen und somit die Wahrscheinlichkeit der Tatbegehung zu verringern.

In diesem Zusammenhang kann es viele verschiedene Kontrollinstanzen geben: Eltern, Peers, Polizei usw. Es stellt sich dabei immer die Frage, ob die jeweiligen Kontrollen auch effektiv sind. Eltern könnten eine mögliche soziale Kontrolle darstellen. Gottfredson und Hirschi machen in diesem Zusammenhang zur Familie folgende Anmerkungen: „The family may reduce crime by guarding the home. (...) In fact, it soon became plain that familial institutions may

[862] Clarke/Felson 1993, S. 3.

play a role in crime control beyond watching their own members, that they can do much by merely protecting their own property.“[863]

Wie gezeigt existieren unzählige unterschiedliche Formen von Hackergruppierungen. Entgegen der allgemeinen Meinung, Hacker seien ausschließlich Jugendliche, handelt es sich teilweise um Erwachsene und um professionelle Gruppierungen. Auf diese Hacker können Eltern keinen Einfluss nehmen. Eltern können somit allein auf den Teil der Hackerszene als Kontrollinstanz Einfluss nehmen, bei denen jugendliche Hacker noch im Elternhaus wohnen. Bei solchen Hackern scheint die Möglichkeit einer Einflussnahme sehr groß. Eltern könnten jederzeit den Zugang zum Internet und Computer einschränken oder überwachen. Leider scheinen die meisten Eltern über eine nur geringe computertechnische Erfahrung zu verfügen. Fehlt ihnen aber dieses Wissen, können sie nicht feststellen, welche Möglichkeiten Kinder und Jugendliche mit dem Computer und dem Internet haben, welche Seiten Jugendliche besuchen und wie sie diese Handlungen verhindern können, ohne gleich vollständig den PC-Gebrauch zu verbieten. Wie in der Studie zum Account-Missbrauch gezeigt, fühlen sich viele Eltern mit dieser Problematik überfordert und sind froh, wenn staatliche Instanzen diese Aufgabe übernehmen. Somit scheint es, als ob Eltern als Kontrollinstanz mangels Effektivität ausscheiden.

Peers könnten hier einen höheren Einfluss und eine Kontrollfunktion übernehmen. Abgesehen von Freunden und Kollegen im Alltag kommen vor allem die Kontakte der Peers im Netz in Frage. Die Kontakte über E-Mail, Usenet oder Diskussionsforen könnten dazu genutzt werden, kontrollierend auf das Verhalten anderer Hacker Einfluss zu nehmen. Hier treten vor allem Hacker des CCC hervor, die sich zum Ziel gemacht haben, die Computertechnik und die Gesellschaft voranzubringen. Jedoch können solche Organisationen nur als Vorbildfunktion, aber nicht als Kontrollinstanz dienen. Gottfredson und Hirschi sehen Peers zudem noch in einem ganz anderen Kontext. Sie gehen davon aus, dass Jugendliche, denen es an Selbstkontrolle mangelt, sich gezielt Gruppen danach aussuchen, in denen Gleichgesinnte, nämlich ebenfalls mangelhaft selbstkontrollierte Jugendliche, verkehren. Nicht die Gruppe verleite daher zur Delinquenz, sondern Personen suchen sich gleichstrukturierte Gruppen aus. Somit suchen sich im Sinne von Gottfredson und Hirschi Hacker mit kriminellen Neigungen Gruppen mit denselben kriminellen Neigungen. Das würde heißen, dass Hacker sich in speziellen Gruppen finden, gleiche Ansichten teilen und deshalb auch keinen kontrollierenden Einfluss

[863] Gottfredson/Hirschi 1994, S. 57.

aufeinander haben können, sondern vielmehr einen sich gegenseitig bestärkenden Einfluss haben.

Eine weitere mögliche Kontrollinstanz könnten die Strafverfolgungsbehörden darstellen. In diesem Zusammenhang erläutern und ergänzen Gottfredson und Hirschi Cohen und Felsons „capable guardians“ mit den Überlegungen von Thomas Hobbes und Jeremy Bentham.[864] Thomas Hobbes ging von der Vorstellung aus, dass eine soziale Ordnung nicht naturgesetzlich entstehe, sondern erst dadurch, dass sich eine Gesellschaft darauf einigt, welche Verhaltensweisen als abweichendes Verhalten angesehen und bestraft werden sollen. Dabei ging Hobbes von der Nutzenmaximierung menschlichen Verhaltens aus, dem ein Kostenfaktor im Sinn von negativen Sanktionen gegenüberstehe. Darauf aufbauend greifen Gottfredson und Hirschi Benthams allgemeine Theorie menschlichen Handelns auf, um abweichendes Verhalten zu beschreiben.[865] Danach ist die Natur der Menschen darauf gerichtet, stets „pleasure“ zu erzielen und „pain“ zu vermeiden.[866] Abweichende wie auch konforme Verhaltensweisen sind von dieser Kosten-Nutzen-Kalkulation gleichermaßen bestimmt. Sanktionen stellen dabei einen entscheidenden Kostenfaktor dar. Somit hängt die Begehung von kriminellen Handlungen in besonderer Weise von der Antizipation positiver und negativer Konsequenzen des Handelnden ab, daher insbesondere von den angedrohten und denkbaren Sanktionen.[867] Die Strafverfolgungsorgane und ihre Sanktionen können nach Gottfredson und Hirschi einen Einfluss auf Kriminalitätsentstehung haben. Es bleibt hierbei zu beachten, dass Kontrollinstanzen auch im Bereich der Computerkriminalität ihren Aufgaben gerecht werden müssen. Ist eine Kontrollinstanz zwar anwesend, aber ineffektiv, verringert diese die Wahrscheinlichkeit der Tatbegehung nur in geringem Ausmaß oder gar nicht.[868]

Um zu erläutern, ob die Polizei eine Kontrollinstanz im Bereich der Computerkriminalität für Hacker darstellt, ob diese effektiv arbeitet, d.h. die Wahrscheinlichkeit der Sanktionierung hoch ist, und ob diese Kontrollinstanz als solche auch als effektiv von den Hackern bewertet wird und einen Einfluss auf die Entstehung von Hackerkriminalität hat, werden im Folgenden kurz die Probleme der Strafverfolgungsbehörden im Bereich der Computerkriminalität und die damit zusammenhängende Problematik der Internetstruktur dargestellt und erläutert.

[864] Gottfredson/Hirschi 1990, S. 5 ff.
[865] Bentham wiederum entwirft seine Überlegungen vor dem Hintergrund der von Hobbes gemachten Gedanken.
[866] Bentham 1970, S. 11 f.
[867] Lamnek 1997, S. 122.
[868] http://www.crimereduction.gov.uk/skills08.htm (zuletzt eingesehen am 23.08.2004)

Tatortfrage

Im Gegensatz zu anderen Kriminalitätsformen muss im Bereich der Computerkriminalität der Täter nicht notwendigerweise zur Tatzeit am Tatort sein. Des weiteren besteht zwischen Täter und Opfer kein unmittelbarer Kontakt. Dies hat zur Folge, dass der Täter eine gewisse Distanz hat und eher das Gefühl entstehen kann, von dem Opfer oder sonstigen Personen nicht entdeckt zu werden. Bei der gewöhnlichen Kriminalität hinterlässt der Täter Spuren und kann vom Geschädigten oder von Zeugen gesehen und nach Geschlecht, Körpergröße, Bekleidung, Sprache usw. beschrieben werden. Im Bereich der Computerkriminalität ist der Täter grundsätzlich nie am eigentlichen Tatort. Da er sein Angriffsziel nach IP-Nummern oder Telefonnummern auswählt, ist ihm oftmals nicht bewusst, an welchem Ort die Straftat stattfindet, da der physische Standort des Rechners nicht zwangsläufig der logische Standort des Ziels ist. Eine räumliche Verbindung zwischen Tatort, Aufenthaltsort des Geschädigten und Aufenthaltsort des Täters ist nicht gegeben, wodurch eine gewisse Anonymität seitens des Täters entsteht.

Internetstruktur

Die Problematik der Kontrollinstanzen fängt mit der Struktur des Internets an. Es gibt weder einen vollständigen Übersichtsplan, Orientierungs- und Sortiersysteme noch inhaltliche Kontrollen über die angebotenen Informationen.[869] Diese Offenheit der Gestaltung und die freie Möglichkeit des Internetzugangs machen die Attraktivität dieses Netzes erst aus. Die Vielfalt und Größe der Angebote, Dienste, Anwendungen, Kommunikationsmöglichkeiten und Zugänge machen es schwer, dieses Netzwerk strukturell zu erfassen und zu kontrollieren. Die Menge der Inhalte im Netz führt zu einer Undurchschaubarkeit und zu einer erschwerten Überwachung des Systems. Im Internet gibt es keine zentrale Verwaltung, Kontrollinstanzen oder Eingreiftruppen, vielmehr ist das Internet durch Eigeninitiative und Dezentralität geprägt. Aufgrund der fehlenden physischen Grenzen ist es im Internet schwer, den Zugang und Abgang von Daten zu kontrollieren. Die Prinzipien des „freien Flusses von Informationen“ und der „Dezentralität“ werden noch durch das Prinzip der „Reziprozität“ ergänzt.[870] Das Internet ist dergestalt ausgelegt, dass alle Nutzer sich gleichwertig interaktiv betätigen können, d.h. sie sind nicht allein Empfänger oder Sender von Informationen, sondern sie können beides

[869] Helmers 1995, S. 39.
[870] Helmers 1995, S. 42 ff.

gleichzeitig zur selben Zeit sein. Eine solche komplexe und undurchsichtige Struktur macht es Strafverfolgungsbehörden schwer, sich zurechtzufinden und Täter ausfindig zu machen.

Anonymität

Ein weiterer wichtiger Gesichtspunkt ist die zum Teil empfundene Anonymität des Internets. Dadurch bekommt ein möglicher Täter verstärkt das Gefühl, dass die Strafverfolgungsbehörden ihn nicht ermitteln können. Es entsteht somit der Eindruck, dass keine Kontrollinstanzen vorhanden sind oder diese zumindest nicht effektiv handeln können. Die Anonymität kann hierbei durch verschiedene Faktoren verstärkt werden: Die Fülle der zu ermittelnden Daten, Internationalisierung und Anonymizer.

Grundsätzlich ist die Rückverfolgung der Datenspuren eines Hackers nur möglich, wenn dieser über die von ihm während seines Aufenthalts im Internet mitgeführte IP-Nummer identifiziert werden kann. Eine solche IP-Nummer erhält jeder Nutzer mit der Einwahl in das Internet. Beim Einwahlknoten ist dann unter Umständen feststellbar, welchem Nutzer eine bestimmte IP-Nummer für einen bestimmten Zeitraum zugewiesen war. Probleme können sich für die Strafverfolgungsbehörden hierbei in mehrfacher Hinsicht ergeben. Gerade bei großen Internet-Providern entstehen im Verlauf eines Tages sehr umfangreiche Dateien, zu deren Inspektion bereits ein erheblicher Zeitaufwand notwendig ist. Soweit die Internet-Provider darüber hinaus dem Geltungsbereich des deutschen Telekommunikationsgesetzes unterfallen, dürfen sie solche Zugangsdaten als Verbindungsdaten aus Gründen des Datenschutzes nur eingeschränkt erheben und abspeichern, was sowohl den Datenumfang als auch die Speicherdauer betrifft. Die Strafverfolgungsbehörden haben daher das Problem, gegen die Zeit zu arbeiten, da ansonsten relevante Informationen verloren gehen. Sofern der Zugang über Knotenrechner im Ausland gesteuert wird, besteht gleichfalls die Gefahr der vorherigen Löschung der Log-Dateien durch den ausländischen Anbieter. Auch der Datenaustausch in so genannten Chaträumen erweist sich als kaum überprüfbar. Eine Überwachung oder Kontrolle mag im Einzelfall noch möglich sein, wenn solche virtuellen Räume im Internet Relay Chat auch für andere Nutzer frei zugänglich sind. Wenn mehrere Nutzer eigene Räume für einen auch nur kurzen Zeitraum ohne Zutritt für andere eröffnen und danach wieder schließen können, bleiben auch die Strafverfolgungsbehörden ausgeschlossen.

Auch die von einigen Providern, Onlinediensten oder privaten Servern angebotene Anonymisierung von Nachrichten erschwert das Auffinden des Absenders erheblich oder macht dieses nur mit einem sehr hohen Aufwand möglich. Anonymizer (auch Remailer genannt) erschweren die Verfolgung von Tätern und geben ihnen das Gefühl, nicht verfolgbar zu sein. Anonymous-Remailer verwenden Pseudonyme bei E-Mails und News. Der Täter verschickt eine E-Mail an einen Remailer-Server, wo die Absenderangabe durch ein Pseudonym ersetzt wird. Die anonymisierte Nachricht wird anschließend an den Empfänger weitergeleitet. Die Zuordnung des Pseudonyms zum Absender wird automatisch vorgenommen und auf dem Remailer gespeichert, um Antwort-Mails zustellen zu können.[871] Eine bessere Form der Anonymisierung bieten Anonymizer, die keine gespeicherte Zuordnung von Pseudonymen vornehmen, so dass Antwort-Mails ausgeschlossen sind. Cyberpunk-Remailer nehmen verschlüsselte Nachrichten mit chiffrierter Empfängerangabe entgegen, entschlüsseln die Mail und stellen sie ohne Hinweis auf den richtigen Absender zu. Bei Mixmaster-Remailer werden darüber hinaus die ausgehenden Nachrichten verschlüsselt und in exakt gleich lange Pakete zerteilt.[872] Strafverfolgungsbehörden greifen im Rahmen einer Ermittlung auf die Pseudonym-Zuordnungstabellen der Remailer zu. Erst durch die Zuordnung des Anschlusses, des Zeitpunktes seines Zugangs zum Internet, der Log-Dateien und dem verwendeten Pseudonym kann ein Computeranschluss ermittelt werden. Die Behörde muss jedoch Auskünfte und Dateien der Provider und sonstigen privaten Betreiber der Anonymizer erhalten, um an die Daten zu gelangen. Ist ein Anschluss ermittelt worden, so bleibt noch ungewiss, wer an diesem Computer gesessen hat und die Straftat begangen hat.

Darüber hinaus ist es möglich, durch Beobachtung der empfangenen und gesendeten Nachrichten bei dem Remailer Hinweise auf die entsprechenden Absender zu erhalten. Dem können sich die Internetnutzer jedoch weitgehend entziehen, indem sie ihre Nachrichten über mehrere solcher Remailer in verschiedenen Nationen laufen lassen, um eine schnelle Identifizierung zu verhindern.[873] Die Täter fühlen sich hierdurch sicher. Welche der genannten Faktoren dazu führte, dass bei vielen Tätern in der Studie über den Account-Missbrauch ebenfalls die Meinung vorherrschte, dass sie nicht ermittelbar seien, ist in der Studie leider nicht weiter erörtert worden.
Erschwert wird eine Aufklärung zudem dadurch, dass bei der Zusammenarbeit zwischen Verfolgungsbehörden und Service-Providern zum Teil verschiedene Interessen miteinander kon-

[871] Köhntopp 1998, S. 131.
[872] Ebd.
[873] Ebd.

kurrieren. Da die Verhaltenstechniken gerade von Hackern sehr umfangreich und schnell stattfinden, müsste auch eine sehr schnelle Reaktion durch die Strafverfolgungsorgane gegeben sein, um effektiv dagegen vorzugehen. In dieser Hinsicht kommt das geringe computertechnische Wissen vieler Beamter, die mangelnde technische Ausstattung, die Schwerpunktsetzung auf Pornografie und Computerbetrug erschwerend hinzu, sodass Hacker im Allgemeinen nicht das Gefühl bekommen, wirklich verfolgt zu werden.[874] Peter Grabosky meint hierzu:

„Another fundamental issue, at least at the present historical moment, is the difficulty faced by police services around the world in retaining expert computer crime investigators. Much like the priesthood, policing was formerly a lifetime vocation, in many police services today, trained computer crime investigators must battle for the equipment which they regard as nessary to do their job. The development of expertise in forensic computing, moreover, may require a concentration and specialization that precludes the development of the more general expertise required for advancement through the ranks. With the traditional high status areas of policing such as homicide investigation now joined by those of general management as the most prestigious areas of policing, prospects for upward mobility and the part of the computer crime investigator are thus limited.“[875]

Die Internationalisierung des Internets stellt einen Faktor dar, der die Anonymität verstärkt. Peter Grabosky stellt hierzu fest:

„One of the more significant aspects of computer-related crime is its global reach. While international offending is by no means a uniquely modern phenomenon, the global nature of cyberspace significantly enhances the ability of offenders to commit crimes in one country which will affect individuals in a variety of other countries. This poses great challenges for the detection, investigation and prosecution of offenders. Two problems arise in relation to the prosecution of telecommunications offences which have an interjurisdictional aspect: first, the determination of where the offence occurred in order to decide which law to apply and, secondly, obtaining evidence and ensuring that the offender can be located and tried before a court. Both these questions raise complex legal problems of jurisdiction and extradition. If an online financial newsletter originating in the Bahamas contains fraudulent speculation about the prospects of a company whose shares are traded on the Australien Stock Exchange, where has the offence occurred? (...) To be sure, Cyberspace is hardly the first or the only policy domain which lies beyond the control of any single nation state. International air traffic, the

[874] Engel 2003, S. 83 ff.; Gill 2003, S. 389.
[875] Grabosky 2001, S. 36 f.

law of the sea, funds transfers, and such environmental considerations as ozone depletion and global warming, among others, have required concerted international efforts. One would expect that the development of international arrangements in response to computer-related crime will occur in a manner not unlike those which have accompanied other extraterritorial issues, from drug trafficking, to nuclear testing to whaling. Whether the realm of telecommunications will be able to achieve a better record of success than these other enduring global issues remains to be seen."[876]

Grundsätzlich sind alle Informationen auf den mit dem Internet verbundenen Computern ohne territoriale Eingrenzung weltweit verfügbar. Diese Internationalisierung kann ebenfalls verstärkend auf die Anonymität wirken. In den unterschiedlichen Staaten gelten verschiedene Rechtsregeln. Die Internationalisierung des Netzes bringt Probleme für die einzelnen Nationalstaaten mit sich. Die inhaltlichen Standards beispielsweise auf dem Gebiet des Persönlichkeitsrechts und der Meinungsfreiheit und die damit einhergehende Inhaltskontrolle der Medien sind unterschiedlich, je nachdem, aus welchem Staat sie erfolgen.[877] Das Völkerrecht verhindert dabei, dass ein Staat dem anderen seine Regulierungsziele und Instrumente aufzwingt. Problematisch ist, dass im Internet eingespeiste Seiten zwar lokal über einen Server an einem bestimmten Standort eingebracht werden, ein Abruf jedoch auf der ganzen Welt erfolgen kann. Die deutsche Strafverfolgung ist grundsätzlich auf die Bundesrepublik Deutschland begrenzt, soweit nicht europäische oder andere internationale grenzüberschreitende Regelungen möglich sind.[878] Für Rechtshilfe und Ermittlungen im Ausland gelten grundsätzlich die allgemeinen Regeln.[879] Viele Täter agieren vom Ausland aus, wo die entsprechende Tathandlung möglicherweise jedoch nicht unter Strafe gestellt ist. Um dauerhaft erfolgreich die Existenz einheitlicher Rechtsnormen im globalen Netz durchzusetzen, wird eine zukünftige Zusammenarbeit auf internationaler Ebene notwendig sein. Meinungs-, Glaubens- und Interessensunterschiede werden allerdings voraussichtlich Probleme aufwerfen. Jede Gesellschaft hat ihre eigenen Wertvorstellungen, die in dem entsprechenden Recht, in der Verfassung und den Grundrechten ihren Ausdruck finden. Welche Inhalte im Netz zensiert werden und welche nicht, wird durch die einzelnen national unterschiedlichen Normen bestimmt. Demzufolge wird eine internationale Übereinkunft vor allem hinsichtlich der Meinungsfreiheit kaum zu realisieren sein.

[876] Grabosky 2001, S. 49 f.
[877] Janovsky 1998, S. 503 f.
[878] In diesem Zusammenhang kann die Cyber-Crime-Convention genannt werden, die am 08.11.2001 vom Europarat beschlossen wurde, um eine engere europäische Zusammenarbeit im Bereich der Computerkriminalität zu gewährleisten.
[879] Fromm 2003, S. 72 ff.

Die genannten Faktoren minimalisieren die Effektivität der Strafverfolgungsbehörden. Erschwerend kommt das geringe oder zum Teil gänzlich fehlende Computerwissen seitens der polizeilichen Ermittler, Staatsanwälte und Richter hinzu. Selbst die Spezialabteilungen sind oft personell und technisch unzureichend ausgestattet und ausgebildet.[880]

Grundsätzlich kann gesagt werden, dass, je geringer die Wahrscheinlichkeit einer Aufdeckung ist, desto eher die Wahrscheinlichkeit für Kriminalität besteht. Dies erscheint bezogen auf Gelegenheitsstrukturen plausibel. Jedoch führen Gottfredson und Hirschi an anderer Stelle wiederum an, dass gerade risikobehaftete und aufregende Verhaltensweisen von Personen mit Low Self-Control bevorzugt werden.[881] Personen mit Low Self-Control sind risikoliebend und erlebnisgesteuert. Dies ist nach Gottfredson und Hirschi ein Anzeichen für Low Self-Control, womit die Wahrscheinlichkeit von Kriminalitätsentstehung erhöht sei. Gelegenheiten sind jedoch nach deren Aussage wiederum dann erhöht, wenn das Risiko, erwischt zu werden, eher gering ist. Somit scheinen sich die Aussagen bezüglich Low Self-Control und der Wahrscheinlichkeit der Aufdeckung zu widersprechen. Andere Autoren, wie Grasmick, sprechen diese Problematik ebenfalls an: „Inaccurate recall and other problems with self-reported data, as well as the skewed distributions of variables probably are other sources of unexplained variance. In addition, some might also stem from the apparent logical inconsistency between Gottfredson and Hirschi's definition of low self-control, which includes risk seeking, and their definition of criminal opportunity, which includes little risk of detection. To be true to the theory, this inconsistency was incorporated into our operational definitions.“ Diese Annahme bestätigt sich mit den im zweiten Teil aufgezeigten Motiven von einigen Hackern, die gerade den Kick und die Thrills als die eigentlichen Motive ihrer Handlungen ansehen.

Weitere Kontrollinstanzen könnten Firewalls darstellen, da sie das System ähnlich einer Alarmanlage überwachen und vor ungewollten Zugriffen schützen. Jedoch fehlt den Firewalls ein entscheidender Faktor. Zwar versuchen sie, die Computer vor fremden Zugriffen zu schützen, sie haben aber keine alarmierenden Funktionen, die nach außen treten, um so von möglichen Dritten wahrgenommen zu werden. Eine Firewall bleibt intern und unterrichtet im besten Fall den Systemadministrator, der keine hochheitlichen Befugnisse hat, den Täter zu ergreifen. Somit ähnelt eine Firewall eher einer gut geschützten Eingangstür, die jedoch keine

[880] Wetzstein u.a. 1995, S. 218.
[881] Gottfredson/Hirschi 1990, S. 89.

Funktion als Kontrollinstanz erfüllt. Somit kommt der Firewall, wie oben bereits dargestellt, allein im Bereich der suitable targets eine Bedeutung zu.

5. Zusammenfassung und Ausblick

Die vorliegende Arbeit befasst sich mit dem Bereich der Computerkriminalität aus kriminologischer Sicht. Es wurde gezeigt, dass dieser Kriminalitätsbereich bislang kaum untersucht wurde. Auch die bevorzugte Tätergruppe, die Hackerszene, ist bislang nur wenig und undifferenziert betrachtet und analysiert worden. Computerdelikte bieten eine Vielzahl von Anknüpfungspunkten für abweichende oder kriminelle Handlungen und haben zudem eine Bandbreite vom „Kavaliersdelikt“ bis hin zu Virenattacken, die Milliardenschäden verursachen. Daneben zeigte sich, dass Computerkriminalität ein breites Spektrum von Delikten abdeckt. Computerkriminalität erfasst alle Bereiche des Lebens, die in irgendeiner Form digitalisiert worden sind und stellt sich als ein Deliktfeld dar, das sehr schnellen Veränderungen unterworfen ist. Dabei entstehen Bereiche und Handlungen, die sich noch in einer Grauzone bewegen und nur mit umfassendem computertechnischem Fachwissen seitens der Ermittlungsbehörden zu verstehen sind. Aufgrund dieser Problematik ergeben sich auch die damit zusammenhängenden Probleme der Delikterfassung und -zuordnung. Dies spiegelt sich vor allem in der PKS wider. Es wurde in diesem Zusammenhang gezeigt, dass der Begriff Computerkriminalität uneinheitlich definiert und benutzt wird. Dies hängt unter anderem mit der Schnelllebigkeit des Mediums zusammen, die unmittelbar Auswirkungen auf Vorgehensweisen von Tätern hat. Um diesem Problem entgegenzuwirken, wurde eine Definition erstellt, die es möglich macht, Computerdelikte in zwei große Bereiche zu unterteilen: Computerkriminalität i.e.S. und i.w.S. Computerkriminalität im engeren Sinn beinhaltet alle Delikte, die sich gegen das ordnungsgemäße Funktionieren einer elektronischen Datenverarbeitung richten. Computerkriminalität im weiteren Sinn beinhaltet alle Deliktbereiche, bei denen die elektronische Datenverarbeitung eine so gewichtige Bedeutung einnimmt, dass eine Begehung nur mittels des Computers möglich wird. Computerkriminalität i.w.S. wurde offen definiert, damit neue Computerdelikte auch in Zukunft erfasst werden können.

Die Arbeit zeigt zudem, dass Computerkriminalität grundsätzlich im weiteren und im engeren Sinn betrachtet und definiert werden muss, um sie überhaupt strukturiert erfassen zu können. In diesem Zusammenhang wurden im kriminologischen Kontext und unter computertechnischer Betrachtung alle bislang vorherrschenden Delikte dargestellt und erörtert. Dabei wurde anhand von Einzelfällen dargestellt, wie jugendliche Hacker für sie bislang unerreichbare

Kriminalitätsbereiche wie die der Wirtschaftskriminalität erobern. Es konnte gezeigt werden, dass mit den Hackern eine neue Tätergruppe im Bereich der Wirtschaftskriminalität entsteht.

Wichtig ist in dieser Arbeit zudem, dass Computerkriminalität aus zwei unterschiedlichen Perspektiven entsteht: technische Voraussetzungen und Motivation. Ein Virus kann als einfaches Scherzprogramm, das nur ein Bild oder ein Lied erzeugt, bis hin zu einem zerstörerischen Virus, der Daten vernichtet, programmiert sein. Dies zeigt, dass es entscheidend auf die Motivationslage der Täter ankommt, wie ein Übergriff ausfällt. Spezielle Motive bestimmen nicht zwangsläufig auch spezielle computertechnische Übergriffe. Politische Motive können z.B. zum Bau von Viren, zur Veränderung von Webseiten sowie zu gezielten DoS-Angriffen auf staatliche Einrichtungen führen.

Es wurde gezeigt, dass es sich bei Hackern nicht ausschließlich um Jugendliche handelt, sondern um ein weites Täterspektrum. Die Hackerszene ist sehr heterogen ausgestaltet und reicht von unbedarft handelnden Einzeltätern bis hin zu professionellen Gruppierungen. In diesem Zusammenhang hat sich gezeigt, dass es kaum möglich ist, den Hacker als solchen zu definieren, weshalb der Begriff in Medien, Politik und Gesellschaft zum Teil sehr undifferenziert benutzt wird. Dies hängt unter anderem auch mit den unterschiedlichen Motivlagen zusammen, die vom einfachen Spieltrieb über gesellschaftsverändernde Ansätze bis hin zu Racheakten reichen. Dabei zeigte sich, dass eine Unterscheidung in Hacker und Cracker nur aus praktischen Gründen sinnvoll ist, um unterschiedliche Motive aufzuzeigen. Beide Gruppen begehen zum Teil delinquente Handlungen, und selbst in der Szene bezichtigen sich selbst ernannte Hacker gegenseitig als Cracker. Festgehalten werden kann zudem, dass es nur schwer eine positive Definition des Begriffs Hacker im herkömmlichen Sinn geben kann, da das Hacken in jeglicher Form zumindest das Überschreiten von Normen oder Regeln impliziert und ebenso verbotene oder zumindest sozial oder ethisch problematische Vorgehensweisen fördert, unabhängig davon, ob sie einen Straftatbestand darstellen. Es wurde auch deutlich, dass staatliche Normen nicht auf die Motivation von Hackern Einfluss nehmen. Staatliche Normen werden zum Teil aufgrund individueller Abwägungen neutralisiert, zum anderen entwickeln subkulturelle Gruppierungen wie Hacker, Cracker, Virenprogrammierer oder Softwarecracker eigenständige Normen. Dabei spielen unter anderem idealistische Motive, die auf den „freien Zugang zu allen Informationen“ abzielen, eine entscheidende Rolle. Einige sehen das Eindringen in andere Systeme als Kavaliersdelikt an, das nicht bestraft werden dürfe. Und andere wiederum sehen dieses Handeln als eine Notwendigkeit und ihre Aufgabe an, um so die Gesellschaft vor einem größeren Übel zu bewahren. In manchen Gruppen kann sich eine eigene

sellschaft vor einem größeren Übel zu bewahren. In manchen Gruppen kann sich eine eigene Moral und eine interne Belohnungsstruktur durch Ruhm etablieren, die ein Hinwegsetzen über allgemeine ethische und strafrechtliche Konsequenzen erleichtert. Dies zeigen die Verhaltensweisen einiger Hacker, die unbedingt als erste ein Programm „knacken", den besten Virus programmiert oder die meisten und schwierigsten Einbrüche in fremde Systeme begangen haben wollen. Auf diese Weise kann die Gruppe ein Verhalten anregen, zu dem der Hacker als einzelner möglicherweise nicht fähig wäre. Grundsätzlich zeigt die vorliegende Arbeit, dass bezüglich der Hackerszene, ihrer Subkulturen, ihrer Handlungsmuster und ihrer Motive ein erheblicher Forschungsbedarf besteht.

Daneben wurde aufgezeigt, dass auch aus kriminalpolitischer Sicht ein erheblicher Forschungsbedarf besteht. Die Strafverfolgungsbehörden sind kaum ausgebildet und nur unzureichend mit technischen Mitteln ausgestattet. Der Stellenwert der Computerkriminalität scheint hier trotz erheblicher Schäden gering zu sein. Die Struktur der Kriminalität wandelt sich mit dem Computer und dem Internet. Von zu Hause aus können schwerwiegende wirtschaftliche Schäden begangen werden, die zum Teil unkontrollierte Ausmaße annehmen.

Mit der Self-Control Theory haben Gottfredson und Hirschi eine Theorie entwickelt, die ihrer Ansicht nach aufgrund ihrer soziologischen und gelegenheitstechnischen Struktur generelle Erklärungsmuster für kriminelles Verhalten liefern soll. Kriminelles Verhalten ist demnach grundsätzlich die Folge niedriger Selbstkontrolle eines Täters und vorhandener Gelegenheiten. Self-Control entsteht Gottfredson und Hirschi zufolge aufgrund von Sozialisationsprozessen in den ersten acht Lebensjahren. Ob Hacker einen hohen oder niedrigen Grad an Self-Control besitzen, konnte mangels empirischer Untersuchungen über das elterliche Verhalten bezüglich ihrer Kinder nicht beantwortet werden. Vielmehr musste auf Zusammenhänge zurückgegriffen werden, in denen sich laut Gottfredson und Hirschi Anzeichen mangelnder Selbstkontrolle zeigen. Hierbei hat sich gezeigt, dass das Konstrukt Self-Control an einigen Stellen Lücken oder Fehler aufweist und sich teilweise widerspricht. Dies könnte auch daran liegen, dass die von Gottfredson und Hirschi herangezogenen Arbeiten, mit denen sie Self-Control begründen, wie die von Glueck/Glueck (1930) oder McCord (1979) eher als veraltet angesehen werden.

Die Neigung von Personen, kurzfristige Ziele zu bevorzugen und langfristige Ziele zu übersehen, konnte im Bereich der Hackerszene nicht bestätigt werden. Zwar können aufgrund der

unterschiedlichen Gruppierungen nicht alle Hacker gleich behandelt werden, jedoch zeigen zumindest diejenigen Hacker, die in andere Systeme eindringen und Daten ausspähen, im Sinn der Self-Control Theory ein hohes Maß an Selbstkontrolle, da sie durch das Erlangen eines hohen Grads an computertechnischem Fachwissen und einer geplanten Vorgehensweise langfristige Ziele verfolgen. Andere Anhaltspunkte wie Abenteuerlust, Rachegefühle oder eine hohe Anerkennung konnten zum Teil bestätigt werden. Es besteht somit generell keine eindeutige Klärung, ob Hacker über High oder Low Self-Control verfügen. Dies mag zum einen daran liegen, dass die einzelnen Hacker aus unterschiedlichen Untergruppen stammen und unterschiedliche Motive haben, und zum anderen daran, dass die Self-Control Theory aufgrund der sehr hohen Qualifikation und komplexen Vorgehensweise von Hackern in diesem Bereich nicht bestätigt werden kann.

Das Entstehen von Gelegenheiten führen Gottfredson und Hirschi auf die Anwesenheit attraktiver Ziele und das Fehlen von Kontrollinstanzen zurück. Es hat sich gezeigt, dass die Attraktivität der mit dem Computer und dem Internet verbundenen Ziele durch die Digitalisierung eine neue Dimension erreicht hat. Digitalisierte Zielobjekte haben quasi kein physisches Gewicht, so dass das Problem des Abtransports eines Gegenstands in dieser Hinsicht gänzlich entfällt. Zudem ist die Erreichbarkeit von Zielen durch das Internet derart erleichtert worden, dass von jedem Ort aus alle digitalen Zielobjekte zugänglich sind. Viele Instanzen sozialer Kontrolle wie Eltern können diese Funktion mangels computertechnischer Erfahrung nicht ausfüllen. Die Strafverfolgungsbehörden können zudem kaum die Vielzahl der Taten administrativ bearbeiten aufgrund fehlender personeller und ausstattungstechnischer Ressourcen. Verstärkt wird diese Problematik durch den schnellen computertechnischen Wandel im Hardware- sowie im Softwarebereich, der Auswirkungen auf kriminelle Begehungsformen hat. Bei der Strafverfolgung hat sich zudem gezeigt, dass die globale und teilweise anonyme Struktur des Internets dazu führt, dass eine umfangreiche Strafverfolgung kaum realisierbar ist. Die gängigen und bewährten Ermittlungsmethoden von Polizeibehörden und Justiz reichen im Zeitalter der globalen multimedialen Vernetzung nicht mehr aus. Beispielsweise dauert das Verschicken einer verschlüsselten elektronischen Mitteilung zwischen den Kontinenten nur wenige Sekunden. Insbesondere ist infolge des bei Internetstraftaten meist vorhandenen Auslandsbezugs ein Verweis auf den förmlichen Rechtshilfeweg aufgrund der Flüchtigkeit der Daten und der allenfalls kurzen Speicherungsdauer bei Providern und Onlinediensten fast gleichbedeutend mit einem Scheitern der Ermittlungen.

Somit kann festgehalten werden, dass einige Aspekte der Self-Control Theory sich widersprechen und einige gänzlich ungeeignet sind, Computerkriminalität zu erklären. Somit kann die Einschätzung, bei der Self-Control Theory handele es sich um eine „General Theory of Crime", nicht geteilt werden. Es scheint, als ob die Theorie gute Ansätze besitzt, aber es noch weiterer Forschungen bedarf, damit sie alle Variablen enthält, die für eine General Theory of Crime notwendig wären. Gottfredson und Hirschi haben diese Probleme wohl auch schon bei der Entwicklung ihrer Theorie geahnt, weshalb sie ihr Konstrukt sehr vorsichtig definiert haben und es für andere Eigenschaften von Personen als mögliche Gründe für Kriminalitätsentstehung offen ließen: „In our view, lack of self-control does not require crime and can be counteracted by situational conditions or other properties of the individual."[882]

Generell stellt sich hier jedoch die Frage, was eine Theorie noch wert ist, wenn ein zentraler Teil der Aussagen unbrauchbar geworden ist. Hat sie dann noch den wissenschaftlichen Gehalt, den eine kriminologische Theorie haben müsste? Gottfredson und Hirschi führen hierzu jedoch allgemein aus: „The source of any theory is an idea, an idea the theory itself attempts to articulate or express. As a result, tests of theory are tests of the articulation of an idea and, if done properly, of the value of the idea itself. The idea that serves as the basis for A General Theory of Crime (Gottfredson and Hirschi 1990) is the idea of control, an idea with deep roots in the thinking of ordinary people, an idea that has been used to make sense of a variety of observations in many fields of study. We are not the first to explore the implications for crime of the idea of control, and we doubt that we will be the last. We do not presume to own the idea, and do not see ourselves as spokesmen in its defense."[883]

Den Gehalt einer Theorie lediglich in einer neuen Idee zu sehen, scheint zu wenig. Die Self-Control Theory hat seit ihrer Veröffentlichung viel berechtigte Kritik erfahren. Die Theorie hat zwei Dimensionen: Self-Control und Gelegenheiten. Das eigentlich Neue an der Theorie ist jedoch Self-Control. Gelegenheiten sind in Anlehnung an Cohen und Felson weitgehend übernommen worden. Die vorliegende Arbeit kann jedoch nicht die Annahmen von Gottfredson und Hirschi bezüglich Self-Control und ihrer Parameter bestätigen. Self-Control als Erklärungsansatz lässt sich nicht überzeugend auf Computerkriminalität, geschweige denn auf Hackerkriminalität anwenden. Ein wesentlicher Teil der Self-Control Theory ist für die kriminologische Forschung nicht geeignet, da sie Motive für Kriminalität nicht in angemessener Form erklären kann.

[882] Gottfredson/Hirschi 1990, S. 89.
[883] Gottfredson/Hirschi 1993, S. 47.

Literaturverzeichnis

Akers, Roland L. — Self-Control as a General Theory of Crime
in:
Journal of Quantitative Criminology 1991, 7
S. 201-211
(zit.: Akers 1991)

Akers, Roland L. — Self Control and Criminal Opportunity:
A Prospective Test of the General Theory of Crime
in:
Social Problems 1998, 45
S. 102-113
(zit.: Akers 1998)

Arneklev, Bruce J./
Grasmick, Harald G./
Tittle, Charles R./
Bursit, Robert J. — Low Self-Control and Imprudent Behavior
in:
Journal of Quantitative Criminology 1993, 9
S.225-247
(zit.: Arneklev u.a. 1993)

Arneklev, Bruce J./
Grasmick, Harald G./
Bursit, Robert J. — Evaluation of the Dimensionality –
an Invariance of Low Self Control
in:
Journal of Quantitative Criminology 1999, 15
S. 307-331
(zit.: Arneklev/Grasmick/Bursit 1999)

Anonymus — Hacker's Guide - Sicherheit im Internet und im lokalen Netz. München 2003. (zit.: Anonymus 2003)

Barth, Thomas — Soziale Kontrolle in der Informationsgesellschaft - Systemtheorie, Foucault und die Computerfreaks als Gegenmacht zum Panoptismus der Computer- und Multimedia-Kultur. Frankfurt a. M. 1997. (zit.: Barth 1997)

Barton, Dirk — Multimedia-Strafrecht - Ein Handbuch für die Praxis. Neuwied 1999. (zit.: Barton 1999)

Bartusch, Dawn R. Jeglum/ Lyanm, Donald R./ Moffit, Terrie E./ Silva, Phil A. — Is Age Important? Testing a General versus a Developmental Theory of Antisocial Behavior. in: Criminology 1997, 35. S. 13-48. (zit.: Bartusch u.a. 1997)

Becker, Howard S. — Regelverletzung und Abweichung. in: Abweichung und Kriminalität - Konzeptionen, Kritik, Analysen. Hamburg 1975. S. 18-32. (zit.: Becker 1975)

Bendit, René/
Erler, Wolfgang/
Nieborg, Sima/
Schäfer, Heiner — Kinder- und Jugendkriminalität,
Opladen 2000
(zit.: Bendit u.a. 2000)

Bentham, Jeremy — An Introduction of the Principles of Morals and Legislation
London 1970
(zit.: Bentham 1970)

Beukelmann, Stefan — Prävention von Computerkriminalität,
Frankfurt a. M. 2001
(zit.: Beukelmann 2001)

Britt, Chester L. — Comment on Paternoster and Brame
in:
Crimonology 2000, 38
S. 965-982
(zit.: Britt 2000)

Burton Jr.,Velmer S./
Evans, T. David/
Cullen, Francis T./
Olivares, Kathleen M./
Dunaway, R. Gregory — Age, Self-Control, and Adults' Offending Behaviors:
A Research Note Assessing a General Theory of Crime
in:
Journal of Criminal Justice 1999, 27
S. 45-54
(zit.: Burton u.a. 1999)

Chaos Computer Club/
Wieckmann, Jürgen — Das Chaos Computer Buch,
Hacking made in Germany
Hamburg 1988
(zit.: CCC/Wieckmann 1988)

Clarke, Ronald V./
Felson, Markus — Routine Activity and Rational Choice
New Jersey 1993
(zit.: Clarke/Felson 1993)

Cohen, Albrecht K./
Short, James F. Jr. — Zur Erforschung delinquenter Subkulturen
in:
Sack, Fritz und König, René (Hg.):
Kriminalsoziologie
Wiesbaden 1979
S. 372-394
(zit.: Cohen/Short 1979)

Cohen, L. E./
Felson, M. — Social Change and Crime Rate Trends -
A Routine Activity Approach
in:
American Sociological Review 1979, 44
S. 588–608
(zit.: Cohen/Felson 1979)

Colvin, Mark/
Cullen, F.T./
Vander Ven, T. — Coercion, Social Support, and Crime -
An Emerging Theoretical Consensus
in:
Criminology 2002, 40

S. 19-42
(zit.: Colvin 2002)

Coradi, Maja — MUDs - Faszinierende virtuelle Welten -
Ein Vergleich der Selbstdarstellung in Multi-User-Dungeons und im "Realen Leben" mit Hilfe von Theorien Erving Goffmans
1997
in:
http://socio.ch/intcom/t_mcorad01.htm
(zuletzt eingesehen am 11.02.05)
(zit.: Coradi 1997)

Denning, Dorothy — Activism, Hacktivism, and Cyberterrorism -
The Internet as a Tool for Influencing Foreign Policy,
1999
in:
http://69.44.62.160/gps/info-policy/workshop/papers/denning.html
(zuletzt eingesehen am 15.03.05)
(zit.: Denning 1999)

Eckert, Roland/
Vogelgesang, Waldemar/
Wetzstein, Thomas A./
Winter, Rainer — Auf digitalen Pfaden -
Die Kulturen von Hackern, Programmierern, Crackern und Spielern
Darmstadt 1991
(zit.: Eckert u.a. 1991)

Eifler, Stefanie — Einflussfaktoren von Alkoholkonsum:
Sozialisation, Self-Control und differentielles Lernen
Wiesbaden 1997

(zit.: Eifler 1997)

Eifler, Stefanie
Machen Gelegenheiten Raucher? -
Theoretische und empirische Analysen der Beziehungen zwischen Self-Control, Ressourcen und dem Genuss von Tabakwaren
in:
Soziale Probleme 1998
Heft 1/2
S. 90-116
(zit.: Eifler 1998)

Eifler, Stefanie
Routineaktivitäten und Gelegenheiten –
Eine quasi-experimentelle Untersuchung situativer Einflüsse auf das Verhalten
in:
Bielefelder Arbeiten zur Sozialpsychologie Nr. 190
Bielefeld 1999
S. 1-16
(zit.: Eifler 1999)

Eisenberg, Ulrich
Kriminologie
6. Auflage
München 2005
(zit.: Eisenberg 2005)

Engel, Christian
Bekämpfung der Internetkriminalität nur durch Mithilfe von Spezialisten möglich
in:
Die Kriminalpolizei 2003
Heft 3
S. 83-86
(zit.: Engel 2003)

Eser, Albin/
Kaiser, Günther/
Weigend, Ewa — Drittes deutsch-polnisches Kolloquium über Strafrecht und Kriminologie
Baden-Baden 1986
(zit.: Eser/Kaiser/Weigend 1986)

Evans, T. David/
Cullen, Francis T./
Burton, Velmer S./
Dunaway, R. Gregory/
Bewon, Michael L. — The Social Consequences of Self-Control -
Testing the General Theory of Crime
in:
Criminology 1997
S. 475–504
(zit.: Evans u.a. 1997)

Fattah, Ezzat A. — Criminology: Past, Present, and Future -
A Critical Overview
New York 1997
(zit.: Fattah 1997)

Freedman, David H. — How to Hack a Bank
2000
in:
http://www.forbes.com/asap/2000/0403/056.html
(zuletzt eingesehen am 20.10.05)
(zit.: Freedman 2000)

Fromm, Heinz — Extremismus im Internet
in:
Schriftenreihe Deutsche Strafverteidiger e.V., Bd. 23

Kriminalität@net
Jürgen Welp (Hrsg.)
Baden-Baden 2003
(zit.: Fromm 2003)

Gantar, Reinhard
Sasser und die Folgen
in:
Telepolis, Magazin der Netzkultur
vom 17.05.2004
in:
http://www.heise.de/tp/deutsch/inhalt/te/17433/1.html
(zuletzt eingesehen am 03.08.05)
(zit.: Gantar 2004)

Geiger, Gebhard
Information Warfare –
Bedrohung und Schutz IT-abhängiger gesellschaftlicher Infrastrukturen
Datenschutz und Datensicherheit 2000
S. 129-136
(zit.: Geiger 2000)

Gerlach, Henrik
Ausblick auf internationale und supranationale Ansätze zur Kontrolle der „cyber-crimes“ (inkl. Datenschutz-Problematik)
2003
http://www.jura.uni-bonn.de/institute/krimsem/Cyber-Crime/Left/Empirisches/Wissenschaft/CyberCrime-CyberCrimeKontrolle-SS2003/SammlungCyberCrime/Gerlach.pdf
(zuletzt eingesehen am 21.11.05)
(zit.: Gerlach 2003)

Gill, Peter
Bekämpfung der Computerkriminalität -
Bericht über das Forensic-Team der Staatsanwaltschaft Basel-Stadt

in:
Kriminalistik 2003, 6
S. 389-390
(zit.: Gill 2003)

Girtler, Roland — Die Randkultur der Hacker –
Rebellen, Spione und Diebe
in:
Elektronik und Informationstechnik 2003
S. 216-219
(zit.: Girtler 2003)

Glaser, Daniel — Criminality Theories and Behavioral Images
in:
American Journal of Sociology 1956, 61
S. 433-444
(zit.: Glaser 1956)

Geis, Gilbert — On the Absence of Self-Control as the Basis for General Theorie of Crime-
A Critique
in:
Theoretical Criminology 2000, 4
S. 35-53
(zit.: Geis 2000)

Glueck, Sheldon/
Glueck, Elearon — 500 Criminal Careers
New York 1930
(zit.: Glueck/Glueck 1930)

Gottfredson, Michael R./
Hirschi, Travis — A General Theory of Crime
Stanford 1990
(zit.: Gottfredson/Hirschi 1990)

Gottfredson, Michael R./
Hirschi, Travis — Commentary: Testing the General Theory of Crime
in:
Journal of Research in Crime and Delinquency
1993, 30
S. 47-53
(zit.: Gottfredson/Hirschi 1993)

Gottfredson, Michael R./
Hirschi, Travis — The Generality of Deviance
New Brunswick 1994
(zit.: Gottfredson/Hirschi 1994)

Göppinger, Hans — Kriminologie
5. Auflage
München 1997
(zit.: Göppinger 1997)

Grabosky, Peter — Computer Crime -
A Criminological Overview
in:
Forum on Crime and Society
2001, 1
S. 35-53
(zit.: Grabosky 2001)

Graf, Jürgen — Internet –
Straftaten und Strafverfolgung
in:

Deutsche Richterzeitung 1999
S. 281-286
(zit.: Graf 1999)

Grasmick, Harold G./
Tittle, Charles R./
Bursik, Robert J./
Arnekker, Bruce J. Testing the Core Empirical Implications of Gottfredson and Hirschi Genaral Theory of Crime
in:
Journal of Research in Crime and Delinquency
1993, 30
Seite 5–29
(zit.: Grasmick u.a. 1993)

Groebel, Jo Internet 2002: Deutschland und die digitale Welt - Internetnutzung und Medieneinschätzung in Deutschland und Nordrhein-Westfalen im internationalen Vergleich,
Schriftenreihe Medienforschung der LfM,
Bd. 46
Opladen 2003
in:
http://www.lfm-nrw.de/downloads/internetstudie.pdf
(zuletzt eingesehen am 28.05.05)
(zit.: Groebel 2003**)**

Gröndahl, Boris Hacker
Hamburg 2000
(zit.: Gröndahl 2000)

Gühne, Gerd Sicherheitslücken in Microsoft Windows Netzwerken
2002
in:
http://www.marfir.rhcs.de/DVBeleg.pdf

(zuletzt eingesehen am 20.10.05)
(zit.: Gühne 2002)

Hartmann, Frank — Wirtschaftskriminalität im Internet - Geschäftsrisiken durch Computermissbrauch und Datenspionage Köln 2001 (zit.: Hartmann 2001)

Hayslett-McCall, Karen L./ Bennard, Thomas J. — Attachment, Masculinity and Self-Control - A Theory of Male Crime Rates in: Theoretical Criminology 2002, 6 S. 5–33 (zit.: Hayslett-McCall/Bennard 2002)

Hebecker, Eike — Die Netzgeneration - Jugend in der Informationsgesellschaft Frankfurt/Main 2001 (zit.: Hebecker 2001)

Helmbrecht, Udo — Viren – Die niemals endende Bedrohung in: http://www.manager-magazin.de/ebusiness/cebit/0,2828,289175,00.html (zuletzt eingesehen am 13.07.05) (zit.: Helmbrecht 2004)

Helmers, Sabine — Per Mausklick zur Couch Potatoe - Über die Welt des Internets, gewachsene kulturelle Ordnungen und gegenwärtige Turbulenzen in: Fred Schell, Bernd Schorb und Hans-Jürgen Palme (Hrsg.)

Jugend auf der Datenautobahn -
Sozial-, gesellschafts- und bildungspolitische Aspekte von Multimedia
München 1995
S. 38-46
(zit.: Helmers 1995)

Hess, Henner/
Scheerer, Sebastian — Theorie der Kriminalität
in:
Dietrich Oberwittler und Susanne Karstedt (Hrsg.)
Soziologie der Kriminalität 2004
S. 69-92
(zit.: Hess/Scheerer 2004)

Hirschi, Travis/
Gottfredson, Michael R. — In Defense of Self-Control
in:
Theoretical Criminology
2000, 4
S. 55-69
(zit.: Hirschi/Gottfredson 2000)

Hirschi, Travis — Causes of Delinquency
Berkeley 1969
(zit.: Hirschi 1969)

Himanen, Pekka — Die Hacker-Ethik -
Und der Geist des Informations-Zeitalters
München 2001
(zit.: Himanen 2001)

Huegen, Craig — The Latest in Denial of Service Attacks: “Smurfing”
Description and Information to Minimize Effects

2000
in:
http://www.pentics.net/denial-of-service/white-papers/smurf.cgi
(zuletzt eingesehen am 16.04.05)
(zit.: Huegen 2000)

Jaeger, Stefan — Computerkriminalität
Augsburg 2002
(zit.: Jaeger 2002)

Janovsky, Thomas — Internet und Verbrechen -
Die virtuelle Komponente der Kriminalität
in:
Kriminalistik 1998, 7
S. 500-504
(zit.: Janovsky 1998)

Jessen, Ernst — Zugangsberechtigung und besondere Sicherung im Sinne von § 202a StGB
Frankfurt am Main 1994
(zit.: Jessen 1994)

Kaiser, Günther — Jugendkriminalität -
Rechtsbrüche, Rechtsbrecher und Opfersituationen im Jugendalter
3. Auflage
Basel 1982
(zit.: Kaiser 1982)

Kaiser, Günther — Kriminologie -
Ein Lehrbuch
3. Auflage
Heidelberg 1996
(zit.: Kaiser 1996)

Karstedt, Susanne/
Greve, Werner — Die Vernunft des Verbrechens -
Rational, irrational oder banal? Der „Rational-Choice“-Ansatz
in der Kriminologie
in:
Bussmann, K.-D. und Kreissl, R. (Hrsg.):
Kritische Kriminologie in der Diskussion;
Opladen 1996
S. 171-210
(zit.: Karstedt/Greve 1996)

Keupp, Heinrich — Abweichung und Alltagsroutine -
Die Labeling-Perspektive
in:
Theorie und Praxis
Köln 1976
S. 51-107
(zit.: Keupp 1976)

Konrad, Rachel — What Makes a Hacker Hack?
in:
News Security
Februar 2002
in:
http://news.zdnet.com/2100-1009_22-831095.html
(zuletzt eingesehen am 20.10.05)
(zit.: Konrad 2002)

Köhntopp, Marit — Stacheldraht im Internet
in:
Stefan Bollmann und Christiane Heidbach (Hrsg.)
Kursbuch Internet -
Anschlüsse an Wirtschaft und Politik, Wissenschaft und Kultur
Hamburg 1998

S. 125-141
(zit.: Köhntopp 1998)

Kubica, Johann — Internetkriminalität -
Wesentliche Erscheinungsformen und Bekämpfungsmaßnahmen
in:
Die Kriminalpolizei 2001,3
S. 75-80
(zit.: Kubica 2001)

La Grange, Teresa C. /
Silverman, Robert A. — Low Self Control and Opportunity -
Testing the General Theory of Crime as an Explanation
for Gender Differences in Delenquency
in:
Criminology 1999, 37
S. 41-72
(zit.: La Grange/Silverman 1999)

Lamnek, Siegfried — Neue Theorien abweichenden Verhaltens
2. Auflage
München 1997
(zit.: Lamnek 1997)

Lamnek, Siegfried — Jugendkriminalität. Erscheinungen – Entwicklungen
– Erklärungen
in:
Gegenwartskunde –
Zeitschrift für Gesellschaft, Wirtschaft, Politik und Bildung.
1998
S. 379-412
(zit.: Lamnek 1998)

Levy, Steven — Hackers - Heroes of the Computer Revolution, New York 1984 (zit.: Levy 1984)

Lilly, J. Robert/ Cullen, Francis T./ Ball, Richard A. — Criminological Theory - Context and Consequences, Second Edition, Thousand Oaks, 1995 (zit.: Lilly u.a. 1995)

McCord, William — Some Child-Rearing Antecedents of Criminal Behavior in Adult Man, in: Journal of Personality and Social Psychology 1979, 37 S. 1477–1486 (zit.: Mc Cord 1979)

Medosch, Armin/ Röttgers, Janko — Netzpiraten - Die Kultur des elektronischen Verbrechens, Hannover 2001 (zit.: Medosch/Röttgers 2001)

Meier, Bernd-Dieter — Kriminologie, 2. Auflage, München 2005 (zit.: Meier 2005)

Meier, Bernd-Dieter — Softwarepiraterie – eine Straftat? – Überlegungen zum Strafrechtsschutz für

Computerprogramme
in:
Juristenzeitung 1992
S. 657-665
(zit.: Meier 1992)

Merton, Robert K. Sozialstruktur und Anomie
in:
Sack, Fritz und König, René (Hrsg.)
Kriminalsoziologie
Wiesbaden 1979
S. 360-371
(zit.: Merton 1979)

Mitnick, Kevin D./
Simon, William L. Die Kunst der Täuschung -
Risikofaktor Mensch
Bonn 2003
(zit.: Mitnick/Simon 2003)

Moschitto, Denis/
Sen, Evrim Hackerland -
Das Logbuch der Szene
Köln 1999
(zit.: Moschitto/Sen 1999)

Möhrenschlager, Manfred Computerstraftaten und ihre Bekämpfung in der Bundesrepublik Deutschland
in:
Zeitschrift für Wirtschaft, Steuer und Strafrecht 1991
S.321-331
(zit.: Möhrenschlager 1991)

Mörth, Ingo
Regionale Kultur- und Medienszenen -
Eine explorative Analyse ihrer Merkmale und ihres Verhältnisses zum Ars Electronica Center Linz
Linz 2003
(zit.: Mörth 2003)

Mulhall, Tom
Where have All the Hackers Gone? -
A Study in Motivation, Deterrence, and Crime Displacement.
in:
Computers & Security
Heft 16
1997
S. 277-284
(zit.: Mulhall1997)

Nikoltchev, Susanne
Filme im Internet –
Zwischen Urheberrechten und redlicher Nutzung
in:
Rechtliche Rundschau der europäischen audiovisuellen Informationsstelle
Ausgabe 4/2002
Straßburg
http://www.obs.coe.int/oea_publ/iris/iris_plus/iplus4_2002.pdf.de
(zuletzt eingesehen am 29.01.05)
(zit.: Nikoltchev 2002)

Ohrmund, Andreas/
Tiedemann, Paul
Internet für Historiker –
Eine praxisorientierte Einführung
Darmstadt 1999
(zit.: Ohrmund/Tiedemann 1999)

Opaschowski, Horst — Generation @ -
Die Medienrevolution entlässt ihre Kinder:
Leben im Informationszeitalter
Hamburg 1999
(zit.: Opaschowski 1999)

Opaschowski, Horst — Der gläserne Konsument -
Die Zukunft von Datenschutz und Privatsphäre in einer vernetzten Welt
Hamburg 2001
(zit.: Opaschowski 2001)

Paternoster, Raymond/
Brame, Robert — Multiple Routes to Delinquency? -
A Test of Developmental and General Theories of Crime
in:
Criminology 1997, 35
S. 49-84
(zit.: Paternoster/Brame 1997)

Paternoster, Raymond/
Brame, Robert — On the Association among Self-Control, Crime, and Analogous Behaviors
in:
Criminology 2000, 38
S. 971-982
(zit.: Paternoster/Brame 2000)

Picko, Helmut — Der Computer als Tat- und Beweismittel –
Computerkriminalität: Dialer
in:
Der Kriminalist 2000, 34
S. 282-286
(zit.: Picko 2002)

Polakowsky, Michael — Linking Self- and Social Control with Deviance - Illuminating the Structure Undelying a General Theoery of Crime and its Relation to Deviant Activity
in:
Journal of Quantitative Criminology 1994, 10
S. 41–78
(zit.: Polakowsky 1994)

Popitz, Heinrich — Über die Präventivwirkung des Nichtwissens - Dunkelziffer, Norm und Strafe
in:
Recht und Staat in Geschichte und Gegenwart
Tübingen 1968
S. 3-25
(zit.: Popitz 1968)

Power, Richard — Attacken im Web - Fälscher, Hacker, Datenklauer – Die Schattenseiten des Cyberspace
München 2001
(zit.: Power 2001)

Pratt, Travis C./
Cullen, Francis T. — The Empirical Status of Gottfredson und Hirschi's General Theory of Crime: A Meta-Analysis
in:
Criminology 2000, 38
S. 501-534
(zit.: Pratt/Cullen 2000)

Puaschitz, Martin — Hacker
2002
in:
http://it-academy.cc/content/glossary_browse.php?ID=1023
(zuletzt eingesehen am 16.11.05)

(zit.: Puaschitz 2002)

Raithel, Jürgen/
Mansel, Jürgen — Kriminalität und Gewalt im Jugendalter –
Hell- und Dunkelbefund im Vergleich
Weinheim 2003
(zit.: Raithel/Mansel 2003)

Raymond, Eric — The New Hacker's Dictionary
Cambridge, Massachusetts/USA 1996
(zit.: Raymond 1996)

Raymond, Eric — The Cathedral and the Bazaar -
Musings on Linux and Open Source by an accidental Revolutionary
Beijing 1999
(zit.: Raymond 1999)

Rentrop, Christian — Hacker, Cracker, Script-Kiddie: Eine Begriffsklärung
http://www.sec-world.net/news/67766-hacker-cracker-scriptkiddie-eine-begriffserklaerung.html
2004
(zuletzt eingesehen am 26.04.05)
(zit.: Rentrop 2004)

Robins, Lee — Deviant Children Grown up
Baltimore 1966
(zit.: Robins1966)

Russel, Ryan/
Cunningham, Stace — Das Hacker-Buch -
Bonn 2001
(zit.: Russel/Cunningham 2001)

Scheerer, Sebastian — Ein theoretisches Modell zur Erklärung von sozialrevolutionärer Gewalt
in:
Hess, Henner u.a.(Hrsg.)
Angriff auf das Herz des Staates
Frankfurt am Main 1988
S. 75-189
(zit.: Scheerer 1988)

Scheerer, Sebastian — Kriminalität der Mächtigen
in:
Kaiser, Günther u.a. (Hrsg.)
Kleines kriminologisches Wörterbuch
Heidelberg 1993
S. 246-249
(zit.: Scheerer 1993)

Schneider, Hans Joachim — Kriminologie
3. Auflage
München 1992
(zit.: Schneider 1992)

Schneider, Hans Joachim — Kriminologie für das 21. Jahrhundert -
Schwerpunkte und Fortschritte der internationalen Kriminologie
Münster 2001
(zit.: Schneider 2001)

Schneider, Hans-Jochen — Lexikon der Informatik und Datenverarbeitung,
München 1997
(zit.: Schneider 1997)

Schönstein, Jürgen — Ahnungslose Opfer -
Ex-Hacker Kevin Mitnick verrät, wie kriminelle Profis Firmen

und Behörden ausspionieren, bevor sie in deren Computersysteme eindringen.
in:
Focus 2002, 44
S. 126-128
(zit.: Schönstein 2002)

Schulze, Gerhard — Die Erlebnisgesellschaft -
Kultursoziologie der Gegenwart
Frankfurt a. Main/New York 1997
(zit.: Schulze 1997)

Schwind, Hans-Dieter — Kriminologie -
Eine praxisorientierte Einführung mit Beispielen
8. Auflage
Heidelberg 2004
(zit.: Schwind 2004)

Shinder, Debra Littlejohn — Scene of the Cybercrime -
Computer Forensics Handbook
Rockland, MA 2002
(zit.: Shinder 2002)

Sieber, Ulrich — Computerkriminalität und Strafrecht -
Köln 1980
(zit.: Sieber 1980)

Sieber, Ulrich — Missbrauch der Informationstechnik und Informationsstrafrecht-Entwicklungstendenzen in der internationalen Informations- und Risikogesellschaft.
in:
Tauss/Kollbeck (Hrsg.)
Deutschlands Weg in die Informationsgesellschaft :
Herausforderungen und Perspektiven für Wirtschaft,

Wissenschaft, Recht und Politik
Baden-Baden 1996
S. 608 - 651
(zit.: Sieber 1996)

Sieber, Ulrich — Multimediarecht – Strafrecht und Strafprozessrecht -
München 1999
(zit.: Sieber 1999)

Stillich, Sven/
Liedtke, Dirk — Der Wurm von der Wümme
2004
in:
http://www.stern.de/computer-technik/internet/?id=525454
(zuletzt eingesehen am 14.10.05)
(zit.: Stillich/Liedtke 2004)

Stoll, Clifford — Kuckucksei -
Die Jagd auf die deutschen Hacker, die das Pentagon knackten.
Frankfurt a. Main 2001
(zit.: Stoll 2001)

Streck, Ralf — Größter Schlag gegen Europas Piraterie?
2004
in:
http://www.heise.de/tp/deutsch/special/copy/16547/1.html
(zuletzt eingesehen am 22.02.05)
(zit.: Streck 2004)

Sykes, Gresham M./
Matza, David — Techniken der Neutralisation -
Eine Theorie der Delinquenz
in:
Sack, Fritz und König, René (Hrsg.)

Kriminalsoziologie
Wiesbaden 1979
S. 360-371
(zit.: Sykes/Matza 1979)

Szallies, Daniel/
Längsfeld, Carsten — Netzsicherheit -
Seminararbeit im Proseminar IT-Sicherheit am Fachgebiet Programmiermethodik, Technische Universität Darmstadt
2001
in:
http://www.computec.ch/dokumente/allgemein/netzwerksicherheit/netzwerksicherheit.pdf
(zit.: Szallies/Längsfeld 2001)

Taylor, Paul A. — Hackers -
Crime in the Digital Sublime
New York 2001
(zit.: Taylor 2001)

Tittle, Charles R. — Control Balance -
Toward a General Theory of Deviance
Colo u.a. 1995
(zit.: Tittle 1995)

Troxler, Peter — Virtual Criminology Report –
Bericht von McAfee zum Thema virtuelle Kriminalität – Erste europaweite Studie über das organisierte Verbrechen und das Internet
München 2005
(zit.: Troxler 2005)

Turkle, Sherry — Die Wunschmaschine -
Der Computer als zweites Ich

New York 1984
(zit.: Turkle 1984)

Turkle, Sherry — Leben im Netz -
Identität in Zeiten des Internets
Hamburg 1999
(zit.: Turkle 1999)

Vick, Jens/
Roters, Franz — Account-Missbrauch im Internet -
Ein Sammelverfahren mit anschließender kriminologischer Auswertung
Bundeskriminalamt Wiesbaden 2003
(zit.: Vick/Roters 2003)

Voss, Andreas — Das große PC- und Internet-Lexikon 2004
Düsseldorf 2004
(zit.: Voss 2004)

Vogelgesang, Waldemar — Wie beeinflusst das Netz die Jugendkultur?
Das Internet als jugendkulturelle Arena
2003
in:
http://www.waldemar-vogelgesang.de/mainz.pdf
(zuletzt eingesehen am 15.08.05)
(zit.: Vogelgesang 2003)

Walter, Michael — Jugendkriminalität -
Eine systematische Darstellung
3. Auflage
Stuttgart 2005
(zit.: Walter 2001)

West, Donald/
Farrington, David — Who becomes Delinquent?
London 1973
(zit.: West/Farrington 1993)

Wetzstein, Thomas A./
Dahm, Hermann/
Steinmetz, Linda/
Lentes, Anja/
Schampaul, Staphan/
Eckert, Roland — Datenreisende -
Die Kultur der Computernetze
Opladen 1995
(zit.: Wetzstein u.a. 1995)

Wiedemann, Peter — Tatwerkzeug Internet -
Ein Überblick über das System und seine kriminelle Nutzung
in:
Kriminalistik 2000, 4
S. 229-239
(zit.: Wiedemann 2000)

Winter, Rainer — Medien und Fans -
Zur Konstellation von Fan-Kulturen
in:
Kursbuch Jugendkultur. Stile, Szenen, Identitäten vor der Jahrtausendwende
Mannheim 1997
S. 40-53
(zit.: Winter 1997)

Wischner, Stefan — Frisch gepresst -
MP3-Files abspielen

in:
Chip Extra 2000, 1
S. 40–43
(zit.: Wischner 2000)

Wolf, Ilse/
Wolf, Rudolf — Software-Piraterie ist kein Kavaliersdelikt –
2000
in:
http://www.monitor.co.at/index.cfm?storyid=2583
(zuletzt eingesehen am 19.10.05)
(zit.: Wolf/Wolf 2000)

Zehnder, Matthias — Geschichte und Geschichten des Internets
Kilchberg 1998
(zit.: Zehnder 1998)

Zimmerman, Christian — Der Hacker -
Computerkriminalität: Die neue Dimension des Verbrechens
München 2002
(zit.: Zimmermann 2002)

Zimprich, Stefan — Spam-Gesetze -
Das Prinzip Hoffnung
2004
in:
http://www.spiegel.de/netzwelt/politik/0,1518,298784,00.html
(zuletzt eingesehen am 23.09.05)
(zit.: Zimprich 2004)