Proseminar - Ethische Aspekte der Informationsverarbeitung

Internetkriminalität und Cracker

von Matthias Noack

Einleitung

- *"Wir kämpfen nicht mehr gegen den Gegner von gestern, junge Computerfreaks ohne Freundin, sondern gegen Kriminelle, die mit Phishing oder Spam Millionen scheffeln."* Trend-Mirco-Manager Udo Schneider
- *"Schon heute wird mit Internet-Crime mehr verdient als mit dem Drogenhandel."*, US-Kryptovordenker Phil Zimmerman
- Begriffsklärung **Internetkriminalität**: sind Straftaten die auf dem Internet basieren oder mit den Techniken des Internet geschehen. Dabei gibt es klassische Delikte die auf das neue Medium adaptiert wurden und neue Formen.
- Begriffsklärung **Cracker**: Vielfältige Bedeutung, allgemein kann man in unserem Kontext sagen, dass es sich um destruktive Hacker handelt. Ihren Handlungen liegt eine negative bis kriminelle Absicht zu Grunde. Die Handlungen an sich können dabei durchaus die selben sein, wie sie von Hackern ausgeübt werden. Hacker unterwerfen sich und ihr Handeln aber einer Hacker-Ethik. Auch für Leute die Kopierschutzmechanismen umgehen indem sie (kompilierte) Programme verändern ist der Begriff gebräuchlich. Oft fälschlicherweise für Hacker verwendet, vor allem in den Medien.
- Begriffsklärung **Delinquenz**: lat. delinquere, sich vergehen; ist die Tendenz, vor allem rechtliche, aber auch soziale Grenzen zu überschreiten; die Neigung zu kriminellem Verhalten.

Fakten zum Internet

- 1969 ARPANET: ursprünglich militärisches Forschungsprojekt, das Ziel war **Zuverlässigkeit**.
- Nicht für wirtschaftliche Nutzung und Sicherheit konzipiert . Das Konzept ist eher hinderlich für sichere Kommunikation.
- In den 90ern Erfolg des WWW, Internet wurde zum **Massenmedium**.
- Ende der 90er: Hochgeschwindigkeitszugänge und Flatrates.
- Extrem schnelle Entwicklung und Verbreitung; Sicherheit hielt nicht Schritt bzw. setzte erst später ein.
- Heute 2/3 der Deutschen Online, weltweit ca. 1 Mrd. Nutzer.
- Extrem **hohe Kommunikationsdichte** im Vergleich zu klassischen Medien. Statt einer Einweg-Kommunikation zwischen wenigen Sendern und vielen Empfängern ist jeder Teilnehmer gleichzeitig Sender und Empfänger.
- Hinzu kommt Internationalität/Interaktivität.
- Internet an sich ist nur ein Medium, d.h. die Nutzung bestimmt den ethischen Wert, es gibt positive wie negative Möglichkeiten der Nutzung, aus kriminologischer Sicht ergibt sich vor allem eine neue Gelegenheitsstruktur
- Nach modernen Soziologen bestehen Gesellschaften in erster Linie aus Kommunikation, das Internet bildet daher die Grundlage einer "**Cyber-Society**", deren wirtschaftlicher Rohstoff geistiges Eigentum ist.

Ethisches Handeln

- Begriffsklärung **Ethik**: Ist die Disziplin, die sich mit moralischer Pflicht und Verpflichtung, und damit was gut und was schlecht ist, beschäftigt. Also: Was ist in einer gegeben Situation richtiges und was falsches Handeln - was sollten wir tun?
- Philosophen versuchen schon seit Jahrtausenden dies zu definieren, es gibt keine einheitliche Sicht da subjektiv und auch vom Kulturkreis abhängig.
- Ein möglicher Ansatz: Die Handlung selbst unabhängig von den jeweiligen Folgen betrachten. Der Zweck heiligt nicht die Mittel.
- Diese Philosophie geht davon aus, dass das Recht einer Handlung von der Handlung selbst und nicht von den Folgen bestimmt wird.
- Es wird die Frage gestellt ob eine Tat angemessen ist, und es auch wäre wenn jeder das selbe tun würde? Denn wenn das Ergebnis im großen Rahmen offensichtlich gefährlich bzw. nicht zufriedenstellend wäre, sollte auch die einzelne, individuelle Tat so eingeschätzt werden.
- Im Gegensatz dazu sind manche Philosophen auch der Meinung, dass der Zweck die Mittel heiligt, aber das lässt sich nicht mit einer Gesellschaft vereinbaren, auch wenn einzelne danach handeln.
- Ein ethisches System, das primär die Konsequenzen der Handlungen in Betracht zieht, lässt eine Bewertung der gegenwärtigen Handlungen nicht zu, das ist aber der Zeitpunkt zu dem man eine Einschätzung benötigt.

➔ **Man muss die Bewertung also auf die Handlung an sich und nicht auf die möglichen Konsequenzen beziehen.**

- Auch hilfreich: Parallelen mit klassischen Handlungen.

Hacker-Ethik

- *Der Zugang zu Computern und allem, was einem zeigen kann, wie diese Welt funktioniert, sollte unbegrenzt und vollständig sein.*
- *Alle Informationen müssen frei sein.*
- *Misstraue Autoritäten - fördere Dezentralisierung.*
- *Beurteile einen Hacker nach dem, was er tut und nicht nach de üblichen Kriterien wie Aussehen, Alter, Rasse, Geschlecht oder gesellschaftliche Stellung.*
- *Man kann mit einem Computer Kunst und Schönheit schaffen.*
- *Computer können dein Leben zum besseren verändern.*
- *Mülle nicht in den Daten anderer Leute.*
- *Öffentliche Daten nützen, private Daten schützen.*

- Nur bedingt einheitlich definiert, stammt ursprünglich auch aus Zeiten als sich viele Leute wenige Computer teilen mussten.
- In ständiger Diskussion und Entwicklung.
- Frage: Steht der Glaube über der Moral (z.B. Förderung von Informationsfreiheit und Transparenz gegen sorgsamen Umgang mit fremden Systemen) - religiöse Parallelen.

Kategorisierung I

- Bereiche von Internetkriminalität nach der "Cybercrime Convention" des Europarates vom 23.11.2001:
  - ◊ **A**: *Straftaten gegen die Vertraulichkeit, Unversehrtheit und Nutzbarkeit von Computerdaten und Computersystemen* (z.B. illegaler Zugang, Abfangen, Behinderung von Daten/Systemen, Viren, Hacken, Cracken, DoS-Attacken ...)
  - ◊ **B**: *Computerbezogene Straftaten* (z.B. Online-Betrug, Online-Fälschungen), also Computernetze als neues Medium für klassische Straftaten
  - ◊ **C**: *Inhaltsbezogene Straftaten* (z.B. Kinderpornographie, verfassungsfeindliche Inhalte wie Rassismus, Extremismus, ...) Internet als Medium bereits bekannter Delikte
  - ◊ **D**: *Straftaten bezüglich Urheberrechtsverletzungen* (z.B. Diebstahl geistigen Eigentums, Piraterie-Delikte) Bekannte Delikte im neuen Medium aber mit ganz neuer Qualität und Quantität

Kategorisierung II

- Computerkriminalität bezogen auf Deutschland:
  - ◇ Strafrecht:
    - □ *Computerbetrug* (§263a): Vermögensbeschädigung durch Missbrauch von Daten
    - □ *Datenveränderung* (§303a): jegliches Verändern, Löschen oder Unterdrücken fremder Daten
    - □ *Computersabotage* (§303b): Stören einer fremden Datenverarbeitungsanlage, die für eine Firma oder Behörde von wesentlicher Bedeutung ist; auch z.B. durch Verbreiten von Computerviren oder Computerwürmern
    - □ *Ausspähen von Daten* (§202a): Verschaffung von geschützten Informationen aus Computersystemen
  - ◇ Urheberrecht nennt weitere Rechtsverletzungen wie Pirateriedelikte, Dekompilierung oder das Umgehen von Kopierschutzmaßnahmen, zivilrechtlich über Schadensersatzansprüche durchsetzbar
  - ◇ Im Zuge des Telekommunikationsgesetzes (TKG) auch Spam (Verweis Spam-Vortrag)
- International keine einheitlichen Regelungen, daher kann man allenfalls die Schnittmenge der gesetzlichen Regelungen als Straftat oder Verbrechen bezeichnen. Alles andere beschreibt der Begriff **Delinquenz** besser.
- Das Spektrum der auftretenden Delikte reicht von gravierenden aber seltenen Delikten (Cyber-War, Cyber-Terror, ...) bis hin zu massenhaften Phänomenen (Piraterie, Viren, ...)

Motive:

- Allgemein niedrigere Hemmschwelle als in der klassischen Gesellschaft:
  - ◇ niedrige Kosten, geringer physischer Aufwand, vermeintliche Anonymität
  - ◇ bei ausreichendem Know-How praktisch keine Barrieren (außer moralischer Bedenken)
  - ◇ Anleitungen sind verfügbar, Gleichgesinnte treffen sich in Foren und Chats
  - ◇ => Gelegenheitsstrukturen sind vorhanden
- Ruhm und Ehre:
  - ◇ Anerkennung von Gleichgesinnten durch Demonstration von Expertise
  - ◇ Medienaufmerksamkeit durch spektakuläre Angriffe
- Andere persönliche Motive:
  - ◇ Rache, z.B. dem (ehemaligen) Arbeitgeber schaden
  - ◇ Überzeugung
  - ◇ Langeweile, Kanalisation von ungenutzter Energie
  - ◇ Geltungsdrang ("Scriptkiddies", als Halbstarke der Cyber-Society)
- Politische/Religiöse Motive:
  - ◇ Terrorismus, Extremismus
  - ◇ Gezielte Attacken auf gegnerische Internetpräsenzen
- Demonstration von Sicherheitslücken und dem technisch Machbaren (ohne Rücksicht auf Verluste)
- Geld:
  - ◇ Auftragsarbeiten, Daten erlangen und zu Geld machen, Kontrollierte Rechner nutzen
  - ◇ Handel mit Daten, Drogen, Waffen, Kinderpornographie

Delikte und Maßnahmen I

- Urheberrechtsverstöße / Piraterie:
  - ◊ spätestens seit P2P-Tauschbörsen und Flatrates ein Massenphänomen
  - ◊ Es gibt dabei konkurrierende Gruppierungen die veröffentlichen.
  - ◊ Es gibt dabei Cracker, Uploader, Webmaster und Insider.
  - ◊ Bei reinen Inhalten in großem Maße auch schlicht private Anbieter in P2P-Netzen.
  - ◊ Industrie fordert gesetzliche Maßnahmen und hartes Durchgreifen von Staat und Polizei
  - ◊ Behörden fordern Lösung durch technische Maßnahmen
  - ◊ Vergleichbar mit Ladendiebstählen von Datenträgern, damit nicht ethisch. Was wäre wenn es jeder Täte? - Schwere wirtschaftliche Schäden.
  - ➔ Maßnahmen:
    - □ Immer komplexere Kopierschutzverfahren
    - □ Industrie ermittelt eigenständig und erstattet Anzeige
    - □ Werbekampagnen ("Raubkopierer sind Verbrecher.")
    - □ Lobbyarbeit => Urheberrechtsnovelle

Delikte und Maßnahmen II

- Einbrüche in fremde Computersysteme:
  - ◊ Kriminelles Ziel kann sein: Datendiebstahl, Datenmanipulation, Sabotage
  - ◊ Technisch vielfältig zu realisieren
  - ◊ Nach der Hacker-Ethik mit folgenden Argumenten nicht unethisch:
    - □ Aufdecken von Sicherheitslücken
    - □ Nutzung brach liegender Ressourcen
    - □ Wahrung der Informationsfreiheit
    - □ Überwachen von Überwachern
    - □ Bildungszwecke
  - ◊ Nach dem ethischen Handeln vom Anfang immer unethisch
  - ➔ Maßnahmen:
    - □ Software auf dem aktuellen Stand halten und richtig konfigurieren, Möglichkeiten nutzen
    - □ Menschliche Fehler vermeiden, sonst nutzen die besten Systeme nicht viel
    - □ Auf dem aktuellen Stand bleiben (Newsletter etc.)

Delikte und Maßnahmen III

- Phishing:
  - ◇ Neue Form des Social Engeneering, erste Phishingmails 1996 in den USA
  - ◇ Es wird versucht an Daten zu kommen indem man Dienstleister des Anwenders nachahmt
  - ◇ Meist Spam-Mails mit Anfragen von Banken (Verifikation, Freischaltung, Sicherheitsprüfung)
  - ◇ E-Mail-Daten werden gehandelt und sog. Casher leiten das Geld über mehrere Konten weiter (Zunehmend von Laien durchgeführt)
  - ◇ Tricks der Phisher: Absenderadressen fälschen, ähnliche Domainnamen, täuschende Links, Personalisierung, Host-Datei manipulieren
  - ◇ Hinweise auf Phishing:
    - □ unverschlüsselte Verbindung, kein Zertifikat
    - □ fehlerhaftes Deutsch, ungewöhnliche Wortwahl, ausgeschriebene Umlaute
    - □ Frage nach vertraulichen Daten, Betonung der Dringlichkeit, Drohung von Konsequenzen bei Nichtbeachtung, unpersönliche Anrede
  - ➔ Maßnahmen:
    - □ Hinweise beachten
    - □ iTAN-Verfahren, HBCI für Homebanking verwenden
    - □ manche Spam-Filter, Virenprogramme erkennen Phishing-Mails
    - □ keinen unaufgeforderten E-Mails vertrauen
  - ◇ Ist man Opfer geworden: Bank und Polizei informieren, Passwort ändern, im Zweifelsfall Konto sperren, die betreffende Mail sichern

Delikte und Maßnahmen IV

- DoS-Attacken:
  - ◇ Überlastung von internetbasierten Dienstleistungen mittels massenhafter Anfragen
  - ◇ Ziel sind meist wirtschaftliche Schäden durch den Dienstausfall
  - ◇ Technisch realisiert durch tausende, mit Malware infizierter (Windows-) Rechner
  - ➔ Maßnahmen:
    - □ Wenn angreifende Rechner aus dem selben IP-Bereich diesen blocken
    - □ Service unter anderem Namen mit anderer IP bereitstellen
    - □ Abschalten und warten um wenigstens Ressourcen zu schonen
    - □ Mehr Server bereitstellen
  - ◇ Eher angedroht als durchgeführt um mittels Erpressung Geld zu machen
- Kreditkartenbetrug:
  - ◇ Suche-Biete-System in IRC-Channels (#cctradez, #cccards, #creditcard, #check-card)
  - ◇ Rollen hierbei sind:
    - □ Casher, die Daten zu Geld machen, erhalten ca. 70% des Gewinns
    - □ Von Cashern beauftragte Leute die Kreditkartendaten auf Whitecards überspielen und damit das Geldholen am Automaten ermöglichen
    - □ Lieferanten von Kreditkartendaten (ca. 100$ für Kreditkartendaten), die Daten stammen oft aus Computereinbrüchen, z.B. bei Onlinehändlern mit Kundendatenbanken
  - ➔ Auch hier Polizei und Kreditinstitut informieren.

Delikte und Maßnahmen V

- Warenbetrug:
  - ◇ Online-Bestellungen werden nicht bezahlt, folgende Methoden finden Verwendung:
    - □ Waren werden mit gestohlenen Kredikartendaten bestellt
    - □ Rückbuchung nach Erhalt der Ware
    - □ Unterlassen der Zahlung bei Rechnung als Zahlungsart
    - □ Konten mit unzureichender Deckung bei Lastschriften
  - ➔ Maßnahmen:
    - □ Betrugsfälle zur Anzeige bringen
    - □ Kreditinstitut informieren, dieses steht in den meisten Fällen für den Schaden gerade wenn der Betrugsversuch erfolgreich war
  - ◇ "Das Risiko für den Online-Händler und Kunden ist in Deutschland gleich Null.", Rüdiger Trautmann, Vorstandsvorsitzender des Internet-Zahlungsdienstleisters Pago
- Identitätsdiebstahl:
  - ◇ Mit Hilfe gestohlener Daten eine fremde Identität annehmen um mittels dieser kriminelle Handlungen zu begehen.
  - ◇ z.B. Ebay-Betrug über fremde Zugangsdaten (meist von inaktiven Nutzern)
  - ➔ Maßnahmen:
    - □ sorgsam mit Datenumgehen
    - □ nicht überall das selbe Passwort verwenden (z.B. in einem Forum unter Angabe der E-Mail-Adresse mit dem Passwort des E-Mail-Kontos anmelden)

Delikte und Maßnahmen VI

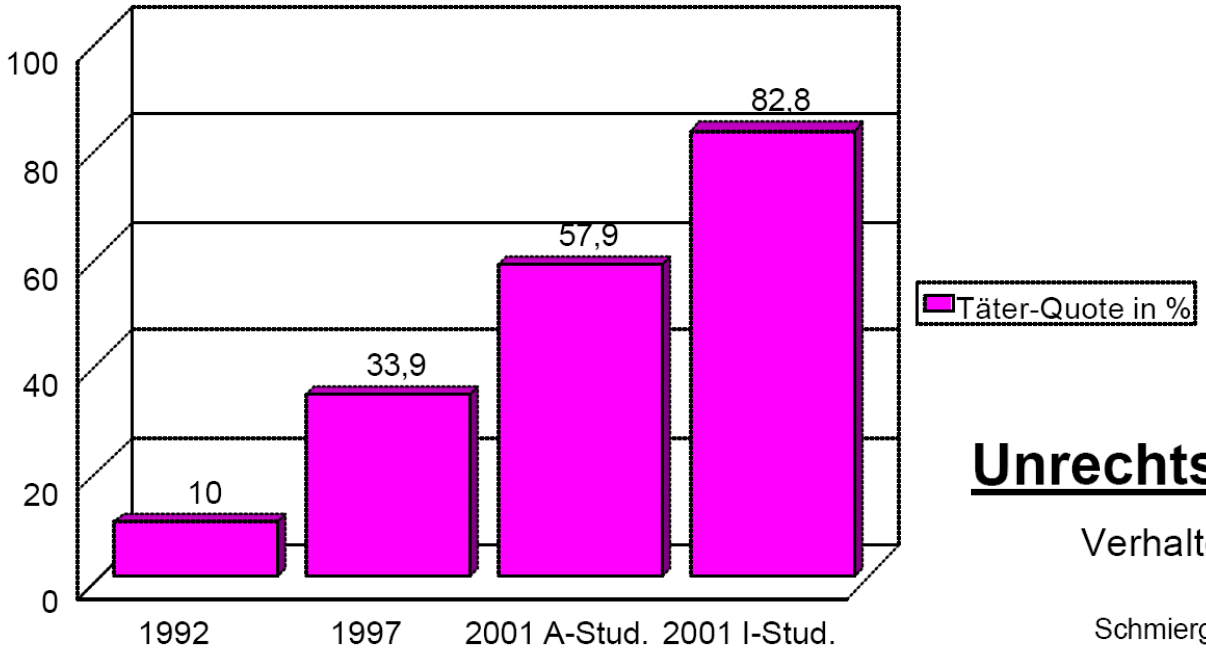
- Verbreitung illegaler Daten:
  - ◇ Einerseits Extremismus, Foren/Anleitungen für delinquentes Verhalten, z.B. Bombenbauanleitungen oder Selbstmord-/Kannibalismusforen
  - ◇ Vor allem aber Kinderpornographie:
  - ◇ früher: Handel unter der Ladentheke
  - ◇ heute: weltweit verfügbar über das Internet
  - ◇ auch neu: Kontaktaufnahme mit potentiellen Opfern über Chats
  - ◇ prinzipiell kann jeder im Netz auf solches Material stoßen würde er danach suchen, d.h. es bietet sich eine Gelegenheit für Leute die neugierig sind, aber in der klassischen Gesellschaft nie auf die Idee kämen sich solches Material zu besorgen
  - ◇ 2005: in NRW über 100 Razzien bei unvorbelasteten Bürgern, diese Leute können die Folgen nicht absehen: Verlust von Arbeitsplatz, Familie, Haus, Freunden, sozialen Kontakten usw. bei Bekanntwerden
  - ➔ Maßnahmen:
    - □ "Polizei agiert wie jemand der mit einem Fahrrad einem Rennwagen hinterher fährt."
    - □ Polizisten die das Netz nach solchem Material durchsuchen und anonymen Hinweisen nachgehen, "verdachtsunabhängige Recherche"
    - □ Internationale Zusammenarbeit, Europol, Interpol, BKA ist teils Mittler zwischen den einzelnen Behörden, z.B. gab schon Aktionen bei denen in 21 Ländern 200 Wohnungen zeitgleich durchsucht wurden
    - □ aber: Ermittlungen dauern bis zu 20 Monaten

Zahlen

- Softwarepiraterie: Schätzungen gehen von ca. 12 Mrd. $ Schaden aus (Zahlen der Business Software Alliance von 2001; geschätzt anhand verkaufter Hardware und nicht verkaufter, zugehöriger Software)
- Urheberrechtsverletzungen in Kriminalstatistiken (2001):
  Kaum erfasst, 0,9% Computerkriminalität (2001), 4/5 davon Scheck-Karten-Betrug, an zweiter Stelle Computerbetrug, gefolgt von Pirateriedelikten; hochgerechnet auf die Bevölkerung ergäbe das 3 Pirateriedelikte auf 100.000 Einwohner (also 3 Pirateriedelikte in Cottbus, 2001)
- Verlagerung: Ladendiebstählen (von Datenträgern) gehen kontinuierlich zurück
- Dunkelbefragungen: Softwarepiraterie unter Studenten 82,8% in Bonn, 2001 (hochgerechnet 7-stelliges Straftatenpotential); mangelndes Unrechtsbewusstsein, 2/3 der Befragten finden das Herunterladen geschützten Materials in Ordnung
- Phishing: Heute (2005-08-11) mehr als 250 000 Phishing-Attacken täglich
- Kinderpornographie 2004: 2000 Fälle vom BKA, weitere 15000 Fälle von Polizeibehörden bundesweit aufgedeckt, geschätzte Dunkelziffer: 85 bis 95%
- Aktuelle Kriminalstatistik, 2005 erstmals Straftaten im Internet gesondert erfasst (Baden-Würtemberg von Januar bis November 2005):
  - ◇ 12.244 Internetstraftaten, 85,3 % aufgeklärt, 4197 Tatverdächtige ermittelt
  - ◇ 61,1 % Waren und Kreditbetrug
  - ◇ 8,3 % Computersabotage und Ausspähen von Daten
  - ◇ 6,5 % Urheberrechtsdelikte (vermutlich sehr hohe Dunkelziffer)
  - ◇ 3,9 % Besitz und Verbreitung von Kinderpornographie
  - ◇ 2,2 % Phishing (1,3 Mio. € Schaden)

Software-Piraterie bei Studenten

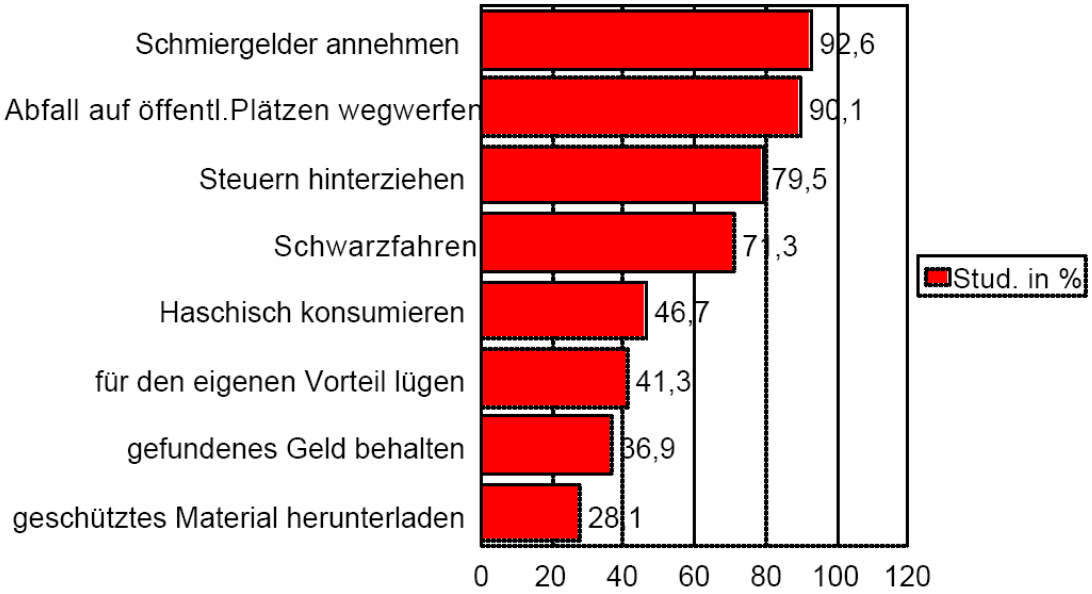
Selbstberichtete Delinquenz im Zeitvergleich



Quellen: Hollinger 1992; Skinner 1997; Rüther/Tübben 2001

Unrechtsbewußtsein von Studierenden

Verhalten, das man möglichst nicht tun darf (0 - 4)



Quelle: Krim.Sem. Uni Bonn, Stud. Wertestudie 2001 (n=122)

Fazit

- Rechtlich nur international zu lösende Probleme
- Viel zu oft werden Computer nur als simple Maschinen die Algorithmen ausführen gesehen. Es wird vergessen, dass ihr Gebrauch ernsthafte ethische Fragen aufwirft und auch nicht vorhersehbare Konsequenzen haben kann.
- Cyber-Ethics für Cyber-Society:
  - ◇ D.h. grundlegende Regeln und Normen bewusst machen und vermitteln, Strafrecht ist allenfalls Hilfestellung zur gesellschaftlichen Normbildung und Normstabilisierung
  - ◇ "**Medienkompetenz** muss im Grunde genauso erlernt werden wie das Sprechen, Lesen und Schreiben", Heribert Rech, Innenminister Baden-Würtemberg (Dez. 2005)
  - ◇ Dabei können ethische Standards aus der klassischen Gesellschaft übernommen werden. Ansatzpunkt sind Sozialisationsinstanzen: Elternhaus, Schule, Medien.
  - ◇ Problem: In die Technik hinein gewachsene Jugendliche mit noch wenig Moral gegenüber mangelnder Technik-Kompetenz bei Erziehungspersonen, denen damit auch die Moral-Vermittlungs-Kompetenz abhanden zu kommen droht.
  - ◇ Ziel: Schaffung von mehr Kompetenz im Umgang mit digitalen Medien bezüglich technischer und moralischer Aspekte. Verantwortungsvoll handelnde Cyber-Citizen.
  - ◇ Es gibt viele Initiativen und Aufklärungsangebote, z.B.:
    http://www.cybercitizenship.org/ (vom US-Justizministerium initiiert)
    http://www.sicherheit-im-internet.de/ (von mehreren Bundesämtern)
- Anwender sind zu blauäugig (ca. 1% der E-Mails verschlüsselt) und nicht bereit für mehr Sicherheit zu bezahlen (im Gegensatz zur klassischen Gesellschaft)

Ausblick

- Immer schnellere Zugänge: ADSL2+ mit bis zu 25 MBit/s Down, 1 MBit/s Upstream
- Immer mehr Einschränkungen bei digitalen Medien (DRM, TPM), der Anwender zahlt für die Entwicklung entmündigender Kopierschutztechniken
- Alternative: Kulturflatrates, neue Verwertungsmodelle und Angebote
- Vorratsdatenspeicherung, verstärktes juristisches Vorgehen, weitere gesetzliche Neuregelungen (wahrscheinlich härter im Bezug auf Internetkriminalität)
- VoIP ist auf dem besten Weg, in naher Zukunft das Telefonieren ins Internet zu bringen und auf längere Sicht das Telefonnetz abzulösen. Das bringt neue Möglichkeiten für kriminelle Handlungen, z.B. das gezielte Abhören von Telefongesprächen (von Firmenchefs etc.), Spyware die Gespräche mitschneidet, VoIP-Spam/-Phishing
- Klassische Firewall-Technologien behindern VoIP, 75% der Unternehmen die VoIP eingeführt haben, planen einen Ersatz ihrer Sicherheitstechnik. Die Sicherheitstechnik hinkt auch hier dem technischen Fortschritt hinterher.
- Unternehmen rüsten auf, vor einigen Jahren konnte ein Wurm ganze Unternehmen lahmlegen, heute gibt es schon Netzwerktechnologie und Software die Angriffsmuster erkennen und Maßnahmen einleiten kann. Diese Entwicklung wird weitergehen.
- Weitere neue Technologien die unvorhersehbare Potentiale haben kommen mit Sicherheit.

Quellen

- Werner Rüther: Internet-Delinquenz und Prävention. http://www.praeventionstag.de/content/7_praev/doku/ruether/Int-Delinquenz-Vortrag1.pdf (1. 4. 2006).
- Eugene H. Spafford: Are computer-hacker break-ins ethical? http://users.ece.gatech.edu/~owen/Academic/ECE4112/Fall2005/Spafford.pdf (1. 4. 2006).
- Holger Schmidt: Computerhacker wollen Geld statt Ruhm und Ehre. FAZ, 14. 9. 2005, S. 18.
- Ingrid Müller-Münch: Steckbrief: männlich, unauffällig. Frankfurter Rundschau, 30. 9. 2005, S. 8.
- Robert Meyer: Passwort-Phisher werden immer dreister. Neues Deutschland, 8. 11. 2005, S. 10.
- Provider-Untätigkeit gefährdet Firmen. Computer Zeitung, 5. 12. 2005, S. 1.
- http://de.wikipedia.org/wiki/Cybercrime (2006-06-10)
- http://de.wiktionary.org/wiki/Delinquenz (2006-06-10)
- http://de.wikipedia.org/wiki/Phishing (2006-06-10)
- http://www.polizei-bw.de/pressearchiv2005/prm139_05.pdf (2006-06-10)
- http://bundesrecht.juris.de/stgb/ (2006-06-10)
- http://www.ccc.de/hackerethics?language=de (2006-06-09)