Hacker-Ethik

Die ursprüngliche Ethik der Hacker-Kultur [1, 3]

In den 1950er- und 1960-Jahren entwickelte sich in den vereinigten Staaten in meist universitärem Rahmen, so zum Beispiel an den Institutionen MIT und Standford, eine Kultur von Gleichgesinnten Spezialisten in Computern und Kommunikation, die sich mit dem Problem ausseinandersetzten, dass Computerrechenleistung und Informationsdatenbanken nur in der Hand grosser Gesellschaften und dem Staat waren. Man war sich in diesen Kreisen einig, dass Information und Technologie jedem zugänglich sein sollten. Ausserdem stand man Autorität prinzipiell mistrauisch gegenüber, da man der Meinung war, Autoritäre Körper tendierten eher zu Korruption, Geheimhaltung und Hortung von Informationen, Technologie und Wissen. Der "Personal Computer" als Gegenkraft zum "Mainframe" wurde insofern als wünschenswerte Technologie angesehen, da er die Macht dezentralisiert, und jedem ermöglicht Informationen zu erstellen, auszutauschen, und zu sammeln. So dreht sich der Kodex der "alten Hacker" aus den 1960-Jahren primär um Wert- und Gesellschafts-Ideale.

Veränderte moralische Richtlinien in den 1990er-Jahren [1, 3]

Mit der Verbreitung des Personal Computers und der immer grösseren Vernetztheit zwischen privaten Nutzern wuchs das Potential, global Einfluss auf die Computerbranche und auch die Gesellschaft zu nehmen. Auch konnten bösartige Aktivitäten immer höhere Wellen schlagen. Deshalb finden sich im Verlauf der Zeit immer mehr Verhaltensregeln in der "Untergrundethik" der Hacker. Das Eindringen in Fremdsysteme zum Zweck der "Erkundung" oder zum Nutzen brachliegender Ressourcen wird als vertretbar angesehen. Zwar wird der Privatsphäre jeder Person Respekt gezollt, jedoch wird nie klar definiert, inwieweit das Ausspähen von Informationen erlaubt ist, und wo es beginnt, die Privatspähre zu verletzen. Weiterhin ist es erwünscht, sich gegen Autorität zu sträuben, und sich ihr zu wiedersetzen, wo sie im Weg des freien Informationsaustausches steht. Softwarepiraterie wird als vernünftige und gar positive Handlung angesehen, da sie anderen Personen erlaubt, Software vor dem Kauf auszuprobieren, und weil die jeweilige Software kostenfrei an Bekanntheit gewinnt. Hacker sehen ihre Autoritätswiederspänstigkeit als Dienst an der Gesellschaft: Wenn Unternehmen wissen, dass sie gehackt werden können, werden sie ihre Macht nicht missbrauchen oder überschreiten.

Kritik an der modernen Hacker-Ethik [1]

Der "Kodex" der modernen Hacker wird als zu idealistisch und nicht praktikabel angesehen. Hacken sei prinzipiell eine individuelle, egozentrische Tätigkeit, und die "Community" somit lediglich ein Mittel zum Zweck der Bekräftigung eigener Interessen. Es gibt keine einheitliche Hacker-Ethik, sondern Regeln bilden sich mehr oder weniger Willkürlich, da es sich auch nicht um einen professionellen Kodex handelt.

"Hacken" als Kunst [2]

Völlig anders an in den Medien bekannt, bezeichnen sich manche Programmierer, und vertreter der Open-Source-Bewegung als "Hacker". Hacken bedeutet in diesem Kontext, elegante Lösungen zu finden, und Technologie auf innovative Art und Weise einzusetzen. Diese Form des "Hackens" hat

nichts mit dem Eindringen auf Fremdmaschienen zu tun. Personen, die letzteres begehen, werden von Hackern als “Cracker” bezeichnet und verachtet. “Hackers build things, crackers break them” ist hier das Motto. Auch diese Hacker berufen sich auf gewisse Grundsätze. Zentral ist hier das Interesse am Finden neuer Problemlösungen. Langeweile und monotone, repetitive Arbeit werden stark negativ Empfunden, da sie den Hacker von dem abhalten, was er am besten kann: Neue Probleme lösen. Es gehört zu den ethischen Verpflichtungen, der Welt neue Problemlösungen mitzuteilen, sodass andere darauf aufbauen können.

Cracker

Versuch einer Definition [1, 4, 5, 6, 7]

Der Begriff Cracker hat verschiedene, leicht abweichende Bedeutungen. Zum einen kann mit „Cracker“ eine Person gemeint sein, die der Tätigkeit des unethischen hackens nachgeht. Cracker spezialisieren sich auf das (wenn nötig gewaltsame) Eindringen in Fremdsysteme. Cracker sind aber nicht minder begabte Programmierer. In einem ähnlichen Tätigkeitsfeld verwirklichen sich die Warez-d00dz, die eine eigene Subkultur der Crackerszene bilden. Sie konzentrieren sich auf das cracken von proprietärer Software um diese Kopierschutzbereinigt an die Szene zu verteilen. Eine dritte Art der Cracker konzentriert sich hauptsächlich auf das Schreiben von Schadsoftware darunter Viren, Würmer, Trojaner, etc. Sie cracken Fremdsysteme nicht mehr von Hand, sondern lassen ihre selbst geschriebene Software die Arbeit automatisiert erledigen. Zu guter letzt sollen die Skript-Kiddies erwähnt werden. Diese werden jedoch in der Regel nicht als „echte“ Cracker angesehen, da sich ihr programmiertechnisches Können meist auf das Ausführen von Cracksoftware beschränkt.

Kurze Geschichte der Cracker [8]

Die ersten Cracker werden in den 70er-Jahren aktiv, jedoch ist ihre Spielwiese zu der Zeit noch das Telefonnetz. Diese Cracker nennen sich Phreaker. Sie nutzen ihr Wissen um kostenlose Telefonate zu führen.
In den 80er Jahren machen viele Phreaker den Sprung vom Telefon zum Computer. 1985 wird erstmals der Begriff „Cracker“ von Hackern benutzt, die sich gegen die Anschuldigungen eines Journalisten zu wehren versuchen. Cracker beschreiben sich gerne selbst als Hacker, was diese jedoch nicht billigen und deshalb diese eigene Bezeichnung für „unetische Hacker“ einführten. In den USA wird 1986 der „Computer Fraud and Abuse Act“ verabschiedet, der das unerlaubte Eindringen in Fremdsysteme verbietet. Zuvor gab es aufgrund der vergleichsweise rasanten Bildung der Szene keine griffigen Gesetze gegen Cracker.
In den 90er-Jahren erfährt die Crackerszene einen Schub durch das neu aufkommende Internet. Mitgliederzahlen wachsen exponentiell und die Szene wird durch die weltweite Vernetzung von Rechnern noch gefährlicher als zuvor. Gegen Ende des Jahrzehnts wird Windows 98 veröffentlicht. In der Folge werden dermassen viele Sicherheitslücken entdeckt, dass sich ein Markt für Sicherheitssoftware zu formen beginnt.

Verbrecherethik [9]

Es stellt sich die Frage, ob eine Ethik auch unter Verbrechern existieren kann, und wenn ja, welche Formen diese annehmen kann. Zum Vergleich sollen hier die zehn goldenen Regeln der „Cosa Nostra“ angeführt werden.

1. Keiner darf sich alleine einem unserer Freunde vorstellen, es muss immer ein Dritter dabei sein.
2. Schaue niemals Deiner Freunde Frauen an.
3. Lass dich niemals mit Polizisten ein.
4. Gehe nicht in Tavernen und Clubs.
5. Du musst der Cosa Nostra allzeit zur Verfügung stehen - wenn nötig sogar wenn Deine Frau ein Kind zur Welt bringt.
6. Vereinbarungen müssen kategorisch eingehalten werden.
7. Man muss den Ehefrauen Respekt entgegenbringen.
8. Wenn man etwas gefragt wird, dann muss man die Wahrheit sagen.
9. Man darf sich nicht des Geldes anderer [Clanmitglieder] und anderer Clans bemächtigen.
10. Die Cosa Nostra lässt niemanden in ihre Reihen treten, der nahe Verwandte in den verschiedenen Ordnungskräften hat, in dessen Familie Verrat vorgekommen ist, oder der sich schlecht benimmt und sich nicht an moralische Werte hält.

Dies soll verdeutlichen, dass sich erstaunlich viele ihrer Regeln auch auf Personen ausserhalb ihrer Organisation übertragen lassen. Grundsätzlich kann also nicht festgehalten werden, dass Verbrecher ausnahmslos unethisch handeln. Sie bedienen sich einer an ihre „Bedürfnisse“ angepasste Ethik.

Cracker-Ethik [10]

Cracker verstossen gegen einige zentrale Maxime der Hacker-Ethik, namentlich gegen die Regeln, keinen Schaden zu verursachen, Privatsphäre zu schützen, Information und Software zu teilen, und für die Verbesserung der Sicherheit zu hacken.
Gleichwohl teilen sie sich jedoch viele ethische Grundregeln mit den Hackern, vorallem mit denen der 60er Jahre. Insbesondere sind dies die Regeln der freien Information (in weniger strenger Form) und der Bewertung einer Person nur nach ihrem Können. Die neue Hacker-Ethik der 90er Jahre versucht, sich von Crackern zu distanzieren und beinhaltet daher kaum Maxime, die auch für Cracker vertretbar sind.
Cracker ergänzen diese Maxime durch die eigenen Auffassungen, dass Information, egal welcher Art, frei sein und frei verteilt werden soll, auch wenn diese nur in geschützter Form vorliegt. Insbesondere dürfen Sicherheitsmechanismen wie ein Kopierschutz oder eine Firewall ausgehebelt werden.
Wiederum eine eigene Auslegung der Crackerethik haben die warez-d00dz. Sie ergänzen die gängigsten Regeln der Cracker um Maxime wie: Plagiarismus ist verpönt. Schmarotzer werden nicht geduldet. Die Anerkennung der Szene dient als starke Triebkraft. Auf den fairen Wettkampf unter den Release-Groups wird sehr grosser Wert gelegt.

Penetrationstester - „Berufshacker“

Einleitung und Begriffserklärungen

Unter einer **Penetration** versteht man in der Informationstechnik das unautorisierte Eindringen in ein System, meistens durch eine Fremdperson.[11]
Ein **Penetrationstest** ist die Prüfung der Sicherheit eines Systems durch Anwenden von Mitteln und Methoden, die eine Person (Hacker/Cracker) zur Durchführung einer Penetration verwenden könnte. Penetrationstests sind Unterformen von den heute im Software Engineering gängigen Audits (Soll-Ist-Vergleich).[16]
Im Gegensatz zu Vulnerability Scans, wo ein Tool automatisiert nach Sicherheitslücken sucht, wird ein Penetrationstest immer von einer Person, dem Penetrationstester, und nicht von einer Maschine durchgeführt. Damit soll das Szenario eines Angriffs originalgetreu simuliert werden.[11]

Der Beruf Penetrationstester [12,1 4]

Penetrationstests werden bereits seit etwa 15 Jahren durchgeführt, haben sich aber erst in den letzten 5 Jahren (auch mit der zunehmenden Bedeutung des Internets) richtig etabliert. Seither ist auch der Begriff Penetrationstester aufgekommen. Genau genommen handelt es sich hierbei zum heutigen Zeitpunkt um eine Tätigkeit, nicht um einen Beruf, da es keine entsprechende anerkannte Ausbildung gibt und auch der Berufsbegriff nicht geschützt ist.
Es ist aber durchaus denkbar, dass sich die Tätigkeit Penetrationstester in näherer Zukunft zu einem offiziell anerkannten Beruf (mit staatlicher Prüfung) entwickelt, wie das bei anderen Prüfberufen (z.B. Wirtschaftsprüfer, Lebensmittelkontrolleur) bereits der Fall ist.

Penetrationstests aus ethischer Sicht [13]

Die Tätigkeit eines Penetrationstesters befindet sich nicht nur rechtlich gesehen am Rande der Legalität, sondern ist auch aus ethischer Sicht äusserst kritisch zu betrachten. Im Vordergrund dabei ist das Dilemma, dass ein Penetrationstest einerseits eine vorsätzliche kriminelle Handlung ist, andererseits aber zur Verhinderung genau solcher krimineller Handlungen dient. Man kann diese Situation mit einem Arzt vergleichen, der einem Patienten (kontrolliert) Schmerz zufügen muss (und womöglich damit vorsätzliche Körperverletzung begeht), dies aber in der jeweiligen Situation zum Heilungsprozess beitragen kann [12]. Im Unterschied zu Ärzten, welche von der Gesellschaft ein hohes Vertrauen geniessen, bestehen gegenüber Penetrationstester aber verschiedene Vorurteile, welche die Tätigkeit in ein schlechtes Licht werfen. Oft wird ihnen ein enger Draht zu kriminellen Cracker-Kreisen nachgesagt.
Das zentrale Problem ist, dass Penetrationstester gezwungenermassen gegen ethische Werte verstossen müssen, um das gewünschte Resultat zu erhalten. Folgende These könnte formuliert werden: Je krimineller die Test-Handlung, desto authentischer ist das Szenario, desto aufschlussreicher und aussagekräftiger sind die Ergebnisse. Tangiert werden dabei vor allem die ethischen Werte Respekt vor dem Eigentum und Selbstbestimmung (Privatsphäre).

ethischer Lösungsansatz [12]

Penetrationstests steuern unumstritten zur Sicherheit von IT-Systemen bei. Um sie jedoch auch ethisch vertretbar zu machen, sollten gewisse Regeln in einer Berufsethik verankert werden, wie das in anderen Berufen (z.B. bei Ärzten) bereits der Fall ist:
Penetrationstests sind Massnahmen zur Qualitätssicherung, müssen aber selber ebenfalls qualitätsgesichert werden. Sie sollten immer von Unternehmen durchgeführt werden, welche selber keine eigenen Produkte im Bereich IT-Sicherheit anbieten. Penetrationstester brauchen zwar Wissen und Informationen von Hackern/Crackern, sollten aber verantwortungsbewusste und integere Personen sein und ihr Know-How nur im beruflichen Umfeld nutzen. Schäden und illegale Handlungen sollen wenn immer möglich vermieden werden.
Grundsätzlich sollten sich Penetrationstests an das ethischen Prinzip, dass immer der grösstmögliche Nutzen enstehen soll, halten [15]. Dann sind sie ein sinnvolles und effizientes Werkzeug zur Verhinderung von ungewollte Angriffe und damit zur Steigerung der Sicherheit.

Quellen

[1] Steven Mizrach, “Is there a Hacker Ethic for 90s Hackers?” (URL) Zugriff am 08.03.2010 unter http://www.fiu.edu/~mizrachs/hackethic.html

[2] Eric Steven Raymond, 2001, “How To Become A Hacker” (URL) Zugriff am 08.03.2010 unter http://www.pavietnam.net/

[3] Chuck Hammill, 1987, “From Crossbows to Cryptography: Thwarting the State via Technology” (URL) Zugriff am 08.03.2010 unter http://www.cypher.net/crossbows_to_cryptography.html

[4] Malkin G. (1996) RFC Request for Comments: 1983 (URL) Zugriff am 06.03.2010 unter http://www.rfc-editor.org/rfc/rfc1983.txt

[5] Wikipedia (2010) Computervirus (URL) Zugriff am 03.03.2010 unter http://de.wikipedia.org/wiki/Computervirus

[6] Urban Dictionary (2004) Zugriff am 03.03.2010 unter www.urbandictionary.com

[7] Scubapirate (-) Definitions (URL) Zugriff am 06.03.2010 unter http://www.scubapirate.com/hacker.htm

[8] PCWorld.com (2001) Timeline: A 40-year history of hacking (URL) Zugriff am 06.03.2010 unter http://archives.cnn.com/2001/TECH/internet/11/19/hack.history.idg/

[9] Dreyer C. (2007) Verbrecherethik (URL) Zugriff am 03.03.2010 unter http://www.freilich.ch/blog/?p=442

[10] Krömer J., Sen E. (2007) No Copy - Die Welt der digitalen Raubkopie [Elektronische Version]

[11] Wikipedia (2010) Hackerethik (URL) Zugriff am 05.03.2010 unter http://de.wikipedia.org/wiki/Hackerethik

[12] Schreiber S. (2009) Entwurf einer Berufsethik für Penetrationstester [Elektronische Version].

[13] Schreiber S. (2006) Kosten und Nutzen von Penetrationstests [Elektronische Version].

[14] BSI - Bundesamt für Sicherheit in der Informationstechnik. (2008) Durchführungskonzept für Penetrationstests. (Studie)

[15] Hilty L. (2010) Informatik und Ethik - Theoretische Einführung [PDF]. (Vorlesungsslides)

[16] Gora S. (2007) IT-Sicherheitsaudits (URL) Zugriff am 06.03.2010 unter http://securitymanager.de/magazin/artikel_1385_artikelserie_it-sicherheitsaudits_teil_i.html