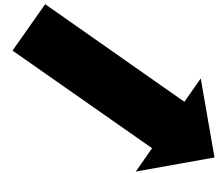











Computerkriminalität

Lagebild 2008

Kriminalitätsentwicklung im Überblick

Computerkriminalität



	2007	2008	in %	
Gesamt	15.467	13.604	- 12,0	
Computerbetrug	4.265	4.024	- 5,6	
Fälschung beweisbarer Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung	1.073	1.312	+ 22,3	
Datenveränderung/Computersabotage	977	628	- 35,7	
Ausspähen; Abfangen von Daten einschl. Vorbereitungshandlungen gem. §§ 202a, 202b, 202c StGB [*]	1.377	1.876	+ 36,2	
Betrug mittels rechtswidrig erlangter Debitkarte mit PIN	6.145	4.975	- 19,0	
Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten	525	585	+ 11,4	
Softwarepiraterie (private Anwendung)	905	166	- 81,7	
Softwarepiraterie (gewerbsmäßiges Handeln)	200	38	- 81,0	

^{*} Erstmögliche Erfassung in diesem Umfang erst ab 2008 (vorher lediglich „Ausspähen von Daten“).

Inhaltsverzeichnis

Seite

1	Lagedarstellung	3
1.1	Entwicklung der Fallzahlen.....	3
1.2	Fallzahlen in einzelnen Deliktsfeldern	3
1.3	Aufklärungsquoten.....	4
1.4	Schaden	4
1.5	Tatmittel Internet.....	4
1.6	Erkenntnisse aus dem Kriminalpolizeilichen Meldedienst luK (KPMD luK)	5
1.7	Zentrale Internetrecherchen	5
1.8	Erkenntnisse aus der EDV-Ermittlungsunterstützung	5
2	Getroffene Maßnahmen.....	6
2.1	Phishing	6
2.2	Präventionshinweise.....	7
3	Ausblick.....	8
4	Anlagen.....	9
4.1	Definitionen.....	9
4.2	Auftrag „Lagebild“	9
4.3	Datenbasis.....	9
4.4	Tabellen und Diagramme	11
4.5	Ansprechpartner / Ergänzende Hinweise	14

1 Lagedarstellung

1.1 Entwicklung der Fallzahlen

Von den insgesamt 1 453 203 in Nordrhein-Westfalen polizeilich bekannt gewordenen Straftaten im Jahr 2008 sind nach der Polizeilichen Kriminalstatistik 13 604 Fälle (0,9 %) der Computerkriminalität im engeren Sinne zuzuordnen. Dies entspricht einer Abnahme um 1 863 Fälle (12,0 %) gegenüber dem Vorjahr (2007: 15 467 Fälle).

Die Computertechnik gewinnt in der Gesellschaft eine immer größere Bedeutung. Die Verbreitung der Technologie hat mittlerweile alle Bevölkerungsgruppen erreicht. Dies schlug sich bis zum Jahr 2001 in kontinuierlich steigenden Fallzahlen der Computerkriminalität nieder. Die Fallzahlen sanken im Jahr 2002 wieder und blieben im Jahr 2003 annähernd konstant. Im Jahr 2004 war ein starker Anstieg festzustellen, während die Fallzahlen im Jahr 2005 und 2006 abnahmen und im Jahr 2007 wieder leicht anstiegen. Im Jahr 2008 haben die Fallzahlen wiederum stark abgenommen.

Der überproportionale Anstieg der Fallzahlen im Jahre 2001 erklärt sich durch mehrere umfangreiche Verfahren im Deliktsbereich Computerbetrug, die mit zusammen ca. 3 300 Fällen Eingang in die PKS fanden.

In den Deliktsfeldern Computersabotage / Datenveränderung ist von einem großen Dunkelfeld auszugehen. Geschädigte Firmen zeigen aus Angst um ihr Ansehen in der Öffentlichkeit erfolgte Straftaten nur sehr selten an. Straftaten werden oftmals nicht als solche erkannt. Bei einer großen Anzahl von versuchten Straftaten sprechen technische Sicherungsmaßnahmen (z. B. Virens Scanner, Firewall oder Intrusion Detection Systeme) an. Der Betroffene löscht die Schadensprogramme, ohne diesen Angriff als Straftat zu erkennen oder anzuzeigen. Darüber hinaus ist mit dem Löschen die Beweisführung erschwert. Die tatsächlichen Fallzahlen im Bereich der Computerkriminalität dürften daher erheblich höher als die gemeldeten liegen. Das Dunkelfeld dürfte bedeutend sein.

1.2 Fallzahlen in einzelnen Deliktsfeldern

Den überwiegenden Anteil an der Gesamtfallzahl stellt nicht mehr allein der „Betrug mittels rechtswidrig erlangter Debitkarte mit PIN“ (4 975 Fälle). Aufgrund der Abnahme um 19 % nähern sich die Fallzahlen denen des „Computerbetrugs“ an (4 024 Fälle).

Die Steigerungsraten in den Deliktsbereichen „Fälschung beweisbarer Daten...“ und „Ausspähung von Daten“ beziehen sich in der Mehrzahl auf das Schwerpunktphänomen Phishing, wobei für das Jahr 2008 erstmalig zusammen mit dem Ausspähen von Daten auch die Vorbereitungshandlungen gemäß der §§ 202b StGB „Abfangen von Daten“, (23 Fälle) und 202c StGB „Vorbereitung des Ausspähens und Abfangen von Daten“ (169 Fälle) erfasst wurden.

Die meisten im Bereich Softwarepiraterie erfassten Delikte resultieren aus Ermittlungsverfahren wegen „Verstoß gegen das Urheberrechtsgesetz“ gegen Nutzer der so genannten „Filesharing-Tauschbörsen“. Hierbei handelt es sich um ein Massendelikt mit einem hohen Dunkelfeld.

Die Schwankungen in diesem Deliktsfeld resultieren regelmäßig aus gezielten Schwerpunktaktionen und dem jeweiligen Anzeigeverhalten der Rechteinhaber.

Zur Ermöglichung einer Identifizierung eines Urheberrechtsverletzers und anschließender zivilrechtlicher Verfolgung erstatteten die Rechtsvertreter der Musikindustrie bis Ende 2007 Strafanzeigen bei den Staatsanwaltschaften. Diese Ermittlungsvorgänge wurden nach Feststellung der IP-Adressen-Benutzer an die örtlichen Polizeibehörden zu weiteren Ermittlungen übersandt. Die Strafverfahren wurden mit Hinweis auf ein Privatklagedelikt durch die Staatsanwaltschaften eingestellt.

Eine von den Generalstaatsanwaltschaften aufgrund der Anzeigenüberflutung für NRW festgelegte Verfahrensweise führte ab 2008 zu einem deutlichen Rückgang der Fallzahlen, da entsprechende Anzeigen nicht mehr an die örtlichen Polizeibehörden zur weiteren Bearbeitung weitergeleitet wurden und somit keine Erfassung in der PKS stattfand. Mit der letzten Novelle des UrHG im Jahr 2008 wurde zudem den Rechteinhabern in § 101 ein eigenes Auskunftsrecht gegenüber den Internet Providern zugestanden, sofern der Täter in „gewerblichem Umfang“ gehandelt hat. Die Rechteinhaber können in diesen Fällen selbst die Anschlussinhaber der IP-Adressen bei den Internet Providern ermitteln. Gleichzeitig wurde in § 53 UrHG die Vervielfältigung zum privaten Gebrauch erlaubt, wenn sie nicht „Erwerbszwecken“ dient. Die Grenze für den „gewerblichen Umfang“ ist in der höchstrichterlichen Rechtsprechung noch nicht

definiert worden. Die Generalstaatsanwälte haben sich für den Erwerbszweck auf Grenzen geeinigt, die mit ca. 3000 Musik- oder 200 Filmdateien so hoch angesiedelt sind, dass sie nur in absoluten Ausnahmefällen erreicht werden. Die im Bereich der Wettbewerbsdelikte erfassten Straftaten machen für 2008 lediglich 0,02 % (0,08%) aller in NRW bekannt gewordenen Straftaten mit einem Anteil von 0,11 % (2007: 0,15 %) an dem insgesamt durch alle Straftaten verursachten Schaden aus.

1.3 Aufklärungsquoten

Die Aufklärungsquote im Jahr 2008 ist mit 34,7 % gegenüber 2007 (39,8 %) gesunken.

Die Aufklärungsquoten in den Deliktsfeldern sind rückläufig oder nur in Einzelbereichen ansteigend ("Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung" und „Datenveränderung / Computersabotage“).

Diese Tendenz resultiert überwiegend aus dem Anstieg des Phänomens Phishing, bei dem die Aufklärung dadurch erschwert wird, dass der Großteil der Tatverdächtigen über das Ausland agiert.

Die hohen Aufklärungsquoten bei der Softwarepiraterie erklären sich daraus, dass hier die Straftaten meist nur bei bekanntem Tatverdächtigen zur Anzeige gelangen, da diese erst bei Feststellung der Tatverdächtigen erkannt werden.

1.4 Schaden

Die Auswirkung der Computerkriminalität zeigt sich vor allem in den registrierten Schäden. Im Jahr 2008 belaufen sich die in der PKS registrierten Schäden aller mit Schadenssummen erfassten Delikte der Computerkriminalität im engeren Sinne auf 10 703 127,- €. Damit sind die registrierten Schäden 2,9 % niedriger als im Vorjahr (Schäden 2007: 11 018 799,- €).

1.5 Tatmittel Internet

Seit 2004 erfolgt die statistische Erfassung der Sonderkennung „Tatmittel Internet“.

Erfasst werden dabei grundsätzlich alle Delikte, zu deren Tatbestandsverwirklichung das Medium Internet als Tatmittel verwendet wird. Die Verwendung eines PC / Notebooks pp. allein reicht nicht aus.

Zu den zu erfassenden Straftaten gehören sowohl diejenigen, die durch das bloße Einstellen von Informationen in das Internet bereits die Tatbestände erfüllen, wie auch solche Delikte, bei denen das Internet lediglich als Kommunikationsmedium bei der Tatausführung eingesetzt wird.

Keine Erfassung erfolgt, wenn das Internet im Hinblick auf die Tatverwirklichung lediglich eine untergeordnete Rolle spielt, beispielsweise wenn Kontakte bzw. Kontaktversuche zwischen Täter und Opfer lediglich der eigentlichen Tat vorgelagert sind.¹

Bei dieser Sonderkennung werden sowohl ein Teil der Computerkriminalität i. e. S. als auch Teile der Delikte aus dem Bereich der Computerkriminalität i. w. S. erfasst.

Insgesamt wurden 25 880 Straftaten erfasst, bei denen als Tatmittel das Internet angegeben wurde, das sind 1,8 % der Gesamtkriminalität (2007: 56 432 Straftaten mit einem Anteil an der Gesamtkriminalität von 3,8 %). Im Vergleich zu 2007 bedeutet dies eine Abnahme um 30 552 Fälle oder 54,1 %. Selbst, wenn man ein Umfangsverfahren mit ca. 8 000 Fällen im Vorjahr herausrechnet, ist für 2008 ein Rückgang um 47 % zu verzeichnen. Dieser Rückgang entspricht nicht den fachlichen Erwartungen, die von einer Zunahme des Tatmittels Internet ausgehen.

Die Aufklärungsquote betrug 76,9 % (2007: 84,0 %).

In 81,9 % der Fälle handelte es sich um Betrugsdelikte, in 4,9 % um Sexualdelikte und in 2,8 % um Urheberrechtsverletzungen (2007: 74,5 % Betrugsfälle, 5,4 % Sexualdelikte, 10,7 % Straftaten gegen Urheberrechtsbestimmungen).

¹ Quelle: Richtlinien für die Führung der Polizeilichen Kriminalstatistik (PKS), RdErl. IM NRW vom 01.01.2003 – 42 – 6410 (SMBl. NRW. 293) i. d. F. vom 01.01.2008

1.6 Erkenntnisse aus dem Kriminalpolizeilichen Meldedienst IuK (KPMD IuK)

Der überwiegende Teil der Meldungen, die im Bereich der Computerkriminalität im Jahr 2008 eingegangen sind, befassen sich mit dem Phänomen Phishing (264 Fälle), die nächst größeren Komplexe sind mit 122 Fällen das Ausspähen von Daten einschließlich von Vorbereitungshandlungen und mit 40 Fällen das Ausspähen und der Einsatz von Kreditkartendaten über das Internet.

Im Jahr 2008 wurden 264 Phishing-Fälle über den KPMD IuK gemeldet (2007: 332, 2006: 293; 2005: 165). Dies bedeutet eine Abnahme von 20,5 % gegenüber 2007.

Auch 2008 erfolgen die Phishing-Attacken überwiegend per Trojanischem Pferd und seltener über gefälschte Internet-Seiten. In 16 Fällen erfolgte die Anwerbung von Finanzagenten über persönliche Kontaktaufnahme in Chat-Räumen. Hier wurde überwiegend von weiblichen Anwerbern die Legende der in Not geratenen russischen Freundin oder Schwester eingesetzt.

1.7 Zentrale Internetrecherchen

Im Jahr 2008 hat die Zentrale Internetrecherche des LKA NRW (ZIR) 547 Strafverfahren initiiert. Sie richten sich fast ausschließlich gegen inländische Tatverdächtige und sind an die Strafverfolgungsbehörden in den jeweils zuständigen Bundesländern abgegeben worden.

291 dieser Verfahren sind der Politisch motivierten Kriminalität (PMK) zuzurechnen und betreffen überwiegend Straftaten gemäß der §§ 86, 86a und 130 StGB².

Die von der ZIR geführte „OP Adel“ umfasste 177 Strafverfahren wegen des Besitzes, der Verschaffung und Verbreitung von Kinderpornografie. Insgesamt konnten 80 Tatverdächtige, davon sieben mit einschlägigen polizeilichen Erkenntnissen, ermittelt werden.

Elf Verfahren im Zusammenhang mit illegalem Handel von Medikamenten hatten Angebote von Anabolika, Potenz- und Schlankheitsmitteln zum Gegenstand.

Ermittlungen wegen des Verdachts des Betruges sind überwiegend auf die Beobachtung der Verkaufsplattformen „ebay.de“, „mobile.de“, „autoscout24.de“ und „hood.de“ zurückzuführen.

1.8 Erkenntnisse aus der EDV-Ermittlungsunterstützung

Auf Grund der zunehmenden Verbreitung der „Digitalisierung“ und „Vernetzung“ wird sich der derzeit schon hohe Bedarf an Maßnahmen der DV-Beweissicherung und kriminaltechnischen Untersuchungen (kurz: DV-Beweissicherung) zukünftig weiter erhöhen.

Die Standardmaßnahmen erstrecken sich im Wesentlichen auf die Beweissicherung an Personalcomputern mit gängigen Betriebssystemen und die auswertungsfähige Bereitstellung der gesicherten Daten für die polizeiliche Sachbearbeitung.

Diese Standardmaßnahmen erfolgen in den einzelnen Kreispolizeibehörden durch entsprechend aus- und fortgebildete Kräfte der IT-Ermittlungsunterstützung bzw. der Kriminalkommissariate Computerkriminalität.

Nur die schwierigen Fälle der DV-Beweissicherung, die ggf. auch den Einsatz spezieller Sicherungs- und Auswertungstechnik erfordern, übernimmt das Sachgebiet 44.1 (EDV-Ermittlungsunterstützung) des Landeskriminalamts Nordrhein-Westfalen als spezialisierte Dienststelle.

Immer mehr verlagert sich die Kommunikation von den „klassischen“ Formen wie persönlichem Gespräch, Brief, Festnetztelefonie, hin zu „digitalisierten“ Formen wie Mobiltelefonie, Computertelefonie (Voice over IP - VoIP), SMS-Versand, E-Mail-Verkehr, Internetforen, Chats etc. Auch bei unterschiedlichsten Kriminalitätsformen findet diese Veränderung der Kommunikation bei Vorbereitung, Begehung und Verschleierung von Straftaten immer mehr Verwendung.

Hier kommt im Rahmen der Strafverfolgung der Beweissicherung an PC-Systemen, Mobiltelefonen, SIM-Karten, PDAs und elektronischen Notizbüchern immer größere Bedeutung zu.

² § 86 StGB (Verbreiten von Propagandamitteln verfassungswidriger Organisationen), § 86a StGB (Verwenden von Kennzeichen verfassungswidriger Organisationen) und § 130 StGB (Volksverhetzung)

In den Vorjahren steigerte sich das Untersuchungsaufkommen bei den Mobiltelefonen und die diesbezüglichen Auswertungen allein beim Sachgebiet 44.1 des Landeskriminalamts Nordrhein-Westfalen um mehrere 100 %. (2005: 327 Mobiltelefone - 2006: 1 031 Mobiltelefone)

Auf Grund der Steigerung der Mobiltelefonauswertung in den Jahren 2005 und 2006 wurde für die 16 Kriminalhauptstellen ein Auswertungssystem für Mobiltelefone beschafft. Dies ermöglichte die Verlagerung eines Großteils der Auswertung auf diese Behörden, was mit einer Verringerung der Wartezeit auf die Auswertungsergebnisse für die Ermittlungsdienststellen verbunden war.

Im Jahr 2008 fielen bei den 16 Kriminalhauptstellen und dem Sachgebiet 44.1 des Landeskriminalamts Nordrhein-Westfalen 4.284 Mobiltelefone zur Untersuchung an (2007: 3 558).

2 Getroffene Maßnahmen

Die Computerkriminalität im weiteren Sinne nimmt deutlich zu. Es ist daher unbedingt erforderlich, dass neben allen Ermittlungsbeamten zur Bekämpfung der Computerkriminalität i. e. S. auch die Ermittlungsbeamten zur Bekämpfung der Computerkriminalität i. w. S. für Ermittlungen in der Computerkriminalität aus- und fortgebildet werden.

Das Landeskriminalamt Nordrhein-Westfalen setzt im Bereich der Bekämpfung der IT-Kriminalität einen strategischen Schwerpunkt („Cybercrime“).

Der interne Informationsaustausch zwischen den Sachraten IT-Ermittlungsunterstützung, den Sachbearbeitern der Computerkriminalität, dem Landesamt für Zentrale Polizeiliche Dienste Nordrhein-Westfalen, dem Landesamt für Aus-, Fortbildung und Personalangelegenheiten der Polizei Nordrhein-Westfalen und dem Landeskriminalamt Nordrhein-Westfalen erfolgt über das Intranetforum Computerkriminalität und über regelmäßig durchgeführte Dienstbesprechungen.

2.1 Phishing

Im Bereich des Computerbetruges wurde der Meldedienst für Phishing-Delikte beschleunigt, indem eine Meldung zum frühest möglichen Zeitpunkt vereinbart wurde.

Darüber hinaus erfolgte für den Meldedienst und das Vorgangsverwaltungsprogramm IGVP die Vereinheitlichung von Schlagworten zum Phänomenbereich Phishing.

Durch das Dezernat 13 (Finanzermittlungen / Geldwäsche) des Landeskriminalamtes Nordrhein-Westfalen werden im Deliktsbereich „Phishing“ auch die Geldwäscheverdachtsanzeigen der Banken entgegengenommen und bearbeitet, die auf die so genannten Finanz-Agenten hinweisen.

Das Dezernat 12 (IuK-Ermittlungen) hält aufgrund der Ermittlungserfahrungen im Deliktsbereich Phishing Vorträge, um für dieses Thema zu sensibilisieren. Diese Vorträge, die nicht nur vor polizeilichem Publikum gehalten werden, sind im gesamten Bundesgebiet stark nachgefragt.

2.2 Präventionshinweise

Die nachfolgenden Organisationen und Institutionen geben teilweise zusammen mit der Polizei Präventionsangebote zum Thema Computer- und Internetkriminalität (umfassend „Cybercrime“) heraus:

Initiative secure-it.nrw

„secure-it.nrw“ ist eine Landesinitiative des Ministeriums für Innovation, Wissenschaft, Forschung und Technologie des Landes Nordrhein-Westfalen, mit der das LKA NRW eine Kooperation eingegangen ist. Sie stellt Arbeitsmaterialien für Schulen zur Verfügung, die im Unterricht zu wesentlichen jugendrelevanten Themen verwandt werden können. Ferner bietet die Initiative auch Informationsbroschüren für den privaten Computernutzer zu Sicherheitsrisiken bei der Nutzung von PC und Internet. Diese Medien sind unter www.secure-it.nrw.de abrufbar. Zudem bietet secure-it.nrw Informationsveranstaltungen und Workshops zu entsprechenden Themen an.

IT-Newsletter des Programms Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK)

Das BKA ist für die Prävention von Computer- und Internetkriminalität bundesweit federführend zuständig und erstellt für das ProPK mindestens vierteljährlich den IT-Newsletter. Er wird über die ProPK-Ansprechpartner der Kommissariate Vorbeugung an die Kreispolizeibehörden weitergeleitet. Er kann auch im Extranet unter www.propk.extrapol.de/aktuelles/ abgerufen werden. Diese Fundstelle ist auch über das Intranetforum „Computerkriminalität/TKÜ“ zu erreichen.

Aktion „Kinder-sicher-im-Netz“

Die gemeinsame Aktion des ProPK, der Telekom AG und der Freiwilligen Selbstkontrolle Multimedia (FSM) unterstützt Eltern, Lehrer und Erziehungsverantwortliche bei der Vermittlung von Medienkompetenz zu den Themen „Sicherheit beim Chatten“, „Gefährliche Seiten im Internet“ und „Allgemeine Sicherheit im Internet“. Hierzu hat sie vor allem Medien-Podcasts und einen Medienkompetenz-Trainer entwickelt. Die Inhalte sind abrufbar unter www.polizei-beratung.de/vorbeugung/medienkompetenz/internet.

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Das dem Bundesministerium des Inneren nachgeordnete Amt ist für Fragen der IT-Sicherheit in der Informationsgesellschaft zuständig. Das BSI untersucht Sicherheitsrisiken bei der Anwendung der Informationstechnik, entwickelt Sicherheitsvorkehrungen, informiert über Risiken und Gefahren beim Einsatz der Informationstechnik und entwickelt Lösungsvorschläge. Das BSI stellt Sicherheitshinweise für Bürgerinnen und Bürger im Inter- wie auch im Intranet unter www.bsi.de und www.bsi-fuer-buerger.de bereit.

Landesanstalt für Medien NRW (LfM)

Zu den Aufgaben des LfM zählen neben der Zulassung und der Aufsicht über private Rundfunkveranstalter auch die Forschung zur Medienentwicklung und die Förderung der Medienkompetenz. Hierzu veröffentlicht sie Forschungsergebnisse und führt Maßnahmen für verschiedene Zielgruppen durch. Auf Anfrage stellt sie Referenten auch für polizeiliche Veranstaltungen zur Verfügung. Inhalte und Ergebnisse ihrer Tätigkeit können auf der Internetseite www.lfm-nrw.de eingesehen werden.

Schulen ans Netz e.V.

Die Initiative des Bundesministeriums für Bildung und Forschung und der Telekom AG zielt darauf ab, speziell in Schulen, am Arbeitsplatz oder im privaten Umfeld Chancen und Risiken digitaler Medien und den richtigen und sicheren Umgang mit ihnen kompetent und gebündelt darzustellen. Neben zielgruppenorientierten Kampagnen bietet sie Kommunikationsräume, Lehrmaterial, Newsletter und Fortbildungen an. Die Informationen sind unter www.schulen-ans-netz.de abrufbar.

3 Ausblick

Die Zahl der Delikte der Computerkriminalität im weiteren Sinne wird voraussichtlich ansteigen. In dem Ausmaß, in dem die Computernutzung immer weitere Bereiche des täglichen Lebens erfasst, wird der Computer vermehrt als Vorbereitungs-, Unterstützungs- oder Begehungsmittel bei Straftaten dienen. Damit wird IuK-Technik immer mehr zum Tat- und Beweismittel.

Gleiches gilt spezieller auch für die Tatbegehungen über das Internet. Deliktsbereiche wie Verstöße gegen das Urheberrecht erhalten durch die immer weiter zunehmende Nutzung von Breitbandzugängen (z. B. DSL) eine andere Qualität und können in kurzen Tatzeiträumen realisiert werden.

Eine Entwicklung, die sich in den letzten Jahren abzeichnet und sich sicherlich weiter fortsetzen wird, ist die „Kommerzialisierung“ der Computerkriminalität. Dort, wo vor Jahren Hacker und Computer-Freaks Rechner angriffen, um ihre Neugierde zu befriedigen und ihr „Können“ unter Beweis zu stellen oder auf Schwachstellen aufmerksam zu machen, werden diese Fähigkeiten heute vermehrt von organisierten kriminellen Strukturen eingesetzt, um schnelle und große Profite zu machen.

Eine umfassende Situationsdarstellung, Analyse von Verbesserungsbereichen und Handlungsempfehlungen zur Bekämpfung der „Cybercrime“, an denen polizeiliche und externe Experten (Vertreter führender, auch sicherheitsrelevanter Unternehmen; Provider; Dienste; BSI; Forschungseinrichtungen usw.) mitwirkten, hat die Bund-Länder-Projektgruppe „Strategie der Bekämpfung der IuK-Kriminalität“ der Kommission Kriminalitätsbekämpfung (KKB) erstellt.

Der Bericht beschreibt die Lage und ihre zunehmende kriminalpolitische Bedeutung, Risiken der weiteren Entwicklung, Verbesserungsbedarf sowie die Notwendigkeit einer nachhaltigen Steuerung über Schwerpunktsetzungen auf den Phänomenbereich „Cybercrime“.

Die Handlungsempfehlungen zielen auf die Verbesserung der Erkenntnisgewinnung, der repressiven und präventiven Bekämpfung, verstärkte Netzwerkarbeit und Zusammenarbeit zwischen öffentlichen und privaten Stellen ab. Sie beleuchten zudem Qualifizierungsaspekte, Organisationsfragen bei Sicherheits- und Strafverfolgungsbehörden sowie die Überprüfung und Fortentwicklung des Rechts und der Rechtshilfe.

Der Bericht der Projektgruppe, an der auch das LKA NRW mitwirkte, befindet sich in der länderübergreifenden Abstimmung. Fragen der Umsetzung in Nordrhein-Westfalen werden gemeinsam mit dem Innenministerium bewertet.

4 Anlagen

4.1 Definitionen

Computerkriminalität im engeren Sinne

Die Computerkriminalität (luK-Kriminalität) umfasst im „engeren Sinne“ alle Straftaten, bei denen Elemente der EDV in den Tatbestandsmerkmalen enthalten sind, wie zum Beispiel Computerbetrug (§ 263 a StGB) oder Ausspähen von Daten (§ 202 a StGB).

Computerkriminalität im weiteren Sinne

Computerkriminalität im weiteren Sinne bezeichnet alle Straftaten, bei denen die EDV zur Planung, Vorbereitung oder Ausführung eingesetzt wird. Diese erstrecken sich mittlerweile auf ein weites Spektrum an Kriminalitätsformen, wie z. B. Wirtschaftskriminalität, Betrugsdelikte u. v. a. Eine spezielle Begehungsform stellt die Verbreitung inkriminierter Inhalte in Schrift, Abbildung, Film oder Tondatei unter Ausnutzung von EDV dar.

Phishing

Der Begriff setzt sich aus „password“ und „fishing“ zusammen und könnte mit „nach Passwörtern angeln“ übersetzt werden. Die Täter versuchen Informationen wie z. B. Kontodaten, Kreditkartendaten, Daten für das Online-Banking oder Daten von Konten in Internet-Versteigerungshäusern / -Kaufhäusern zu erlangen, um diese für eigene Transaktionen zu verwenden.

4.2 Auftrag „Lagebild“

Der Erlass des Innenministeriums Nordrhein-Westfalen vom 22.04.2003 - 42.2. - 6527 „Bekämpfung der Computerkriminalität durch die Polizei Nordrhein-Westfalen,“ beauftragt das Landeskriminalamt Nordrhein-Westfalen in diesem Deliktsbereich phänomen-spezifische und phänomenübergreifende Lagebilder darzustellen.

Seit dem Jahr 2003 erstellt das Landeskriminalamt Nordrhein-Westfalen jährlich ein Lagebild „Computerkriminalität“, um die Informationsbasis der mit der Bearbeitung der Computerkriminalität betrauten Behörden zu erweitern und damit die Bekämpfung der luK-Kriminalität zu verbessern.

4.3 Datenbasis

Grundlage dieses Lagebildes sind sowohl Daten aus der PKS als auch Sachverhalte aus dem KPMD-luK.

In der Polizeilichen Kriminalstatistik werden unter dem Summenschlüssel 8970 nur die Delikte der Computerkriminalität im engeren Sinne zusammengefasst:

- Betrug mittels rechtswidrig erlangter Debitkarten mit PIN
- Computerbetrug nach § 263a StGB
- Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei der Datenverarbeitung nach §§ 269, 270 StGB
- Datenveränderung, Computersabotage nach §§ 303a, 303b StGB
- Ausspähen, Abfangen von Daten einschl. Verbreitungshandlungen gem. §§ 202a, 202b und 202c StGB³
- Softwarepiraterie (privates Handeln)
- Softwarepiraterie (gewerbsmäßiges Handeln)
- Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten

Diese erfassten PKS-Daten ergeben kein wirklichkeitsgetreues Abbild der Computerkriminalität in ihrer kriminologischen Gesamtheit, da die Straftaten der Computerkriminalität im weiteren Sinne, wie z. B. Betrugsdelikte im Zusammenhang mit Online-Auktionshäusern, Beleidigungsdelikte oder Urheberrechtsverletzungen nur unter ihrem Grundtatbestand erfasst werden.

³ In diesem Umfang erst ab 2008 erfasst (vorher Ausspähen von Daten nach § 202a StGB).

Im Kriminalpolizeilichen Meldedienst luK-Kriminalität melden die Polizeibehörden folgende Straftaten der Computerkriminalität:

- § 202a StGB Ausspähen von Daten
- § 202b StGB Abfangen von Daten
- § 202c StGB Vorbereitungshandlungen zum Ausspähen von Daten
- § 263a StGB Computerbetrug (ohne: Missbrauch von Zahlungskarten- und Missbrauch von Internetzugangsdaten)

- § 269 StGB Fälschung beweisheblicher Daten
- § 270 StGB Täuschung im Rechtsverkehr bei Datenverarbeitung
- §§ 271, 274 Nr. 2, 348 StGB Falschbeurkundung/ Urkundenunterdrückung im Zusammenhang mit Datenverarbeitung
- § 303a StGB Datenveränderung
- § 303b StGB Computersabotage

Während sich aus der PKS nur wenige Angaben zu der einzelnen Straftat entnehmen lassen, bietet der KPMD-luK die Möglichkeit einer differenzierten Auswertung von Informationen zur Phänomenologie einzelner Delikte.

Um neue Erscheinungsformen der Computerkriminalität zeitnah erkennen zu können, bietet der KPMD-luK den sachbearbeitenden Dienststellen auch die Möglichkeit, Straftaten über den Katalog hinaus zu melden, wenn

- zur Tatbegehung hohes luK-Fachwissen auf Täterseite erforderlich ist
- durch Täter besondere Techniken zur konspirativen Kommunikation genutzt werden
- eine Tat von grundsätzlicher bzw. bundesweiter Bedeutung ist
- ein überdurchschnittlich hoher Schaden vorliegt
- ein besonderer Modus Operandi festgestellt wird.

Aber auch die Daten aus dem KPMD-luK ergeben keine umfassende Datenbasis polizeilich bekannt gewordener Computerkriminalität, da ein Vergleich zeigt, dass nicht alle in der PKS erfassten Straftaten auch im Meldedienst erscheinen.

4.4 Tabellen und Diagramme

Tabelle 1: Fallzahlen in einzelnen Deliktsfeldern der Computerkriminalität

	Delikte		Zu- bzw. Abnahme		
	2007	2008			%
Computerbetrug	4 265	4 024	-	241	- 5,7
Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung	1 073	1 312	+	239	+ 22,3
Datenveränderung / Computersabotage	977	628	-	349	- 35,7
Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen	1 377	1 876	+	499	+ 36,2
Betrug mittels rechtswidrig erlangter Debitkarte mit PIN	6 145	4 975	-	1 170	- 19,0
Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten	525	585	+	60	+ 11,4
Softwarepiraterie private Anwendung	905	166	-	739	- 81,7
Softwarepiraterie gewerbsmäßiges Handeln	200	38	-	162	- 81,0
Computerkriminalität insgesamt	15 467	13 604	-	1 863	- 12,0

Tabelle 2: Aufklärungsquoten

	aufgeklärte Fälle		Aufklärungsquote %		Zu- bzw. Abnahme % - Punkte
	2007	2008	2007	2008	
Computerbetrug	1 573	1 293	36,9	32,1	- 4,8
Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung	367	586	34,2	44,7	+ 10,5
Datenveränderung / Computersabotage	139	148	14,2	23,6	+ 9,4
Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen	433	483	31,5	23,4	- 8,1
Betrug mittels rechtswidrig erlangter Debitkarte mit PIN	2 372	1 780	38,6	35,8	- 2,8
Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten	269	273	51,2	46,7	- 4,5
Softwarepiraterie private Anwendung	806	162	89,1	97,6	+ 8,5
Softwarepiraterie gewerbsmäßiges Handeln	192	37	96,0	97,4	+ 1,4
Computerkriminalität insgesamt	6 151	4 717	39,8	34,7	- 5,1

Tabelle 3: Entwicklung der Fallzahlen und der Aufklärungsquoten von 1990 bis 2008

Jahr	bekannt gewordene Fälle			Aufklärung	
	erfasste Fälle	Zu- bzw Abnahme	aufgeklärte Fälle	Aufklärungs- quote %	
	insgesamt	%			
1990	1 156	-	1,5	603	52,2
1991	1 910	+	65,2	1 008	52,8
1992	2 746	+	43,8	1 276	46,5
1993	2 950	+	7,4	1 205	40,9
1994	4 788	+	62,3	1 874	39,1
1995	5 909	+	23,4	2 374	40,2
1996	8 271	+	40,0	3 810	46,1
1997	9 914	+	19,9	4 703	47,4
1998	10 921			4 613	42,2
1999	11 347	+	3,9	5 605	49,4
2000	13 323	+	17,4	5 858	44,0
2001	20 736	+	55,6	12 104	58,4
2002	14 059	-	32,2	5 927	42,2
2003	14 098	+	0,3	5 803	41,2
2004	17 026	+	20,8	7 133	41,9
2005	16 806	-	1,3	6 553	39,0
2006	15 068	-	1,0	6 331	42,0
2007	15 467	+	2,7	6 151	39,8
2008	13 604	-	12,0	4 717	34,7

bis 1997 ohne Betrug mittels Zugangsberechtigungen zu Kommunikationsdiensten

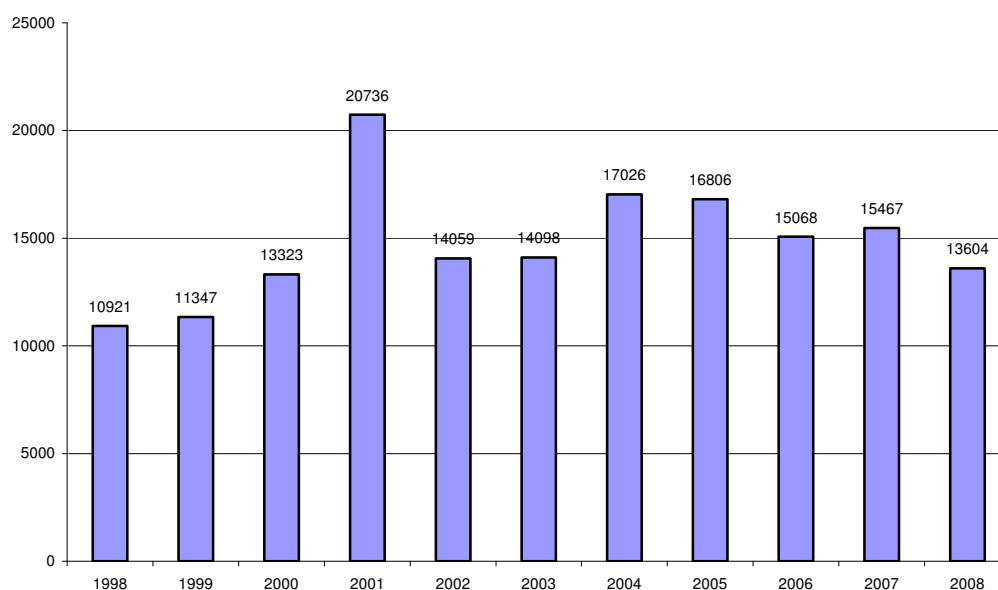
Tabelle 4: Altersverteilung der Tatverdächtigen

Jahr	Tatverdächtige										insgesamt
	14		18		unter 21		ab 21		insgesamt		
	bis unter 14	bis unter 18	bis unter 18	bis unter 21	insgesamt	insgesamt	insgesamt	insgesamt	insgesamt	insgesamt	
	absolut	Anteil %	absolut	Anteil %	absolut	Anteil %	absolut	Anteil %	absolut	Anteil %	
1995	15	1,0	162	10,6	251	16,4	428	28,0	1 098	72,0	1 526
1996	28	1,7	157	9,4	255	15,3	440	26,3	1 230	73,7	1 670
1997	47	2,4	226	11,6	327	16,7	600	30,7	1 354	69,3	1 954
1998	32	1,3	292	11,7	352	14,1	676	27,2	1 812	72,8	2 488
1999	66	2,6	352	13,9	387	15,3	805	31,8	1 727	68,2	2 532
2000	93	2,9	491	15,2	492	15,3	1 076	33,3	2 150	66,7	3 226
2001	115	2,8	798	19,1	710	17,0	1 623	38,9	2 546	61,1	4 169
2002	96	2,9	473	14,3	497	15,0	1 066	32,2	2 240	67,8	3 306
2003	87	2,5	382	11,1	482	14,0	951	27,7	2 480	72,3	3 431
2004	68	1,9	375	10,3	473	12,9	916	25,1	2 739	74,9	3 655
2005	75	2,1	350	9,7	425	11,8	850	23,7	2 739	76,3	3 589
2006	46	1,3	396	11,5	420	12,2	862	25,0	2 589	75,0	3 451
2007	68	1,7	453	11,4	485	12,2	1 006	25,2	2 985	74,8	3 991
2008	61	1,6	383	10,2	457	12,1	901	24,0	2 849	76,0	3 750

Tabelle 5: Tatmittel Internet

Tatmittel Internet			
	erfasste Fälle		darunter
	insgesamt	Tatmittel Internet	
		2008	absolut
Straftaten insgesamt	1 453 203	25 880	1,8
Straftaten gegen die sexuelle Selbstbestimmung	11 861	1 276	10,8
- Verbreitung pornografischer Erzeugnisse	3 332	1 180	35,4
darunter:			
- Besitz / Verschaffen von Kinderpornografie	1 171	475	40,6
- Verbreitung von Kinderpornografie	497	186	37,4
Betrug	197 774	21 189	10,7
darunter:			
- Waren- und Warenkreditbetrug	69 853	14 978	21,4
- Computerbetrug	4 024	1 773	44,1
- Betrug mit Zugangsdaten zu Kommunikationsdiensten	585	126	21,5
Fälschung beweisrelevanter Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung	1 312	732	55,8
Datenveränderung, Computersabotage	628	423	67,4
Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen	1 876	712	38,0
Straftaten gegen Urheberrechtsbestimmungen	2 378	723	30,4
darunter:			
- Softwarepiraterie - private Anwendung	166	52	31,3
- Softwarepiraterie - gewerbsmäßig	200	25	12,5

Diagramm 1: Computerkriminalität - bekannt gewordene Fälle



4.5 Ansprechpartner / Ergänzende Hinweise

Landeskriminalamt Nordrhein-Westfalen
Abteilung 4
Sachgebiet 44.1 - ZISC
KHK Thomas Himmel
0211 / 939 - 4470

Weitere Lagebilder und ergänzende Informationen zu Phänomenen der Computerkriminalität finden Sie im Internet:
www1.polizei.nrw.de/lka/fakten_und_zahlen/lagebilder/

Herausgeber

Landeskriminalamt Nordrhein Westfalen
Völklinger Str. 49
40221 Düsseldorf

Dezernat 44
Sachgebiet 44.1 - EDV-Ermittlungsunterstützung / ZISC
Redaktion:

Tel.: (0211) 939-4470 oder Polizeinetz 07 – 224-4470
Fax: (0211) 939-4479 oder Polizeinetz 07 – 224-4479

SG441.LKA@polizei.nrw.de

Impressum

Landeskriminalamt Nordrhein-Westfalen
Völklinger Str. 49
40221 Düsseldorf

Tel.: (0211) 939-0
Fax: (0211) 939-4119

landeskriminalamt@polizei.nrw.de
www.lka.nrw.de

