

Netzwerkethik



Studienarbeit im Fach

Informationsethik der

Simon



Rosendorf

Prüfer: Hr. Prof. Dr. Capurro

Erlenbach, Januar 2004

Inhaltsverzeichnis

Inhaltsverzeichnis	2
1 Einleitung	3
2 Ziel der Studienarbeit	4
3 Darstellung des Problems	5
3.1 Beispiel	6
4 Netzwerkangriffe aus wissenschaftlicher Sicht	7
4.1 Passwörter	7
4.2 Gnu-Emacs-Editor	8
4.3 Der Einbruch	8
5 Netzwerkangriffe aus rechtlicher Sicht	10
5.1 Hilfe von der Justiz.....	10
5.1.1 Schadensnachweis	11
5.1.2 Einsicht in Ermittlungsakten	11
5.2 Strafvorschriften	12
5.3 Datenschutz	12
6 Netzwerkangriffe aus ethischer Sicht	14
6.1 Darstellung des Problems aus normativer Sicht	14
6.2 Darstellung des Problems aus utilitaristischer Sicht	14
6.3 Darstellung des Problems aus diskursethischer Sicht	14
6.4 Metaethische Aspekte.....	15
7 Fazit und Ausblick	16
Literaturverzeichnis	17

1 Einleitung

Schon zu den Pionierzeiten des Internets, als es gerade den Kinderschuhen des Arpanet entwachsen war, sahen sich Administratoren Angriffen fremder Rechner ausgesetzt.

Das authentische Fallbeispiel eines Unix-Systemadministrators ist der Einstieg, um die Thematik Netzwerke, Netzwerksicherheit und „Hacker“ aus wissenschaftlicher, rechtlicher und ethischer Seite zu betrachten. Dabei werden Angriffsmethoden in Unix-Rechner, Paragraphen des Bundesdatenschutzgesetzes sowie normative, utilitaristische, diskursethische und metaethische Sichtweisen näher beleuchtet.

2 Ziel der Studienarbeit

Ziel dieser Arbeit ist, ein ethisches Grundverständnis für das Zusammenspiel in Netzwerken zu wecken.

Der Grundgedanke von Netzwerken liegt in einer ausgeglichenen und harmonischen Informationskultur, die ein Abgleich und Austausch von Informationen ermöglicht.

Der neue Produktionsfaktor neben Boden, Arbeit und Kapital, die Ressource Information respektive Wissen gewinnt in der heutigen Gesellschaft immer mehr an Bedeutung und gipfelt im Paradigmenwechsel von der Industrie- zur Wissensgesellschaft. Daher ist es umso wichtiger, dass dieser Rohstoff nicht durch ungebührliches Verhalten in den Tiefen der Server versiegt, sondern jedem Anwender zur Verfügung steht, der die Leistung in Anspruch nehmen möchte.

Ein Netzwerk besteht nicht nur aus physikalischen Teilen wie Drähten und Platinen, sondern auch im Grundgedanken der beteiligten Akteure. Nur wenn sich alle an die informellen „Spielregeln“ halten, kann das World Wide Web die tragende Säule sein, die die Menschen zu neuen Errungenschaften trägt.

3 Darstellung des Problems

Ein einzelner, isolierter Rechner ohne Kommunikation mit der Welt ist immun gegen Angriffe. Aber ein Einsiedlercomputer hat nur begrenzten Wert; er kann nicht auf dem Laufenden bleiben über das, was um ihn herum passiert. Computer sind dann von größtem Nutzen, wenn sie mit Menschen, Mechanismen und anderen Maschinen interagieren. Über Netzwerke können Leute Daten, Programme und elektronische Post austauschen.

Was geschieht aber in einem Computernetzwerk? Was haben sich Rechner zu sagen? Die meisten PCs genügen den Bedürfnissen ihrer Besitzer und müssen nicht mit anderen Systemen interagieren. Für Textverarbeitung, Arbeitsblätter für Abrechnungen und Spiele braucht man wirklich keine anderen Computer. Aber wenn man per Modem, ISDN oder DSL an das Netz angekoppelt ist, berichtet es das Neueste vom Aktienmarkt, vom Weltgeschehen und von Gerüchteküchen. Die Verbindung zu einem anderen Computer bietet viele Möglichkeiten, sich in die neuesten Nachrichten einzuschalten. Unsere Netzwerke bilden Nachbarschaften, die alle ein gewisses Gemeinschaftsgefühl haben. Die Netzwerke der Hochschulen zum Beispiel übertragen jeden Menge Daten über wissenschaftliche Tätigkeiten, Forschungsprojekte sowie Klatsch und Tratsch jeglicher Art.

Diese elektronischen Gemeinschaften sind durch die Grenzen ihrer Kommunikationsprotokolle gebunden. Einfache Netzwerke wie bspw. öffentliche „Schwarze Bretter“ verwenden die simpelsten Kommunikationswege. Jeder, der einen PC und einen Anschluss an das Internet hat, kann sich ankoppeln. Fortgeschrittene Netzwerke erfordern gemietete Leitungen und spezielle Rechner, die Tausende von Computern miteinander verbinden. Diese physikalischen Unterschiede setzen Schranken zwischen den Netzwerken. Die Netzwerke selbst sind durch Zugangscomputer (Router) verbunden, die unformatierte Nachrichten zwischen verschiedenen Netzwerken austauschen.

Wie ein Einsteinsches Universum sind die meisten Netzwerke endlich, aber unbegrenzt. Es gibt nur eine bestimmte Zahl beteiligter Computer, dennoch erreicht man nie den Rand des Netzwerkes. Hinter einem Computer gibt es immer einen anderen. Am Ende schließt sich der Kreis und beginnt wieder von vorne.

Mitte der fünfziger Jahre begann die US-Bundesregierung das Interstate Highway System zu bauen. Mit Hilfe von Erinnerungen an Transportengpässe während des Zweiten Weltkrieges stellten die Militärs sicher, dass das Interstate-System für Panzer, Militärkonvois und Truppentransporte ausgelegt war. Heute betrachten nur noch wenige die Interstate-Highways als militärisches System, obwohl es genauso gut Panzer anstatt Lastwagen transportieren kann. Aus denselben Beweggründen begann das Verteidigungsministerium, ein Netzwerk aufzubauen, um Militärcomputer zusammenzukoppeln. 1969 entwickelten sich aus den Experimenten der Defensive Advanced Research Projects Agency (DARPA) das Arpanet und dann das

Internet: ein elektronischer Highway, der hunderttausende von Computern rund um die Welt verbindet.

In der Welt der Datenverarbeitung ist das Internet mindestens so erfolgreich wie das Interstate-System. Beide sind von ihrem Erfolg überrollt worden und leiten jeden Tag Verkehrsströme, die viel größer sind, als sich das ihre Konstrukteure jemals erträumt hätten. Jedes System provoziert regelmäßig Beschwerden über „Verkehrsstaus“, „schlechte Straßen“, zu viele „Baustellen“, kurzsichtige Planung, miserable Wartung sowie das teilweise falsche bis kriminelle Verhalten ihrer Benutzer....¹

3.1 Beispiel

Exemplarisch am wahren Beispiel des Astrophysikers Clifford Stoll soll die drohende Gefahr, die die Arbeitsweise von Netzwerken beeinträchtigen kann, erläutert werden. Als neu eingestellter Systemmanager am Lawrence Berkely Laboratory in Kalifornien stellte er im September 1986 einen Abrechnungsfehler von 75 Cent fest. Jemand hatte Computerbenutzungszeit in Anspruch genommen, aber nicht bezahlt. Als er dem vermeintlichen Buchungsfehler nachgeht, entdeckt er, dass ein Hacker in das System eingedrungen ist und von dort aus hochgeheime Computer des Militärs anzapft. Da alle Warnungen an die Behörden - vom FBI bis zum CIA - nicht fruchten, begibt er sich selbst auf die Jagd nach dem Eindringling im Netz.²

Anfangs störte sich Clifford Stoll nur an der Tatsache, dass da ein Fremder in seinem Netzwerk umher „spazierte“ und bei böswilligem Verhalten in der Lage wäre, wichtige Dateien zu löschen oder gar das System zum Absturz zu bringen.

Durch die Kommunikation mit Administratoren anderer befallener Netze realisierte er jedoch, dass es nicht nur ein physikalisches Problem war, sondern auch ein ideelles. Es bestand zwar die Möglichkeit, durch diverse Gegenmaßnahmen den Hacker aus dem System zu sperren, allerdings wäre dann der Informationsaustausch nur noch unter beschwerlichen Bedingungen möglich, da verschiedene Sicherheitsstufen die einfache Interaktion Mensch/Maschine erheblich behindert hätten.

Ergo wäre der Grundgedanke auf freiheitlichen Informationsaustausch über Grenzen hinweg gestört und der Angreifer hätte durch sein Eindringen einen viel größeren Schaden angerichtet, wie nur Bits und Bytes zu löschen.

Letztlich gelang es ihm dann doch, den Hacker ausfindig zu machen. Die Spur führte über den großen Teich nach Deutschland, genau genommen nach Hannover. Ein junger Mann versuchte mittels der betriebenen Wirtschaftsspionage seinen Drogenkonsum zu finanzieren. Durch geeignete Gegenmaßnahmen und Kniffe konnte dem methodischen Vorgehen des Kriminellen (s. Netzwerkangriffe aus wissenschaftlicher Sicht) Einhalt geboten werden. Er wurde mit seinen eigenen Waffen geschlagen und damit war gewährleistet, dass die Forscher weiterhin ungestört kommunizieren konnten.

¹ Stoll 2001, S. 65

² Stoll 2001, S. 1

4 Netzwerkangriffe aus wissenschaftlicher Sicht

Die Angriffe auf Computersysteme werden immer ausgeklügelter und subtiler. Von DoS-Attacken (Denial of Service), die ganze Server mittels Überlastung lahm legen, bis hin zu Brute-force-Attacken (Angriff mit brutaler Gewalt), die die Beseitigung von Zugangssperren mittels einfachem aber sehr zeitaufwendigen Probierens aller möglichen Kombinationen realisieren, gibt es eine riesige Bandbreite an Möglichkeiten. Die nachfolgenden Unterkapitel erläutern an Hand des bereits genannten Beispiels Einbrüche auf Basis des Unix-Betriebssystems.

4.1 Passwörter

Um einige Hundert Benutzer gleichzeitig bedienen zu können, teilt das Betriebssystem die Hardwareressourcen genauso auf, wie ein Wohnhaus in verschiedene Wohnungen aufgeteilt wird. Jede Wohnung funktioniert unabhängig von der anderen: während ein Bewohner fernsieht, telefoniert ein anderer und ein dritter spült Geschirr. Innerhalb eines Computers kann ein Benutzer ein mathematisches Problem lösen, ein anderer elektronische Post nach Stuttgart schicken und ein dritter wiederum eine Hausarbeit schreiben. Die Dienstprogramme des Computers werden von der Systemsoftware und dem Betriebssystem versorgt.

Der private Bereich im Wohnhaus wird durch Schlösser und Schlüssel geregelt. Ein Bewohner kann die Wohnung eines anderen nicht ohne Schlüssel betreten und die Bewohner stören einander nicht. Im Computer ist es das Betriebssystem, das den Privatbereich des Benutzers sichert. Man kommt nicht ohne das richtige Passwort in fremden Speicherplatz und das Programm eines Benutzers stört die anderen nicht (bei entsprechender Ressourcenverteilung).

Mit einem Universalschlüssel kann der Hausverwalter jedes Zimmer betreten. Mit einem privilegierten Konto kann der Systemverwalter alle Programme und Daten im Computer lesen oder modifizieren.

Der privilegierte Benutzer ist wirklich allmächtig: er ist der einzige, der die nötige Software ins System einpassen kann. Verschiedene Betriebssysteme haben verschiedene Namen für privilegierte Konten – root, Systemverwalter, etc. - .

Diese Konten müssen immer scharf vor Außenseitern behütet werden.

Ein Hacker mit Systemverwalterprivilegien hätte den Computer als Geisel. Mit dem Universalschlüssel zum System könnte er es herunterfahren wann immer er wollte und es so unzuverlässig machen, wie er wollte. Er könnte jede Information im Computer lesen, schreiben oder modifizieren. Keine Benutzerdatei wäre vor ihm geschützt. Auch die Systemdateien stünden zu seiner Verfügung – er könnte elektronische Post lesen,

bevor sie ausgeliefert wird. Er könnte selbst Protokollierungsdateien manipulieren, um seine eigenen Spuren zu verwischen.³

4.2 Gnu-Emacs-Editor

Ein Hacker könnte ein kurzes Programm schreiben, um sich Privilegien zu verschaffen. Normalerweise würde Unix ein solches Programm nicht zulassen, da es niemals Privilegien über das hinaus erteilt, was einem Benutzer zusteht. Lässt jemand das Programm aber von einem privilegierten Konto aus laufen, wird er privilegiert. Sein Problem besteht darin, sein spezielles Programm – das Kuckucksei – zu maskieren, damit es vom System angenommen wird.

Alle fünf Minuten führt das Unix-System sein eigenes Programm, Atrun genannt, durch. Atrun ordnet routinemäßig andere Jobs und führt Aufräumarbeiten durch. Es läuft in einem privilegierten Modus mit der vollen Kraft und Macht des Betriebssystems. Gelingt es jemandem, ein fingiertes Atrun-Programm einzusetzen, würde es innerhalb von fünf Minuten ausgeführt mit voller Systempriorität. Aus diesem Grund sitzt Atrun in geschütztem Speicherplatz, der nur dem Systemverwalter zugänglich ist. Außer ihm hat niemand die Berechtigung, an Atrun herumzuhantieren.

Es ist unmöglich, einen Befehl abzusetzen, um sein Programm in den Systemspeicher zu kopieren.

Aber es gibt hier einen Joker. Das Editierprogramm Gnu-Emacs ist mehr als bloß ein Texteditor. Es kann leicht an persönliche Präferenzen angepasst werden. Es ist eine Grundlage, auf der man andere Programme aufbauen kann. Es hat sogar eine eingebaute elektronische Post.

Ist nun der Gnu-Emacs-Editor im System installiert, kann man damit eine Postdatei vom eigenen Verzeichnis überall hinschicken. Der Editor prüft nicht nach, wer es erhalten sollte oder ob der Empfänger die Datei überhaupt wollte. Er benennt die Datei nur neu und ändert ihre Eigentümererkennung. Man kann somit die Eigentümerschaft der Datei einfach von einem auf den nächsten übertragen, auch in den geschützten Systemspeicher. Folglich kann man jede Datei in den Systemspeicher schicken.

Ein Hacker kann eine spezielle Atrun-Datei gegen die legitime Version des Systems austauschen. Fünf Minuten später brütet das System sein „Kuckucksei“ aus, und er hat die Schlüssel zum Computer in der Hand. Danach schiebt der Hacker das Originalprogramm wieder dahin zurück, wo es hingehört. Die ganze Operation basiert darauf, dass eine Datei verschoben werden kann, wohin man will.

4.3 Der Einbruch

Durch methodisches Passwörterraten kann demnach über ein beliebiges Konto eingedrungen werden. Zuerst wird versucht, sich mittels „guest“ in das Gast-Konto

³ Stoll 2001, S. 20

einzu-loggen. Dann in das Besucherkonto mit „visitor“. Schließlich in die Konten >root<, >system<, >manager<, >service< und >systemooerator<.

Mit Hilfe des Gnu-Emacs-Fehlers kann nun ein Super-User angelegt werden.

Als Super-User (privilegierter Benutzer) des Unix-Rechners versteckt der Hacker sich hinter einem zugelassenem Konto. Dann klopft er einfach an der Tür einer anderen vernetzten Maschine und wird zugelassen, ohne dass ein Passwort benötigt wird und gelangt so nach und nach in immer mehr Computer.⁴

⁴ Stoll 2001, S. 65

5 Netzwerkangriffe aus rechtlicher Sicht

Angriffe aus dem Netz sind heute eher die Regel als die Ausnahme.

Die Rechtslage hat in Sachen Gegenmaßnahmen scheinbar nicht mit dem Fortschritt der Technik mitgehalten. Manchmal möchte man aber doch gegen Angreifer vorgehen, gerade wenn erheblicher Schaden eingetreten ist.

Die erste Reaktion nach einem erkannten Angriff auf das eigene System ist, es so vollständig wie möglich zu prüfen und gegebenenfalls die Sicherheitsmaßnahmen zu perfektionieren. Meist hat es damit aber auch sein Bewenden.

Es mehren sich jedoch die Fälle, bei denen ein nicht zu behebender Schaden durch Datenverlust oder durch personellen und zeitlichen Mehraufwand entsteht. Die Gründe sind in der steigenden Komplexität der Systeme zu suchen, aber auch in Qualität und Quantität der Angriffe.

Um diesen Schaden gegenüber dem Verantwortlichen, also dem Angreifer, geltend zu machen, steht nur der Rechtsweg offen, der aber selten beschritten wird. Das Verhältnis zwischen Juristen und EDV-Spezialisten ist bekannt: ein Seite überblickt nicht, was die andere Seite für Möglichkeiten, aber auch Schwierigkeiten hat. Die Justiz weiß nicht genug über Netzwerkprotokolle, die Möglichkeiten einer Identifizierung und die elektronischen Grundlagen. Die Administratoren wiederum sehen die Anforderungen an die Bestimmbarkeit gerichtserheblicher Tatsachen nicht. Als Folge gesteht man sich gegenseitig wenig Problemlösungskompetenzen zu. Schon deswegen, aber auch um die eigene Reputation nicht zu gefährden, sucht das Opfer eines Angriffs selten die Öffentlichkeit eines Gerichtsverfahrens. Aus demselben Grund blieben bislang viele Prozesse erfolglos.

Mit ein wenig Vorarbeit und optimierter Vorgehensweise passen die Anforderungen beider Seiten aber unter „einen Hut“ und die Erfolgsaussichten für Schadensersatzansprüche steigen. So sehr EDV-Anwender auch manchmal unter der Gesetzgebung leiden, lässt sie „Vater Staat“ dennoch nicht im Stich: diverse Spezialvorschriften stellen unter anderem das Hacken von Systemen unter Strafe oder regelt die Ersatzpflicht für herbeigeführte Schäden.

5.1 Hilfe von der Justiz

Um Ansprüche wirksam anzubringen, muss der richtige Anspruchsgegner bekannt sein. Das muss nicht zwingend eine bestimmte Person sein. Im zivilrechtlichen Bereich genügt es meist, den Angriffs-Ursprung eindeutig der Sphäre eines bestimmten Betriebs zuzuordnen. Die dazu erforderliche Ausforschungsarbeit ist in Eigenleistung - wenn überhaupt - nur schwer oder kostenintensiv machbar. Denn die Aufgabe ist es, eine im juristischen Sinn gesicherte Verbindung zwischen der Angreiferadresse und

der persönlichen Identität des Angreifers beziehungsweise der Angreifersphäre herzustellen.

Am besten bedient man sich dazu der Hilfe der Staatsanwaltschaft. Der stehen deutlich bessere Ermittlungsinstrumente zur Verfügung als jedem Normalbürger, etwa die Durchsuchung oder Beschlagnahme. Die Staatsanwaltschaft kann aufdecken, was sonst keiner vermag und wird auf einen Strafantrag des Verletzten hin tätig. Im Wesentlichen geht es darum, sich die Vorbereitungen für ein Strafverfahren auch in einem Zivilverfahren für eigene Interessen zu Nutze zu machen.

Das ist keineswegs ein Ausnutzen staatlicher Organe, sondern Aufgabe der Strafverfolgungsbehörde. Durch den Angriff auf ein fremdes System (aber nicht durch bloßes Anklopfen) verstößt der „Bösewicht“ in der Regel gegen **Paragraph 303a StGB**. Der Paragraph **303c StGB** wiederum berechtigt das Opfer, einen Strafantrag zu stellen und damit ein Verfahren gegen den Angreifer in Gang zu bringen. Im Einzelfall mag eine andere Vorschrift zusätzlich oder alternativ verletzt sein, was aber meist ohne Belang ist, wenn ein Schaden nachweisbar entstanden ist.

5.1.1 Schadensnachweis

Dieser Schaden muss detailliert aufgeschlüsselt werden. Es bietet sich daher an, genaue Aufzeichnungen zu führen, wer wann wie an der Schadensbehebung gearbeitet hat und welche Kosten im Einzelnen entstanden sind. Die Ermittlungsmotivation der Staatsanwaltschaft steigt mit dem nachgewiesenen Schaden - und für einen Zivilrechtsstreit ist er Voraussetzung.

Den Boden für eine zumindest grobe Vorgabe der Richtung, in die ermittelt werden soll, bereitet eine detaillierte Analyse der vorhandenen Logfile-Dateien. Die Verbindungsdaten, die mit dem Angriff in Zusammenhang gebracht werden können, sind isoliert und kommentiert herauszuarbeiten. Das bereitet Mühe, ist aber wichtig. Kann man beispielsweise den Beamten aufschlüsseln, aus welchen Netzbereichen die Angriffe ihren Ursprung nahmen und wie das aus den Protokollen herzuleiten ist, wissen die Ermittler schon, wo sie ihre Spurensuche beginnen können.

5.1.2 Einsicht in Ermittlungsakten

Hat die Staatsanwaltschaft den Vorgang erfolgreich aufgeklärt, liegt in jedem Fall eine Akte vor, und zwar unabhängig davon, ob ein Strafverfahren fortgeführt oder eingestellt wird. Die Einsicht in diese Ermittlungsakten gibt im Idealfall Auskunft über die Daten des Angreifers, seine Identität, das Unternehmen, für das er tätig ist, den missbrauchten Rechner, kurz alle wichtigen Informationen, um Schadensersatzansprüche gegen ihn oder sein Unternehmen auch im Zivilprozess durchzusetzen. Gewährt wird diese Akteneinsicht nur einem beauftragten Rechtsanwalt, aber nicht dem Geschädigten selbst.

Liegen die Ermittlungsergebnisse vor, sind die Erfolgsaussichten einer Zivilklage abzuschätzen und mit dem Kostenrisiko eines Zivilverfahrens abzuwägen. Schließlich

ist es in einem Zivilverfahren Sache des Klägers, alle anspruchsbegründenden Tatsachen unter Beweis zu stellen. Die dokumentierte Ansicht der Staatsanwaltschaft hat diesbezüglich in einem Prozess einen hohen Stellenwert.

5.2 Strafvorschriften

§ 303a StGB

(1) Wer rechtswidrig Daten (§ 202a Absatz 2) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) Der Versuch ist strafbar.

§ 303b StGB

(1) Wer eine Datenverarbeitung, die für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist, dadurch stört, dass er

1. eine Tat nach § 303a Absatz 1 begeht oder
2. eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) Der Versuch ist strafbar.

§ 303c StGB

In den Fällen des § 303 bis 303b wird die Tat nur auf Antrag verfolgt, es sei denn, dass die Strafverfolgungsbehörde wegen des besonderen öffentlichen Interesses an der Strafverfolgung ein Einschreiten von Amts wegen für geboten hält.

5.3 Datenschutz

Den eigenen Bedürfnissen, möglichst detaillierte Informationen über die Angriffe zu sammeln, stehen die Bestimmungen des Datenschutzrechts gegenüber. Diese beschränken die Speicherung und Weitergabe von Informationen auf das erforderliche Maß. Vielfach entsteht hier die Befürchtung, Datenspeicherungen seien zunächst unzulässig oder nur vorübergehend geduldet. Regelungsgegenstand des Bundesdatenschutzgesetzes (BDSG) sind aber nur personenbezogene Daten.

Nach **§ 3 Absatz 1 BDSG** sind dies "Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmaren natürlichen Person (Betroffener)". Das bedeutet eine notwendige Zuordnung der Daten zu einer bestimmten Person. Bei Verbindungsdaten zwischen Maschinen ist das keinesfalls möglich, wenn keine eindeutige Zuordnung zwischen der Maschine und dem Benutzer möglich ist. Für Bereiche außerhalb des eigenen Unternehmens ist das normalerweise nicht der Fall.

Schon aus diesem Grund bestehen gegen eine detaillierte Aufzeichnung der Verbindungsdaten keine Bedenken.⁵

⁵ Linux-Magazin (Datum des Zugriffs: 12.01.04)

6 Netzwerkangriffe aus ethischer Sicht

Das Adjektiv ethisch bedeutet in der traditionellen Ethik und in der Umgangssprache moralisch oder sittlich. Gemeint sind bspw. die ethischen Handlungen, Ansprüche und Normen.

Die Worte "Ethik" und "ethisch" bleiben hauptsächlich der philosophischen Wissenschaft vorbehalten. Die philosophische Wissenschaft behandelt das moralische und sittliche Handeln des Menschen.

6.1 Darstellung des Problems aus normativer Sicht

Moralische Normen entstehen hier automatisch durch die informationskulturelle Zusammenarbeit in Netzwerken.

Ohne eine ethische Grundlage wäre eine offene, auf Wechselbeziehungen ausgelegte Interaktion nicht möglich, da der Mensch ein gewisses Konstrukt braucht, in das er sich einordnen kann und das es ihm ermöglicht, nach imaginären Regeln zu handeln.

6.2 Darstellung des Problems aus utilitaristischer Sicht

Die Betrachtungsweise unter utilitaristischen Gesichtspunkten ist ein zweiseitiges Schwert.

Auf der einen Seite steht die betroffene Person oder Personengruppe mit einem Schaden an möglicherweise gelesenen sensitiven Daten oder gelöschten Bits und Bytes. Auf der anderen Seite kann das Ziel eines Einbruchs in ein fremdes System jedoch das Auffinden von Sicherheitslöchern sein, ohne selbige für eigene Zwecke zu missbrauchen. Statt dessen wird der betreffende Systemadministrator benachrichtigt und über die Details des Einbruchs informiert, damit das Leck entsprechend gestopft werden kann. Hintergrund hierfür ist die Politik einiger Firmen, aus fehlerhafter Software Kapital zu schlagen, in dem für versteckte Bugfixes Geld verlangt wird. Das Offenlegen von Sicherheitslöchern und deren Untersuchung stellt die Dinge unter einem anderen Gesichtspunkt dar und zwingt die "Täter" zum offenen Handeln.⁶

6.3 Darstellung des Problems aus diskursethischer Sicht

Ein Diskurs unter den beteiligten bzw. betroffenen Personen kann auf Grund der ursächlichen Tätigkeit eines Einbruches nicht stattfinden.

Die moralische Verwerflichkeit seitens der sich rechtswidrig verhaltenden Person steht außer Frage und regt bei entsprechenden Entscheidungen eine Erörterung zwischen

⁶ Christoph et al. 2000, S. 15

dem Geschädigten und dem Gesetzgeber an, um eine Verbesserung der jetzigen unausgereiften Rechtssituation zu erreichen.

6.4 Metaethische Aspekte

Befasst man sich mit dem Thema Netzwerkethik im Allgemeinen bzw. herunter gebrochen bis auf gezielte Rechnerangriffe, gerät man mit Schlagwörter wie

- „Verantwortung“
- „Gewissen“
- „gut“
- „schlecht“

in Verbindung.

„Gute“ Hacker definieren sich hierbei über ihre „Verantwortung“ gegenüber den Systemadministratoren und der Gesellschaft.

Dagegen sprechen die Geschädigten oftmals von „schlechten“ Menschen die ohne „Gewissen“ handeln.

7 Fazit und Ausblick

Das Thema Netzwerkethik ist eine Gratwanderung aus subjektivem Empfinden.

Dabei ist die persönliche Einstellung zu Themen wie Rechtsverständnis, Eigentum, Transparenz und Neugierde der ausschlaggebende Indikator.

Ohne Zweifel kann ein Netzwerk nur funktionieren, wenn alle Beteiligten sich an die formellen wie informellen Spielregeln halten. Das sensible Gebilde bricht in sich zusammen, sobald die offen geprägte Austauschkultur durch mutwillige Angriffe Dritter eingeschränkt oder zerstört wird.

Allerdings ist nicht jeder durchgeführte „Hack“ bei objektiver Betrachtung böse. So kann es paradoxerweise sein, dass sich ein Anwender im Netzwerk informiert, wie man in fremde Computer eindringen kann und diese neu erworbene Taktik im besagten Netz anwendet um Administratoren auf offene Sicherheitslücken aufmerksam zu machen.

Natürlich kann solch ein Angriff auch niedere Beweggründe haben, wie bspw. die Zerstörung von fremdem Eigentum oder Wirtschaftsspionage.

Letztlich führen aber auch diese Aktionen dazu, dass Netzwerke durch erhöhte Sicherheitsmaßnahmen resistenter werden. Die Problematik besteht nun darin, dass hierbei eine Spirale entstehen kann, die sich auf dem Rücken der Anwender unweigerlich nach oben schraubt. Denn jede Aktion erfordert eine Reaktion und erschwert somit die einfache und unkomplizierte Arbeit im Internet. Daher ist der Gesetzgeber gefordert, eine einvernehmliche Regelung zu finden, um den Produktionsfaktor Information zu schützen.

Literaturverzeichnis

Christoph, C. et al.: „Informationsfreiheit“ , Sommersemester 2000, Hausarbeit
Informationsethik, Hochschule der Medien Stuttgart

Stoll, C.: „Kuckucksei“, 5. Auflage, Frankfurt am Main 2001, Fischer Taschenbuch
Verlag

Linux-Magazin: „Rück-Schlag“,
<http://www.linuxmagazin.de/Artikel/ausgabe/2002/03/recht/recht.html>
(Datum des Zugriffs: 12.01.04)