Anhang A

Computerkriminalität – Fakten und Zahlen

Vorbemerkung

Der etablierte Fachbegriff »Computerkriminalität« umfasst die Kriminalität im gesamten Bereich der Informationstechnologie. Von IT-Kriminalität zu sprechen, ist noch nicht üblich.

Auch beim Deliktsbereich Informations-»Diebstahl« ist die Terminologie unscharf: Meist wird Information zwar unerlaubt kopiert, aber an der Quelle selbst nicht gelöscht. Nach klassischer Definition ist aber Diebstahl »Entwenden einer fremden, beweglichen Sache«. Treffender ist daher der Begriff »Ausspähen von Daten« .

A.1 Kriminalitätsstatistik des BKA

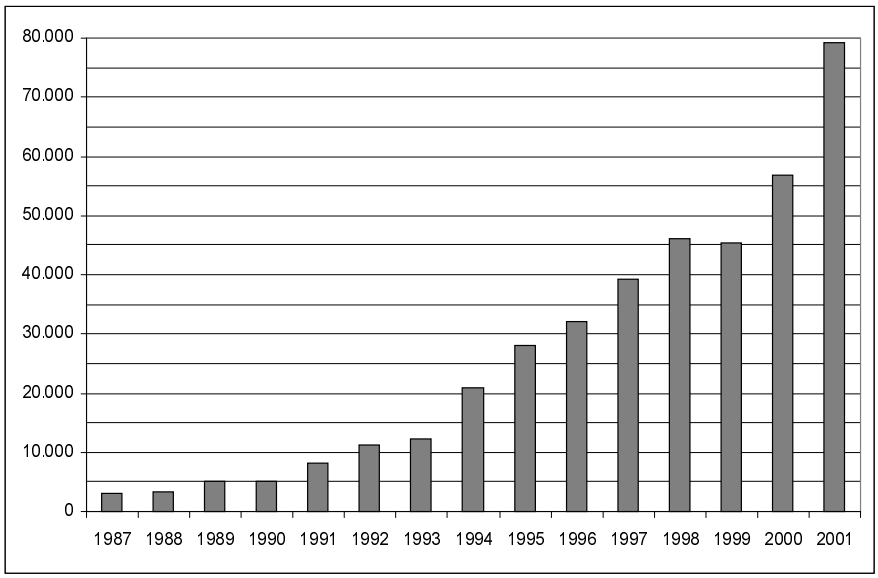

Abb. A.1: Erfasste Fälle von Computerkriminalität in Deutschland

Erfassung der Computerkriminalität in Deutschland

Seit 1987 werden in Deutschland Computerstraftaten in der Polizeilichen Kriminalitätsstatistik des Bundeskriminalamts (BKA) erfasst und vom Innenministerium im Mai des Folgejahrs als Bulletin und im Internet unter `www.bka.de` publiziert.

Die nachfolgende Auswertung der für den Teilbereich Computerkriminalität relevanten Daten aus dem Jahr 2001 basiert auf dem im Mai 2002 veröffentlichten Bericht.

Dunkelziffer

In der BKA-Statistik fehlen allerdings alle Fälle, die nicht angezeigt bzw. den Ermittlungsbehörden nicht bekannt wurden – wie bei jeder Form von Kriminalität. Über die Höhe dieser so genannten Dunkelziffer ist keine seriöse Schätzung möglich. Sie ist im Bereich Computerkriminalität sicherlich hoch, denn viele betroffene Organisationen und Unternehmen schweigen, um ihr Renommee nicht zu gefährden. Außerdem bleiben Manipulationen und »IT-Einbrüche« durch hoch qualifizierte Industrie- und Wirtschaftsspione oder durch Mitarbeiter (Innentäter) oft unbemerkt.

Bei einigen Deliktsbereichen – beispielsweise bei der Software-Piraterie, die nahezu ein »Massenphänomen« ist – lassen bereits die Zahl der erfassten Fälle und die angegebene Aufklärungsquote erkennen, dass zwischen Statistik und Realität erhebliche Differenzen bestehen können.

Auswertung der BKA-Kriminalitätsstatistik für das Jahr 2001

- 2001 wurden 79 286 Computerstraftaten bekannt, das sind 1,2 % der registrierten Gesamtkriminalität.
- Während die erfasste Gesamtkriminalität in Deutschland seit 1993 stagniert bzw. leicht rückläufig ist, stieg die Computerkriminalität bis 1998 im zweistelligen Prozentbereich und war damit der bei weitem am stärksten wachsende Kriminalitätsbereich überhaupt. Nach einem Rückgang um 1,5 % im Jahr 1999 setzte sich in den folgenden Jahren der Anstieg weiter fort. Im Jahr 2000 lag der Zuwachs im Mittel bei 25 %, 2001 bei knapp 40 %. Für die letzten zwei Jahre ergibt sich somit ein Anstieg der Computerkriminalität um insgesamt 75 %.
- Auffallend ist die heterogene Entwicklung der einzelnen Deliktsbereiche, die im Jahr 2001 von einem Rückgang um 56 % bei der »Software-Piraterie in Form gewerbsmäßigen Handelns« bis zu einem Anstieg um 266 % beim »Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten« reichte (siehe nachfolgende Tabelle).
- Die Aufklärungsquote lag 2001 bei 57 % und damit um knapp 4 % über dem Durchschnitt der Gesamtkriminalität.

Deliktsbereiche, Fallentwicklung und Aufklärungsquoten

Bereiche der Computerkriminalität	Fälle 2001	Änderung zu 2000	Aufklärungs-quote
Betrug mittels rechtswidrig erlangter Karten für Geldausgabe- bzw. Kassenautomaten	48 610	+ 10 %	42 %
Computerbetrug (§ 263 a StGB)	17 310	+162 %	78 %
Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten	8 039	+266 %	84 %
Computer-Software-Piraterie			
– zur privaten Anwendung	1 672	+ 23 %	99 %
– in Form gewerbsmäßigen Handelns	410	- 56 %	96 %
Fälschung beweiserheblicher Daten oder Täuschung im Rechtsverkehr bei Datenverarbeitung	920	+243 %	96 %
Ausspähen von Daten	1 463	+172 %	83 %
Datenveränderung oder Computersabotage	862	+ 68 %	45 %

- Über 60 % aller erfassten Computerstraftaten fielen 2001 in den Bereich **Kredit-, Bank- und Geldkartenbetrug**, das sind mehr als 48 000 Fälle. Betrug in diesem Bereich wird meistens angezeigt, so dass die Dunkelziffer als eher klein einzuschätzen ist. Die Aufklärungsquote betrug lediglich 42 %.
  Zu diesem Deliktsbereich schreibt das BKA:

  »Bei weiter fortschreitender Technisierung (elektronische Geldbörse) und Expansion des Einsatzes neuer Techniken durch Straftäter wird dieses Deliktsfeld in den nächsten Jahren weiter an Bedeutung gewinnen. Deshalb bedarf es weiterhin gemeinsamer Anstrengungen von Politik, Wirtschaft und Polizei sowie der Förderung der fachlichen Spezialisierung. Gefordert sind insbesondere Präventionsleistungen der Industrie durch technische Sicherung ihrer Produkte. [...] Durch zwingende Benutzung einer PIN könnten in diesem Bereich durchgreifende Verbesserungen erzielt werden.«

- Mehr als jede fünfte Computerstraftat fiel 2001 in den Bereich **Computerbetrug**. Beispiele dafür sind Manipulationen von Programmen oder Daten im Abrechnungswesen und Veränderungen der Programme von Geldspielautomaten zur Erhöhung der Gewinnchancen.
- **Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten** umfasste über 8 000 Fälle. Dazu gehört das Einloggen bei Internet-Providern mit fremden oder gefälschten Zugangsdaten, aber auch das unbefugte Entsperren von so genannten SIM-Locks bei Mobiltelefonen sowie »Zugangserschleichungen zu Telefonanschlüssen mit illegalem Anwählen von mit hohen Kosten verbundenen 0190er-Nummern« (BKA). Die Aufklärungsquote von 84 % deutet dar-

auf hin, dass solche Fälle überwiegend dann angezeigt wurden, wenn es Hinweise auf den Täter gab. Die Dunkelziffer ist als beträchtlich höher einzuschätzen.

- Bei der **Software-Piraterie** (Raubkopieren) fällt auf, dass wesentlich mehr Delikte im privaten Bereich als im Rahmen »gewerbsmäßigen Handelns« registriert wurden. Zusammen mit dem Rückgang der Fallzahlen in der zweiten Kategorie um 56 % und der sagenhaften Aufklärungsquote von im Mittel 98 % deutet dies stark darauf hin, dass fast ausschließlich aufgeklärte Fälle erfasst wurden. Die Gesamtzahl von 2 082 Fällen liegt mit Sicherheit weit unter den tatsächlichen Verhältnissen.
- Der Gesamtbereich **Fälschung/Täuschung/Ausspähung/Veränderung/Sabotage** umfasste insgesamt 3 245 Fälle und damit 'nur' 4 % aller Computerdelikte, allerdings ist je nach den Umständen von erheblichen Schadenshöhen pro Delikt auszugehen.

A.2 Schätzungen der Schadenshöhe

Das Bundeskriminalamt nennt keine Schadenshöhen durch Computerkriminalität.

Für den Teilbereich Wirtschaftsspionage gibt es Schätzungen von verschiedenen Institutionen: Der Verlust, den deutsche Unternehmen durch Wirtschaftsspionage erleiden, wird zwischen 4,25 und 20 Milliarden EUR pro Jahr taxiert.

Computer-Hacker kosteten europäische Firmen laut Omni Consulting Group im Jahr 2000 über 9 Milliarden DM Umsatz:

»Hackers cost firms billions of dollars

Computer hackers cost European businesses $ 4.3 bn in lost revenue last year, according to recent research. A study of 3,000 businesses worldwide found that lapses in security cost companies between 5.7 and 7 per cent of their annual revenue, or six cents for every dollar in sales.

Frank Bernhard, managing principal of Omni Consulting Group, which carried out the study, said online security problems are growing faster than anyone could imagine. »That whole issue could explode,« he said, adding that when hackers break into company source code, »you're into billions of dollars that just walked out the door.« Bernhard believes that companies need to consider their intellectual property assets and cited Microsoft's recent denial-of-service attacks, which crippled most of its major web properties, as an example.

»The answer is clear: [Microsoft] did not have a corporate policy body looking at security [and] now it does,« he said. Bernhard believes that although European companies are less stringent about introducing security policies and are more relaxed about intrusion threats, they are beginning to recognise the implications

> of hack attacks and the need for protection. »European organisations are more adapt and inclined to scale up towards network security,« he said. He stressed that companies need to put security measures in place and implement policies to protect their intellectual properties. He gave the example of someone walking into an office building and stealing a photocopier. »How can you miss someone walking out with the equipment and how can you miss someone walking away with your source code?«
>
> The study found that non-IT organisations and manufacturing companies were best at protecting their intellectual properties. »The ones that we'd think have the security tools are the weakest link in the puzzle,« he said.«
>
> (Quelle: `www.vnunet.com/News/1117559`)

Die 1998er Studie vom US Computer Security Institute und FBI taxiert den Schaden durch IT-Kriminalität in den USA auf 10 Milliarden US-Dollar jährlich. Schätzungen für den Bereich Industriespionage allgemein in den USA reichen von 63 bis 300 Milliarden Dollar pro Jahr.

Weil der Schaden für Unternehmen existenzbedrohend sein kann, bietet Lloyds seit 1999 erstmals eine Versicherung an, die bis zu einer Höhe von 50 Millionen Dollar vor Risiken des Informationsverlustes durch Cracker, Viren, Computersabotage oder Datenverlust schützt.

A.3 Fallbeispiele

Zum Abschluss sollen einige Fallbeispiele belegen, dass IT-Kriminalität eine reale Bedrohung ist. Kaum ein Tag vergeht, ohne dass die Presse und Online-Informationsdienste, zum Beispiel der Newsticker des Heise-Verlags (`www.heise.de/newsticker`), entsprechende Delikte melden.

Betrug, Erpressung

Der Bereich Kreditkartenbetrug wird von den Geldinstituten verschleiert, um die Kundenakzeptanz nicht zu beeinträchtigen. Der Verlust, den die Banken stillschweigend ertragen, mindert die enormen Rationalisierungsgewinne durch Informationstechnologie nicht wesentlich. Jedoch sind die geschädigten Kunden oft in Beweisnot.

Grundsätzlich sind alle Unternehmen im E-Commerce-Bereich durch IT-Kriminalität gefährdet, wie zwei exemplarische Fallbeispiele zeigen sollen:

- Im Dezember 1999 erpresste ein zunächst »unbekannter Russe« ein Unternehmen mit gestohlenen Kreditkarteninformationen – 300 000 Kreditkartennummern – und publizierte diese teilweise im Web, um seiner Forderung

Nachdruck zu verleihen. Schlagzeile der WELT vom 13.1.2000: »Der größte Datendiebstahl aller Zeiten«.

- Im Januar 2000 berichteten Zeitungen, dass britische Cracker in Systeme von mindestens zwölf internationalen Firmen – unter anderem des Kreditkartenunternehmens Visa – eindrangen, Quellcodes kopierten und Erpressungsgeld in Höhe von insgesamt 31 Millionen Mark forderten. Ein Scotland-Yard-Ermittler sprach von »der bisher schwersten systematischen Verletzung von Sicherheitssystemen«.

Site-Hacking

- Am 5.11.1999 meldeten die Tageszeitungen Site-Hacking beim rumänischen Finanzministerium. Auf dessen Internetseite wurden »Steuern auf Dummheit« angekündigt.
- Im Januar 2000 gelang es chinesischen Hackern, systematisch die Internetseiten verschiedener japanischer Behörden zu hacken und Protest gegen das Nanking-Massaker von 1937 anzubringen, was im »High-Tech-Land Japan« als große Blamage empfunden wurde (Quelle: FAZ vom 28.1.2000).
- Unbekannte veränderten vor einigen Jahren die Homepage des amerikanischen Justizministeriums in »U.S. Department of Injustice«. Schwedische Hacker änderten die CIA-Homepage in »Central Stupidity Agency« und legten »Hot«-Links zu Sex- und Musikangeboten. Eine weitere Blamage: Unbekannte änderten das CIA-Logo in »Central Idiots Agency« und dieses Fake stand volle vier Tage im Web.
- Zunehmend werden auch politische Auseinandersetzungen zum Anlass für Hackerangriffe genommen. So kam es zu einem mehrwöchigen »Schlagabtausch« zwischen chinesischen und US-amerikanischen Hackern, nachdem am 1.4.2001 ein chinesischer Pilot beim Zusammenstoß seines Kampfjets mit einem US-Aufklärungsflugzeug über dem Pazifik getötet worden war.
  Auch nach den Terroranschlägen in New York und Washington am 11.9.2001 traten Hacker in Aktion; in diesem Fall waren Webseiten islamischer Organisationen Ziel diverser Attacken.

Mehr Informationen über solche zweifelhaften »Erfolge« finden Sie im Archiv von »2600 – The Hacker Quarterly« unter `www.2600.com/hacked_pages` und unter `www.ccc.de` (Chaos Computer Club Hamburg e.V.) sowie unter `www.alldas.de`, wo gezeigt wird, was Cracker und »Scriptkiddies« angerichtet haben.

Täuschung durch Manipulation von Information

- Im Dezember 1999 meldeten die Tageszeitungen ein Beispiel dafür, dass die Veränderung von Informationen auf der Site eines großen US-Wirtschaftsdienstes die Börse beeinflusste: »Pairgain Technologies wird übernommen«, lautete dort eine illegal platzierte Meldung.

Informationsbeschaffung

- Eine Milliarde Dollar Streitwert hat das Gerichtsverfahren eines Erdöl-Konzerns gegen einen IT-Dieb, der die Ergebnisse von Testbohrungen in einem neuen Ölfeld crackte (Quelle: Verbrauchermagazin DM 1/2000).
- 1993 wurde der General Motors Manager Lopez mit einem Teil seiner »Warriors« genannten Managerriege von VW abgeworben. Neben 23 000 Blatt vertraulicher Unterlagen brachten sie auch Informationen auf Datenträgern bei VW ein. Die IT-Spezialisten der Staatsanwaltschaft Darmstadt fanden bei einer – zuvor verratenen – Hausdurchsuchung trotz frisch formatierter Festplatten im IT-System von VW Hinweise auf den Informationsraub. Nach außergerichtlicher Einigung leistete VW an GM einen sehr hohen Schadensersatz.
- Jahrelang wurde das Rechnersystem der EU von US-Geheimdienststellen online angezapft und vor wichtigen internationalen Wirtschaftskonferenzen wurden die jeweiligen nationalen Strategien ausspioniert.
- 1997 wurde die Entwicklungsdatenbank der BASF »geknackt und möglicherweise komplett ausgeräumt« (laut Verbrauchermagazin DM 1/2000).
- 1999 wurden im PDS-Parteibüro Laptops und Festplatten gestohlen. BILD-Schlagzeile am 30.7.1999: »Einbrecher stehlen Gysis Computerdaten«.
- Am 4.1.2000 meldete die Frankfurter Rundschau, das gesamte Nuklearwaffenprogramm der USA – ein virtueller Katalog, der 800 000 Seiten entspricht – sei von einem Innentäter auf Datenträger kopiert worden.
- Im Januar 2000 wurde bekannt, dass ein 16-Jähriger aus Kalifornien 27 Internet Service Provider gehackt hat und dabei über 200 000 Passwörter erbeutete.
- Ein ähnlicher Fall ereignete sich 2001 in Deutschland: Eine Gruppe von etwa 30 Personen hatte die Passwörter von mehreren tausend Internetnutzern ausspioniert und auf einschlägigen Webseiten veröffentlicht. Die Zugangsdaten wurden vermutlich in mehreren tausend Fällen von Dritten missbraucht, um auf fremde Kosten im Internet zu surfen oder falsche Online-Verträge mit Internet-Providern abzuschließen (Quelle: Spiegel Online, 3.11.2001).

Industrie- und Wirtschaftsspionage

Nach Ende des Kalten Kriegs betreiben die Geheimdienste Wirtschaftsspionage als neuen Schwerpunkt. Sie verfügen über das Know-how und die beste verfügbare personelle und technische Ausstattung für »elektronische Raubzüge« ohne Spuren.

Aufschlussreich ist der Bericht des Scientific and Technological Options Assessment (STOA) des Europäischen Parlaments: »An Appraisal of the Technologies to Political Control«; Download und aktuelle Ergänzungen siehe `www.europarl.eu.int/dg4/stoa/en` oder `http://cryptome.org/stoa-atpc.htm`.

Durch den weltweit verschärften Wettbewerb wird Industriespionage für Unternehmen Gewinn bringend. Beauftragte High-Tech-Spione stehlen gezielt Know-how und Strategiepläne der Konkurrenz. Forschungs- und Entwicklungskosten können so drastisch reduziert werden. Dabei existiert kein Unrechtsbewusstsein, Konkurrenten werden mit allen verfügbaren Mitteln ausgebootet:

- Siemens verlor den ICE-Auftrag in Korea, weil der französische Geheimdienst das endgültige Angebot ausspionierte. Siemens-Deutschland hatte unverschlüsselt an seine Niederlassung gefaxt, das Angebot wurde daraufhin vom TGV-Konsortium unterboten.
- Enercon konnte seine Windkraftanlagen nicht in die USA exportieren, weil die Technologie bereits durch gezielten Informationsdiebstahl von der Konkurrenz patentgeschützt war.
- Airbus verlor 1994 einen Großauftrag an Boeing, weil die staatlichen Lauscher des NSA über das Echelon-System – siehe `www.echelonwatch.org` – alle Faxe und Telefonate zum Verhandlungspartner in Saudi-Arabien abhörten.

Software-Piraterie

Der »Diebstahl« von Software (Raubkopieren, Software-Piraterie) ist inzwischen ein großer Bereich der Schattenwirtschaft:

- Im Januar 2000 meldeten die Zeitungen, dass eine Düsseldorfer Bande für geschätzte 1,5 Milliarden DM CD-Sets mit Raubkopien von begehrten Programmen in Auflagen von bis zu 20 000 Stück vertrieben hatte.

Virus-Schäden

- Selbst Viren ohne Schadensfunktionen können zu beträchtlichen finanziellen Schäden führen:
  Im November 1999 kam es laut Pressemeldungen beim PC-Hersteller DELL in Irland nach der Installation eines Updates der Anti-Viren-Software zur Meldung, dass Geräte mit dem Virus »FunLove«, einem harmlosen Windows-Virus, infiziert seien. Es wurden rund 12 000 Computer überprüft. Diese waren zum Teil schon ausgeliefert und mussten für diesen Zweck zurückgerufen werden. Der Gesamtschaden wird auf rund 22 Mio. US$ geschätzt.
- Seit dem Auftreten des »ILOVEYOU«-Virus am 4.5.2000, der mithilfe eines »Viren-Baukastens« konstruiert worden war, vergeht kaum eine Woche ohne einen neuen oder »mutierten« Skriptvirus. Besonders dreist gingen Virenprogrammierer in zwei Fällen im Herbst 2001 vor, indem sie ihre Machwerke als Sicherheits-Patch für Microsoft-Produkte (»Redesi«-Wurm) bzw. als »neuen kostenlosen Trojanerscanner« (»Ants«-Wurm) getarnt hatten. Viele Anwender ließen sich durch diese Spielart des Social Engineerings täuschen und trugen mit einem Doppelklick auf das vermeintliche Sicherheitsprodukt zur Weiterverbreitung der Schädlinge bei.

- Gleich mehrere Verbreitungswege nutzte im September 2001 der Wurm »Nimda« aus und infizierte dadurch eine große Zahl von Rechnern: Er verbreitete sich als E-Mail-Attachment, über Web-Server, in deren Webseiten er JavaScript-Code einschleuste, sowie innerhalb von lokalen Windows-Netzwerken über freigegebene Laufwerke und Ordner. Zu seinen Schadensfunktionen gehörte neben der Manipulation von System- und Programmdateien die Einrichtung eines Gast-Accounts mit Administrator-Rechten auf Windows-NT/2000-Systemen, der als Hintertür für andere Angreifer aus dem Internet dienen kann.
  Verbreitung und Schadenshöhe lassen sich nur schwer erfassen, US-amerikanische Medien schätzen jedoch, dass allein 2,2 Millionen Server infiziert wurden, wodurch ein Schaden von über 500 Millionen Dollar entstand.