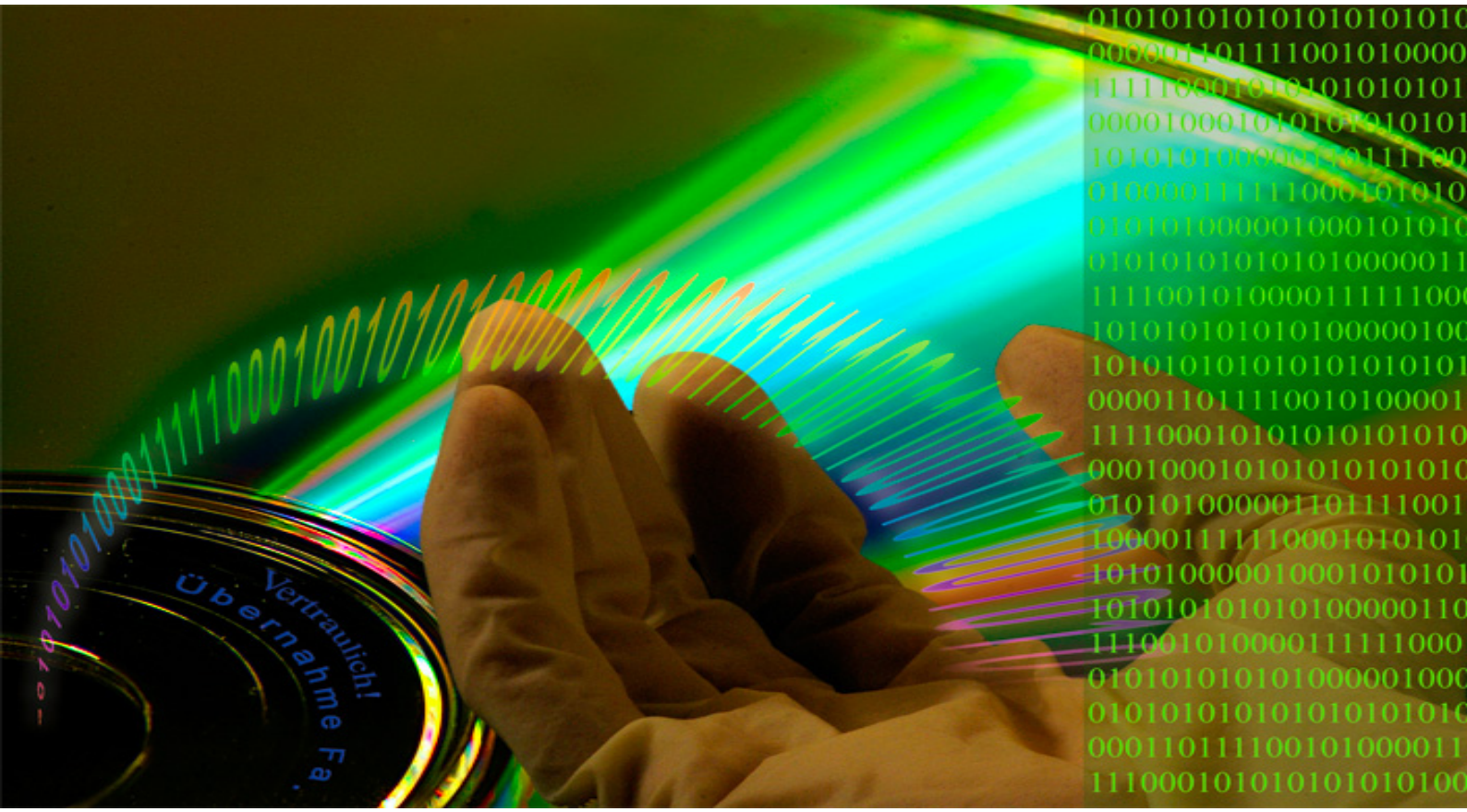
Landeskriminalamt
Nordrhein-Westfalen



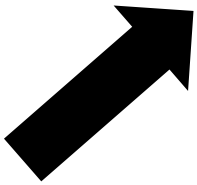
Computerkriminalität

Lagebild 2009

www.lka.nrw.de

Kriminalitätsentwicklung im Überblick

Computerkriminalität



	2008	2009	in %	
Gesamt	**13.604**	**15.541**	**+ 14,2**	↗
Computerbetrug	4.024	5.113	+ 27,0	↗
Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung	1.312	1.256	- 4,3	↘
Datenveränderung/Computersabotage	628	656	+ 4,5	↗
Ausspähen; Abfangen von Daten einschl. Vorbereitungshandlungen gem. §§ 202 a, 202 b, 202 c StGB	1.876	2.695	+ 43,7	↗
Betrug mittels rechtswidrig erlangter Debitkarte mit PIN	4.975	5.027	+ 1,1	↗
Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten	585	722	+ 23,4	↗
Softwarepiraterie (private Anwendung)	166	60	- 63,9	↘
Softwarepiraterie (gewerbsmäßiges Handeln)	38	12	- 68,4	↘

Inhaltsverzeichnis Seite

1 Lagedarstellung

1.1 Entwicklung der Fallzahlen

Von den insgesamt 1.458.438 in Nordrhein-Westfalen polizeilich bekannt gewordenen Straftaten im Jahr 2009 sind nach der Polizeilichen Kriminalstatistik (PKS) 15.541 Fälle (1,1 %) der Computerkriminalität zuzuordnen. Dies entspricht einer Zunahme um 1.937 Fälle (14,2 %) gegenüber dem Vorjahr (2008: 13.604 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. Diese variieren seither zwischen 13.604 (2008) und 17.026 (2004).

In den Deliktsfeldern Datenveränderung/Computersabotage ist von einem großen Dunkelfeld auszugehen. Geschädigte Firmen zeigen aus Angst um ihr Ansehen in der Öffentlichkeit und daraus resultierender wirtschaftlicher Nachteile, Straftaten nur sehr selten an. Darüber hinaus werden Straftaten oft nicht als solche erkannt. Bei einer großen Anzahl von versuchten Straftaten sprechen technische Sicherungsmaßnahmen (z. B. Virenscanner, Firewall oder Intrusion Detection Systeme) an. Der Betroffene löscht die Schadprogramme, 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.

1.2 Fallzahlen in einzelnen Deliktsfeldern

Als häufigstes Delikt hat der „Computerbetrug“ (5.113 Fälle) den „Betrug mittels rechtswidrig erlangter Debitkarte mit PIN“ (5.027 Fälle) abgelöst.
Die hohen Fallzahlen in den Deliktsbereichen „Fälschung beweiserheblicher Daten…“ und „Ausspähen von Daten“ beziehen sich in der Mehrzahl auf das Schwerpunktphänomen Phishing, wobei seit dem Jahr 2008 zusammen mit dem Ausspähen von Daten auch die Vorbereitungshandlungen gemäß der §§ 202 b StGB „Abfangen von Daten„ (2009: 31 Fälle; 2008: 23) und 202 c StGB „Vorbereitung des Ausspähens und Abfangens von Daten“ (2009: 163 Fälle; 2008: 169) erfasst werden.

Die meisten im Bereich Softwarepiraterie erfassten Delikte resultieren aus Ermittlungsverfahren wegen Verstößen gegen das Urheberrechtsgesetz (UrHG) gegen Nutzer der so genannten „Filesharing-Börsen[1]“. Hierbei handelt es sich um ein Massendelikt mit einem hohen Dunkelfeld.
Die Schwankungen in diesem Deliktsfeld resultieren regelmäßig aus gezielten Schwerpunktaktionen der Rechteinhaber und deren Anzeigeverhalten.
Zur Identifizierung der Täter und anschließender Geltendmachung zivilrechtlicher Ansprüche gegenüber diesen erstatteten die geschädigten Firmen der Musikindustrie bis Ende 2007 Strafanzeigen bei den Staatsanwaltschaften. Diese Ermittlungsvorgänge wurden nach Feststellung der IP-Adressen-Benutzer an die örtlich zuständigen Polizeibehörden zu weiteren Ermittlungen übersandt. Die Strafverfahren wurden i. d. R. mit Hinweis auf ein Privatklagedelikt durch die Staatsanwaltschaften eingestellt.
Eine von den Generalstaatsanwaltschaften aufgrund der bis 2007 festzustellenden starken Zunahme entsprechender Strafanzeigen für NRW geänderte Verfahrensweise führte seit 2008 zu einem deutlichen Rückgang der Fallzahlen. Die entsprechenden Anzeigen wurden nicht mehr an die örtlich zuständigen Polizeibehörden zur weiteren Bearbeitung weitergeleitet, wodurch dort auch keine Erfassung in der PKS mehr erfolgte. Mit der letzten Novelle des UrHG im Jahr 2008 wurde zudem den Rechteinhabern in § 101 ein eigenes Auskunftsrecht gegenüber den Internetprovidern zugestanden, sofern der Täter in „gewerblichem Umfang“ gehandelt hat. Die Rechteinhaber können in diesen Fällen selbst die Anschlussinhaber der IP-Adressen bei den Internetprovidern ermitteln. Gleichzeitig wurde in § 53 UrHG die Vervielfältigung zum privaten Gebrauch erlaubt, wenn sie nicht „Erwerbszwecken“ dient. Die Grenze für den „gewerblichen Umfang“ wurde höchstrichterlich bisher nicht konkretisiert. Die Generalstaatsanwälte in NRW orientieren sich derzeit an Grenzwerten von ca. 3.000 Musik- oder 200 Filmdateien. Diese Grenzwerte wurden bisher nur in Ausnahmefällen erreicht bzw. überschritten.

[1] internetbasierte Tauschbörsen, wie BitTorrent, eDonkey2000. Kazaa etc.

1.3 Aufklärungsquoten

Die Aufklärungsquote im Jahr 2009 ist mit 32,1 % gegenüber 2008 (34,7 %) gesunken.
Die Aufklärungsquoten in den meisten Deliktsfeldern sind rückläufig, 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 Server im 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 2009 belaufen sich die in der PKS registrierten Schäden aller mit Schadenssummen erfassten Delikte der Computerkriminalität auf 12.504.181 €. Damit liegt der registrierte Schaden um 16,8 % über dem Wert des Vorjahres (2008: 10.703.127 €).

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.[2]
Bei dieser Sonderkennung werden sowohl ein Teil der IuK-Kriminalität i. e. S. als auch Teile der Delikte aus dem Bereich der IuK-Kriminalität i. w. S. erfasst.

Insgesamt wurden 54.881 Straftaten erfasst, bei denen als Tatmittel das Internet angegeben wurde, das sind 3,8 % der Gesamtkriminalität (2008: 25.880 Straftaten mit einem Anteil an der Gesamtkriminalität von 1,8 %). Im Vergleich zu 2008 bedeutet dies eine Zunahme um 29.001 Fälle oder 112,1 %. Durch diesen deutlichen Anstieg der Fallzahlen wird in etwa wieder der Stand von 2007 (56.432 Fälle und ein Anteil von 3,8 % an der Gesamtkriminalität) erreicht.
Die Aufklärungsquote betrug 77,3 % (2008: 76,9 %).
In 87,4 % der Fälle handelte es sich um Betrugsdelikte, in 2,2 % um Sexualdelikte und in 0,3 % um Urheberrechtsverletzungen (2008: 81,9 % Betrugsdelikte, 4,9 % Sexualdelikte, 2,8 % Straftaten gegen Urheberrechtsbestimmungen).

1.6 Erkenntnisse aus dem Kriminalpolizeilichen Meldedienst IuK (KPMD IuK)

Der überwiegende Teil der Meldungen, die im Bereich der IuK-Kriminalität im Jahr 2009 eingegangen sind, befassen sich mit dem Phänomen Phishing (480 Fälle). Dies bedeutet eine Zunahme von 84,4 % gegenüber 2008 (2008: 264, 2007: 332, 2006: 293; 2005: 165).
Der durchschnittliche Schaden pro Phishing-Fall wird auf ca. 4.000 € bis 5.000 € geschätzt.

[2] 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

Auch 2009 erfolgten die Phishing-Attacken, wie schon in den Vorjahren, überwiegend per „Trojanischem Pferd“ und seltener über gefälschte Internet-Seiten. Der Trend geht hin zum so genannten „Echtzeit-Trojaner“, der Kontodaten und TAN während einer Online-Banking-Aktion abfängt.
Zur Verbreitung der „Trojanischen Pferde“ werden in vielen Fällen Botnetze verwandt.
Die Anwerbung von Finanzagenten erfolgt sowohl über dubiose „Job-Angebote“ wie auch über persönliche Kontaktaufnahme in Chat-Räumen. Hier wurde überwiegend von weiblichen Anwerbern die Legende der in Not geratenen russischen Freundin oder Schwester eingesetzt.
Zunehmend werden Finanzagenten nicht mehr vor Ort angeworben sondern es werden Osteuropäer nach Deutschland geholt, die zeitlich begrenzt in einzelnen Städten verbleiben, dort Konten eröffnen und als Finanzagenten dienen. Nach kurzer Zeit wechseln sie ihr Tätigkeitsgebiet, um in einer anderen Stadt in gleicher Weise vorzugehen, bevor sie Deutschland wieder verlassen.

Aus dem KPMD IuK ergab sich für 2009 ein neues Phänomen, das Hacking von Telefon-Anlagen. In einigen Telefon-Anlagen eines Herstellers (und den baugleichen Anlagen anderer Vertreiber) wurde ein Einrichtungsfehler[3] ausgenutzt, der es gestattete, diese Anlagen von außen zu manipulieren. Über diese Lücke wurden in den Anlagen Rufumleitungen auf ausländische Mehrwertnummern eingerichtet. Dies führte dazu, dass Gebühren generiert und über die Telefonrechnung an die Betreiber der ausländischen Mehrwertnummern abgeführt wurden.

1.7 Ermittlungskommissionen des Landeskriminalamts NRW (LKA NRW)

Die EK Joker wurde 2009 mit den Verurteilungen der beiden deutschen Haupttäter zu mehrjährigen Haftstrafen beendet. Das LG Bonn verhängte dabei Haftstrafen von 4 Jahren sowie 2 Jahren und 2 Monaten. Die Verurteilungen sind somit die höchsten, die in diesem Deliktsbereich in Deutschland bisher verhängt worden sind.
Die vorwerfbaren Schäden im Bereich Phishing beliefen sich auf mindestens 687.783 € aus mindestens 150 vorwerfbaren Einzeltaten.
Es konnten ausländische Mittäter ermittelt werden. Gegen einzelne Mittäter waren Verfahren im Ausland anhängig bzw. dauern die Ermittlungen noch an.

1.8 Zentrale Internetrecherchen

Im Jahr 2009 hat die Zentrale Internetrecherche (ZIR) des LKA NRW 1.143 Strafverfahren initiiert, die sich nahezu ausschließlich gegen inländische Tatverdächtige richteten. In 325 Fällen verfügten die Tatverdächtigen über einen Wohnsitz in NRW.
Zur Kinder-, Jugend-, Gewalt- und Tierpornografie hat die ZIR 501 Strafverfahren, davon 214 mit Tatort in NRW eingeleitet. In Einzelfällen konnten durch weitere Ermittlungen der zuständigen Polizeibehörden Missbrauchssituationen aufgedeckt werden. Unter anderem konnte eine Polizeibehörde in Süddeutschland den mehrere Jahre andauernden Missbrauch von zwei heute 11 und 8 Jahre alten Mädchen durch ihren Vater beenden.
229 Verfahren waren der Politisch motivierten Kriminalität zuzurechnen und betreffen überwiegend Straftaten gemäß § 86 StGB (Verbreiten von Propagandamitteln verfassungswidriger Organisationen), § 86 a StGB (Verwenden von Kennzeichen verfassungswidriger Organisationen) und 130 StGB (Volksverhetzung). In 40 Fällen konnten Tatverdächtige in NRW ermittelt werden.
388 Verfahren, davon 62 in NRW, hatten den illegalen Handel mit Medikamenten und Betäubungsmitteln zum Gegenstand.
Veröffentlichung von Bauanleitungen für Bomben, Ausspähen von Daten, Betrug, Phishing, Landesverrat und Kannibalismus sind weitere Felder, in denen die ZIR Strafverfahren initiierte.
Die Mitarbeiter der ZIR haben zu Recherchezwecken zusätzlich zur Software zur Verfolgung von Straftaten im BitTorrent-Netzwerk ein Tool für das eDonkey2000[4] Netzwerk entwickelt.

[3] In diesen Fällen wurde das entsprechende Kennwort auf der herstellerseitigen Grundeinstellung belassen
[4] BitTorrent und eDonkey2000 sind Netzwerke zum Austausch von Dateien.

1.9 Erkenntnisse aus der IT-Ermittlungsunterstützung

Auf Grund der zunehmenden Verbreitung der „Digitalisierung“ und „Vernetzung“ wird sich der derzeit schon hohe Bedarf an Maßnahmen der EDV-Beweissicherung und kriminaltechnischen Untersuchungen 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 EDV-Beweissicherung, die ggf. auch den Einsatz spezieller Sicherungs- und Auswertungstechnik erfordern, übernimmt das Sachgebiet 44.1 (EDV-Ermittlungsunterstützung) des LKA NRW als spezialisierte Dienststelle.
Immer mehr verlagert sich die Kommunikation von den „klassischen“ Formen wie persönlichem Gespräch, Brief, Festnetztelefonie, hin zu „digitalisierten“ und IP-basierten[5] 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, verteilten Datenbeständen, Mobiltelefonen, SIM-Karten, PDAs und Navigationsgeräten immer größere Bedeutung zu.

In den Vorjahren steigerte sich das Untersuchungsaufkommen bei den Mobiltelefonen derart, dass die Auswertungen nicht mehr allein beim LKA NRW erfolgen konnten. Daher wurde für die 16 Kriminalhauptstellen ein Auswertungssystem für Mobiltelefone beschafft. Dies ermöglichte die Verlagerung eines Großteils der Auswertung auf diese Behörden, was mit einer Beschleunigung der Auswertungen verbunden war.

Im Jahr 2009 fielen bei den 16 Kriminalhauptstellen und dem Sachgebiet 44.1 des LKA NRW 5.023 Mobiltelefone zur Untersuchung an (2008: 4.284).

[5] IP = Internet Protokoll. Die Daten (z. B. bei Voice over IP) werden hier nicht mehr als Audio-Datei in einem fortlaufenden Strom, sondern als Datenpakete über das Internet versandt.

2 Getroffene Maßnahmen

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

Das LKA NRW setzte im Bereich der Bekämpfung der IuK-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 LKA NRW erfolgt über das Intranetforum Computerkriminalität und über regelmäßig durchgeführte Dienstbesprechungen.

2.1 Phishing und Botnetze

Im Bereich des Computerbetruges wurde der Meldedienst für Phishing-Delikte beschleunigt, indem eine Meldung zum frühest möglichen Zeitpunkt zu erstatten ist.
Darüber hinaus erfolgte für den Meldedienst und das Vorgangsverwaltungsprogramm IGVP die Vereinheitlichung von Schlagworten zum Phänomenbereich Phishing.

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

Das Dezernat 12 (Computerkriminalität) 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.
Im Jahr 2009 wurde durch das Dezernat 12 bereits die zweite bundesweite Dienstbesprechung zum Thema Phishing und Botnetze ausgerichtet.

Das LKA NRW führte eine landesweite Dienstbesprechung für die Sachbearbeiter „Phishing“ in den Kreispolizeibehörden durch.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) und der Verband der deutschen Internetwirtschaft (eco) entwickelte ein Konzept, nach dem die Internetprovider ihre Kunden auf eine Bot-Infektion ihres PCs hinweisen. Dazu soll in der ersten Jahreshälfte 2010 eine Beratungsstelle eingerichtet werden, die die Anwender dabei unterstützen soll, ihren Rechner von Viren und Bots zu befreien. Damit soll die Gefährdung durch Botnetze verringert werden.

2.2 Präventionshinweise

Präventionsansätze

Maßnahmen der polizeilichen Kriminalprävention zielen bei den sehr variantenreichen Tatbegehungsformen der IuK-Kriminalität darauf ab, vor allem mit Mitteln der Öffentlichkeitsarbeit über Risiken und Gefahren beim Einsatz von Informations- und Kommunikationstechnik aufzuklären. Außerdem werden technische Sicherungen wie der Einsatz von Virenschutzprogrammen sowie Verhaltensweisen empfohlen, die Risiken minimieren können. Die Polizei konzentriert sich dabei auf Hauptzielgruppen wie private Nutzer des Internets und des Online-Bankings und Multiplikatoren wie Eltern oder Lehrer, die ihre Kinder oder Schüler beispielsweise zum sicheren Surfen im Netz, Teilnahme an Online-Communities oder Chatten in Foren anleiten können.
Das Informationsangebot zur IuK-Sicherheit ist heute vielfältig, leider aber auch unübersichtlich. Deshalb hat die Kommission Kriminalitätsbekämpfung[6] empfohlen, den Bekanntheitsgrad, die Akzeptanz und den Informationsgehalt der bisherigen Angebote der Privatwirtschaft und staatlicher Stellen zu prüfen. Zudem sollen sie – in Kooperation mit anderen Trägern – möglichst unter einer Adresse im Internet zur Verfügung gestellt werden. Diese Vorschläge greift die Projektgruppe „Internetkriminalität“ der Kommission Polizeiliche Kriminalprävention auf.

Aktuelle Präventionstipps bieten:

Intranet des LKA NRW

Das LKA NRW stellt auf seiner Intranetseite einen Informationspool zur Prävention von IuK-Kriminalität bereit, siehe http://pol.duesseldorf-lka.polizei.nrw.de/praev.htm. Zu finden sind dort u. a. Studien und Antworten auf allgemeine Fragen sowie Informationen zu Modi Operandi und Arbeitsmaterialien für Präventionsdienststellen.
Weitere empfehlenswerte Informationen bieten der IT-Newsletter des Programms Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK) www.propk.extrapol.de, die Aktion „Kinder-sicher-im-Netz“ www.sicher-im-netz.de, das Bundesamt für Sicherheit in der Informationstechnik (BSI) www.bsi.de oder www.bsi-fuer-buerger.de, die Landesanstalt für Medien NRW (LfM) www.lfm-nrw.de sowie der „Schulen ans Netz e. V“ www.schulen-ans-netz.de.
Diese Angebote wurden im Lagebild Computerkriminalität 2008 ausführlich beschrieben. Hinzugekommen sind:

Die Initiative „SCHAU-HIN!“

„SCHAU-HIN!“ ist eine vom Bundesministerium für Familie, Senioren, Frauen und Jugend, Vodafone, ARD, ZDF und TV Spielfilm unterstützte Initiative. Sie soll die Öffentlichkeit für die vielfältigen Gefahren, denen Kinder im Umgang mit Medien ausgesetzt sein können, sensibilisieren. Die Initiative stellt Informationen und Arbeitsmaterialien für Eltern, Kinder und Erziehungsbeauftragte kostenlos zur Verfügung, die von Fachkräften verschiedener Ressorts erarbeitet werden. Außerdem veranlassen ihre Partner Aufklärungskampagnen in den TV- und Printmedien. Details sind unter www.schau-hin.info nachlesbar.

„Surfen mit SIN(N)“

Das Kooperationsprojekt „Surfen mit SIN(N) Sicherheit im Netz“ steht unter der Schirmherrschaft des Sozial- und Kriminalpräventiven Rats der Stadt Bielefeld. Beteiligt sind das PP Bielefeld, das Medienzentrum Bielefeld, das Kompetenzteam NRW Bielefeld und die Bürgerstiftung Bielefeld. Das Projekt informiert über die Einsatzmöglichkeiten des Internet in der Schule, klärt über Chancen und Risiken auf, sensibilisiert im Umgang mit Online-Medien, fördert die Medienkompetenz und die Prävention von IuK-Kriminalität. Zielgruppen sind neben den Kindern, die an Schülerprojekten mitwirken, deren Eltern und die Lehrkräfte an Schulen. Näheres dazu unter www.surfen-mit-sinn.de.

[6] Quelle: Bericht der Bund-Länder-Projektgruppe der Kommission Kriminalitätsbekämpfung zur „Strategischen Ausrichtung der Bekämpfung der IuK-Kriminalität“, BKA, 2009.

3 Ausblick

Die Zahl der Delikte der Computerkriminalität 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.

Mit Erlass des Innenministeriums Nordrhein-Westfalen (IM NRW) vom 03.08.2009 - 42.2-62.17.08/42.2-62.18.09 wurde das LKA NRW mit der Einrichtung einer landesweiten Arbeitsgruppe zur Überprüfung des Aktualisierungs- bzw. Fortschreibungsbedarfs der Erlassregelungen hinsichtlich der „Bekämpfung der Computerkriminalität durch die Polizei NRW“ beauftragt.
Das Ergebnis der Arbeitsgruppe soll dem IM NRW im bis Ende April 2010 vorgelegt werden.

4 Anlagen

4.1 Definitionen

Computerkriminalität
Die IuK-Kriminalität „im engeren Sinne“ (Computerkriminalität) umfasst alle Straftaten, bei denen Elemente der EDV in den Tatbestandsmerkmalen enthalten sind. Dazu zählen:

- Betrug mittels rechtswidrig erlangter Debitkarten mit PIN
- Computerbetrug nach § 263 a StGB
- Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei der Datenverarbeitung nach §§ 269, 270 StGB
- Datenveränderung, Computersabotage nach §§ 303 a, 303 b StGB
- Ausspähen, Abfangen von Daten einschl. Vorbreitungshandlungen gem. §§ 202 a, 202 b und 202 c StGB[7]
- Softwarepiraterie (privates Handeln)
- Softwarepiraterie (gewerbsmäßiges Handeln)
- Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten

IuK-Kriminalität im weiteren Sinne
IuK-Kriminalität „im weiteren Sinne“[8] bezeichnet alle Straftaten, bei denen die EDV zur Planung, Vorbereitung oder Ausführung eingesetzt wird. Diese erstrecken sich mittlerweile auf nahezu alle Deliktsbereiche. Eine spezielle Begehungsform stellt die Verbreitung inkriminierter Inhalte in Schrift, Abbildung, Film oder Tondatei unter Ausnutzung von EDV dar.

Cybercrime
Im Zusammenhang mit der Kriminalität unter Nutzung von Informations- und Kommunikationstechnik wird national und international der Begriff „Cybercrime“[9] verwandt. Dieser Begriff ist nicht definiert und wird in unterschiedlichen Zusammenhängen und mit verschiedenen Bedeutungen verwandt. Im Zusammenhang mit diesem Lagebild ist der Begriff „Cybercrime“ mit dem Begriff „IuK-Kriminalität“ gleichzusetzen.

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 betrügerische Transaktionen zu verwenden.

Botnetz
Der Begriff ist die Kurzform von Roboter-Netzwerk. Darunter versteht man ein fernsteuerbares Netzwerk von Computern im Internet. Dieses Netzwerk wird von Bot-Programmen gebildet, die vom Inhaber des befallenen Rechners nicht kontrolliert werden können. Die Kontrolle wird durch „Würmer“ bzw. „Trojanische Pferde“ erreicht, die den Computer infizieren und dann auf Anweisungen aus dem Internet (von sog. „Bot-Servern“) warten. Diese Netzwerke können für Spam-Verbreitung, Verbreitung von Phishing-Mails, Denial-of-Service-Attacken usw. verwendet werden, zum Teil, ohne dass die betroffenen PC-Nutzer dies bemerken.

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

[8] Gemäß Erlass IM NRW vom 22.04.2003 - 42.2-6527 auch als „Computerkriminalität im weiteren Sinne“ bezeichnet

[9] Europarat, Übereinkommen über Computerkriminalität (SEV Nr. 185), Deutschland ratifizierte das Übereinkommen am 09.03.2009; es trat am 01.07.2009 in Deutschland in Kraft.

4.2 Auftrag „Lagebild“

Mit Erlass des IM NRW vom 22.04.2003 - 42.2-6527 „Bekämpfung der Computerkriminalität durch die Polizei Nordrhein-Westfalen„ wurde das LKA NRW beauftragt, in diesem Deliktsbereich phänomenspezifische und phänomenübergreifende Lagebilder zu erstellen.
Seit dem Jahr 2003 erstellt das LKA NRW jährlich ein Lagebild „Computerkriminalität“, um die Informationsbasis der mit der Bearbeitung der Computerkriminalität betrauten Behörden zu erweitern und damit die Bekämpfung der IuK-Kriminalität zu verbessern.

4.3 Datenbasis

Grundlage dieses Lagebildes sind Daten aus der PKS und Sachverhalte aus dem KPMD IuK.
In der Polizeilichen Kriminalstatistik werden unter dem Summenschlüssel 8970 nur die Delikte der Computerkriminalität im engeren Sinne zusammengefasst (siehe Nr. 4.1)
Diese erfassten PKS-Daten ergeben kein wirklichkeitsgetreues Abbild der IuK-Kriminalität 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.

Im KPMD IuK melden die Polizeibehörden folgende Straftaten der Computerkriminalität:

- § 202 a StGB — Ausspähen von Daten
- § 202 b StGB — Abfangen von Daten
- § 202 c StGB — Vorbereitungshandlungen zum Ausspähen von Daten
- § 263 a StGB — Computerbetrug (ohne: Missbrauch von Zahlungskarten- und Missbrauch von Internetzugangsdaten)
- § 269 StGB — Fälschung beweiserheblicher Daten
- § 270 StGB — Täuschung im Rechtsverkehr bei Datenverarbeitung
- §§ 271, 274 Nr. 2, 348 StGB — Falschbeurkundung/Urkundenunterdrückung im Zusammenhang mit Datenverarbeitung
- § 303 a StGB — Datenveränderung
- § 303 b StGB — Computersabotage

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

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

- zur Tatbegehung hohes IuK-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 oder
- ein besonderer Modus Operandi festgestellt wird.

Aber auch die Daten aus dem KPMD IuK 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		
	2008	2009			%
Computerbetrug	4.024	5.113	+	1.089	+ 27,0
Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung	1.312	1.256	-	56	- 4,3
Datenveränderung/ Computersabotage	628	656	+	28	+ 4,5
Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen	1.876	2.695	+	819	+ 43,7
Betrug mittels rechtswidrig erlangter Debitkarte mit PIN	4.975	5.027	+	52	+ 1,1
Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten	585	722	+	137	+ 23,4
Softwarepiraterie private Anwendung	166	60	-	106	- 63,9
Softwarepiraterie gewerbsmäßiges Handeln	38	12	-	26	- 68,4
Computerkriminalität insgesamt	13.604	15.541	+	1.937	+ 14,2

Tabelle 2: Aufklärungsquoten

	aufgeklärte Fälle		Aufklärungsquote %		Zu- bzw. Abnahme
	2008	2009	2008	2009	% - Punkte
Computerbetrug	1.293	1.610	32,1	31,5	- 0,6
Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung	586	630	44,7	50,2	+ 5,5
Datenveränderung / Computersabotage	148	211	23,6	32,2	+ 8,6
Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen	483	517	23,4	19,2	- 4,2
Betrug mittels rechtswidrig erlangter Debitkarte mit PIN	1.780	1.754	35,8	34,9	- 0,9
Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten	273	199	46,7	27,6	- 19,1
Softwarepiraterie private Anwendung	162	57	97,6	95,0	- 2,6
Softwarepiraterie gewerbsmäßiges Handeln	37	11	97,4	91,7	- 5,7
Computerkriminalität insgesamt	4.717	4.989	34,7	32,1	- 2,6

Tabelle 3: Entwicklung der Fallzahlen und der Aufklärungsquoten von 1990 bis 2009

Jahr	insgesamt		%	Fälle	quote %
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
2009	15.541	+	14,2	4.989	32,1

bis 1997 ohne Betrug mittels Zugangsberechtigungen zu Kommunikationsdiensten

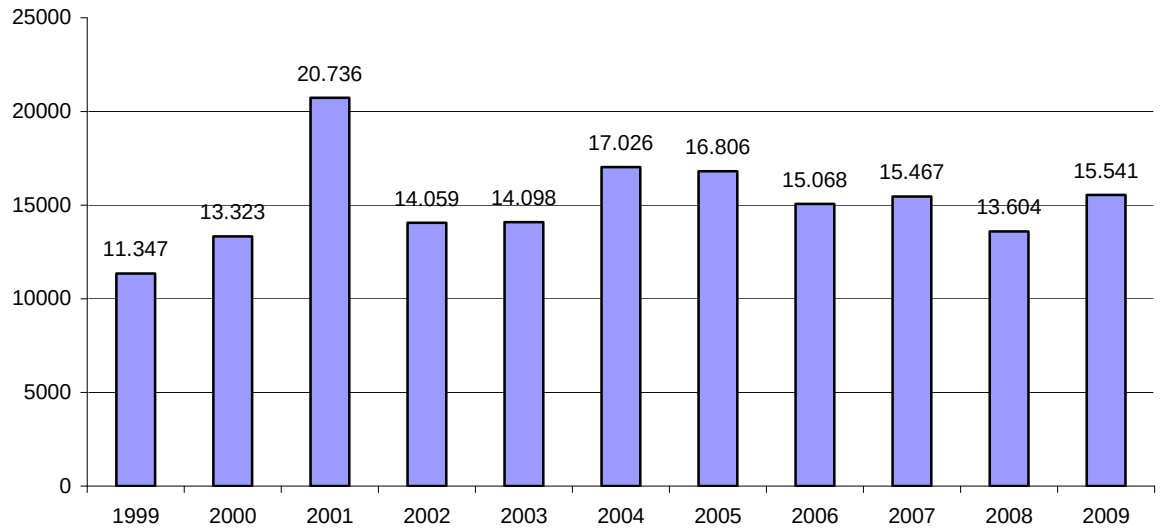
Tabelle 4: Altersverteilung der Tatverdächtigen

	Tatverdächtige										
	bis unter 14		14 bis unter 18		18 bis unter 21		unter 21 insgesamt		ab 21 insgesamt		insge-samt
Jahr	**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
2009	65	1,4	412	9,1	544	12,0	1.021	22,6	3.499	77,4	4.520

Tabelle 5: Tatmittel Internet

Tatmittel Internet			
	erfasste Fälle	darunter	
	insgesamt	Tatmittel Internet	
	2009	absolut	Anteil %
Straftaten insgesamt	**1.458.438**	**54.881**	**3,8**
Straftaten gegen die sexuelle Selbstbestimmung	10.435	1.208	11,6
- Verbreitung pornografischer Erzeugnisse	2.195	1.164	53,0
darunter:			
- Besitz/Verschaffen von Kinderpornografie	682	424	62,2
- Verbreitung von Kinderpornografie	854	524	61,4
Betrug	223.405	47.945	21,5
darunter:			
- Waren- und Warenkreditbetrug	86.841	33.248	38,3
- Computerbetrug	5.113	3.938	77,0
- Betrug mit Zugangsdaten zu Kommunikationsdiensten	722	400	55,4
Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung	1.256	857	68,2
Datenveränderung, Computersabotage	656	580	88,4
Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen	2.695	1.758	65,2
Straftaten gegen Urheberrechtsbestimmungen	2.428	900	37,1
darunter:			
- Softwarepiraterie - private Anwendung	60	45	75,0
- Softwarepiraterie - gewerbsmäßig	12	6	50,0

Diagramm 1: Computerkriminalität - bekannt gewordene Fälle



Grafik LKA NRW 2010

4.5 Ansprechpartner/Ergänzende Hinweise

Landeskriminalamt Nordrhein-Westfalen
Abteilung 4
Sachgebiet 44.1 - ZISC
KHK Thomas Himmel
0211-939-4470
thomas-himmel@polizei.nrw.de

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 - ZISC
Redaktion:
Tel.: 0211-939-4470 oder Polizeinetz 07-224-4470
Fax: 0211-939-194470 oder Polizeinetz 07-224-194470

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