POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

Cybercrime in NRW – Entwicklung und Bewertung

Lagebild 2012

www.lka.nrw.de

POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

Kriminalitätsentwicklung im Überblick

Cybercrime[1] in NRW – Entwicklung und Bewertung

- Fallzahlen der Cybercrime im engeren Sinne[2] steigen weiter an
- niedrigste Aufklärungsquote seit Erfassung der Cybercrime im engeren Sinne (1987)
- erneut starke Zunahme der Erpressungen mit Tatmittel Internet
- Datenveränderung und Computersabotage - Fallzahlen mehr als verdoppelt

	2011	2012		in %	Tendenz[3]
Cybercrime im engeren Sinne	**20.036**	**22.228**	+	**10,9**	↗
Computerbetrug	6.277	6.087	-	3,0	↘
Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung	1.994	2.278	+	14.2	↗
Datenveränderung/Computersabotage	1.498	4.118	+	174,9	↗
Ausspähen; Abfangen von Daten einschl. Vorbereitungshandlungen gem. §§ 202 a, 202 b, 202 c StGB	3.257	4.373	+	34,3	↗
Betrug mittels rechtswidrig erlangter Debitkarte mit PIN	6.108	4.880	-	20,1	↘
Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten	881	419	-	52,4	↘
Straftaten mit Tatmittel Internet	**47.992**	**54.339**	**+**	**13,2**	↗
Betrug mit Tatmittel Internet	37.923	35.987	-	5,1	↘
Erpressung mit Tatmittel Internet	336	1.324	+	294,0	↗

[1] Der international gebräuchliche Begriff „Cybercrime“ ist der Computerkriminalität gleichgesetzt (RdErl. des MIK NRW vom 29.02.2012 – 423.62.18.09)

[2] Informationen zur Definition und Abgrenzung unter 6.1

[3] Farbe Schwarz = moderate Tendenz, Farbe Rot = deutlich negative Tendenz, Farbe Grün = deutlich positive Tendenz

POLIZEI Nordrhein-Westfalen Landeskriminalamt

Inhaltsverzeichnis

Seite

1 Lagedarstellung

1.1 Vorbemerkungen

Das Lagebild Cybercrime stellt phänomenspezifisch und phänomenübergreifend die Entwicklung der Cybercrime im engeren Sinne sowie einzelner Delikte, die mit Hilfe des Tatmittels Internet begangen werden, im Land Nordrhein-Westfalen dar. Die Daten[4] basieren auf Verfahren der Polizeibehörden in NRW, die nach einheitlichem Standard erhoben werden. Die Klammerwerte im Text beziehen sich, soweit nicht anders angegeben, auf die entsprechenden Vorjahreswerte. In einzelnen Phänomenen ist von einem enormen Dunkelfeld auszugehen, da der Polizei viele Straftaten nicht bekannt werden.

1.2 Verfahrensdaten

Im Jahr 2012 stieg die Anzahl der Straftaten in der Polizeilichen Kriminalstatistik im Bereich der Cybercrime im engeren Sinne um 2.192 auf den bisherigen Höchststand von 22.228 Fällen. Der Anstieg fällt im Vergleich zum Vorjahr 2011 mit 10,9 % wieder deutlicher aus. Insgesamt steigen die Fallzahlen (nach einem Rückgang in den Jahren 2005-2008) seit 2009 kontinuierlich an (2009: +14,2 %, 2010: +27,2 %, 2011: +1,3 %). Unter den insgesamt 3.753 ermittelten Tatverdächtigen waren 783 oder 20,9 % Nichtdeutsche. Wiederholt fand eine Vielzahl von polizeilich bekannt gewordenen Fällen insbesondere der Datenveränderung bzw. Computersabotage durch im Ausland agierende Täter in der Polizeilichen Kriminalstatistik keine Berücksichtigung. Diese Auslandsstraftaten (z. B. "BKA-Trojaner") wurden nach der bisher geltenden bundeseinheitlichen Richtlinie in der Polizeilichen Kriminalstatistik nicht erfasst.

1.3 Einzelne Deliktsfelder

Computerbetrug

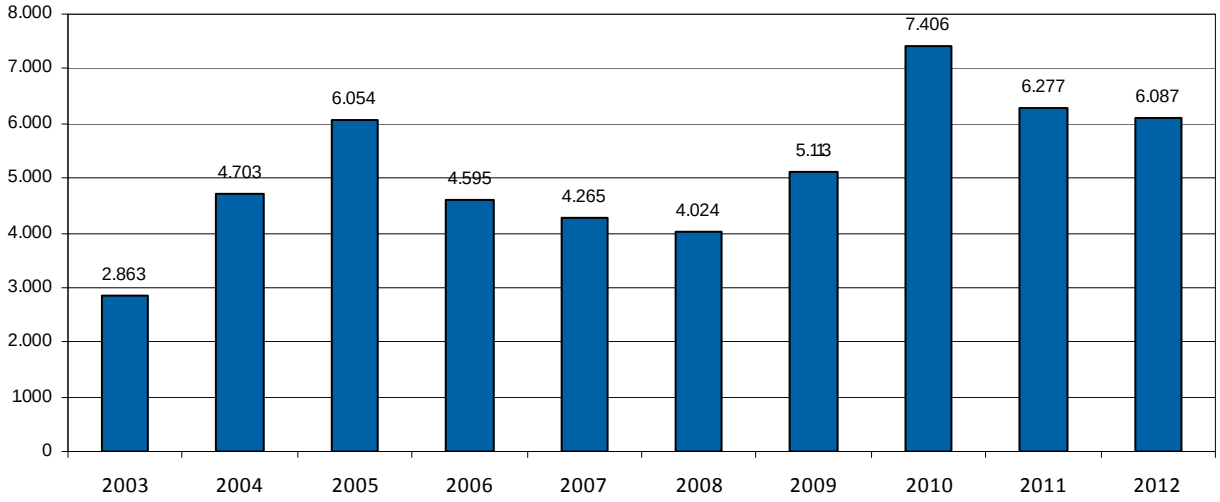
In diesem Deliktsfeld ist ein erneuter Rückgang um 190 Fälle (-3,0 %) zu verzeichnen. Vor allem Fälle des Missbrauchs ausgeforschter Bankzugangsdaten und E-Commerce-Accounts werden hierunter gefasst. Die Einführung wirksamer technischer Sicherungen wie eTAN[5] und mTAN[6] (vgl. 3.1) erschwert den unberechtigten Einsatz von Kontozugangsdaten und dürfte maßgeblich zum Rückgang der Fallzahlen beigetragen haben.

[4] Erläuterungen zu den Datenquellen unter 6

[5] Die temporär gültige TAN wird durch einen individualisierten TAN-Generator erzeugt.

[6] mobile Transaktionsnummer, die per SMS übertragen wird

Computerbetrug



Grafik: LKA NRW 2012

Datenquelle: PKS 2012

Diagramm 1: Entwicklung der Fallzahlen des Computerbetrugs

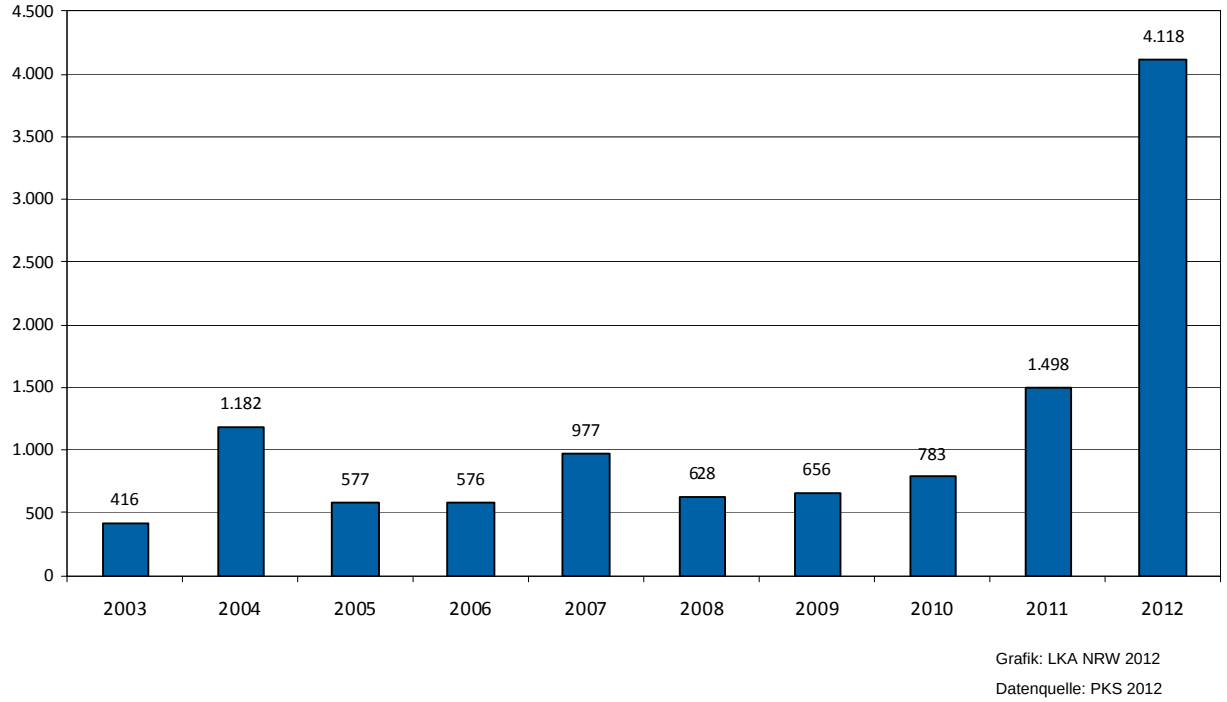
Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei der Datenverarbeitung

Die Auswertung der gestiegenen Fallzahlen (+14,2% = 284 Fälle) weist einen hohen Anteil von Phishing-Delikten aus. In vielen Fällen kommt es dabei nicht zu einer Zugangsdatenerlangung, so dass strafrechtlich lediglich die Fälschung beweiserheblicher Daten erfüllt ist. Dies führt zu einer geänderten Erfassung in der Polizeilichen Kriminalstatistik und bestätigt die Vorjahresthese aus dem Lagebild IuK-Kriminalität NRW 2011, wonach die Sensibilisierung der Nutzer und die technischen Sicherheitsvorkehrungen zunehmend greifen.

Datenveränderung, Computersabotage

Während sich bereits im Jahr 2011 die Fallzahlen nahezu verdoppelten, fällt die Zunahme im Jahr 2012 mit einer Steigerung von 174,9 % noch deutlicher aus. Ursächlich ist u. a. das weiterhin hohe Aufkommen von Ransomware (vgl. 3.3). Auch die Verbreitung sonstiger Schadprogramme nimmt weiter zu. Die kompromittierten Computersysteme werden dabei nicht nur nach sensiblen Daten durchsucht und ausgespäht, sondern mitunter als Bestandteil großer fernsteuerbarer Netzwerke (so genannte Bot-Netze) für Straftaten genutzt.

Datenveränderung/Computersabotage



Grafik: LKA NRW 2012
Datenquelle: PKS 2012

Diagramm 2: Entwicklungen der Fallzahlen der Datenveränderung/Computersabotage

Ausspähen, Abfangen von Daten einschließlich Vorbereitungshandlungen

Die Fallzahlen stiegen 2012 von 3.257 Fällen um 1.116 oder 34,3 % auf 4.373 Fälle an. Der Deliktschwerpunkt lag beim Ausspähen von Daten (3.276 Fälle oder 74,9 %).

Eine genauere Betrachtung der Fälle weist auch für diesen Bereich einen bedeutenden Anteil von Phishing-Fällen aus. Die Cyberkriminellen konzentrierten sich dabei insbesondere auf Zugangsdaten zu Onlinebanking-Konten, Packstationen, E-Commerce-Konten und Kreditkartendaten.

Betrug mittels rechtswidrig erlangter Debitkarten[7] mit PIN

Der Rückgang der Fallzahlen um 1.228 Fälle (-20,1 %) könnte mit dem gleichzeitigen Rückgang von Taschendiebstählen (-17,3 %) in Zusammenhang stehen. Der missbräuchliche Einsatz durch Diebstahl erlangter Debitkarten unter Nutzung der PIN zählt zu den typischen Verwertungshandlungen. Trotz aller Warnungen ist der leichtfertige Umgang der Geschädigten mit ihrer PIN, die oftmals als Notiz in der Geldbörse oder Handtasche mitgeführt wird, eine häufige Ursache.

Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten

Mit 419 erfassten Fällen ist ein deutlicher Rückgang von 52,4 % im Vergleich zum Vorjahr (881 Fälle) zu bilanzieren. Der missbräuchliche Einsatz von SIM-Karten (z. B. nach Diebstahl auf dem Postweg oder

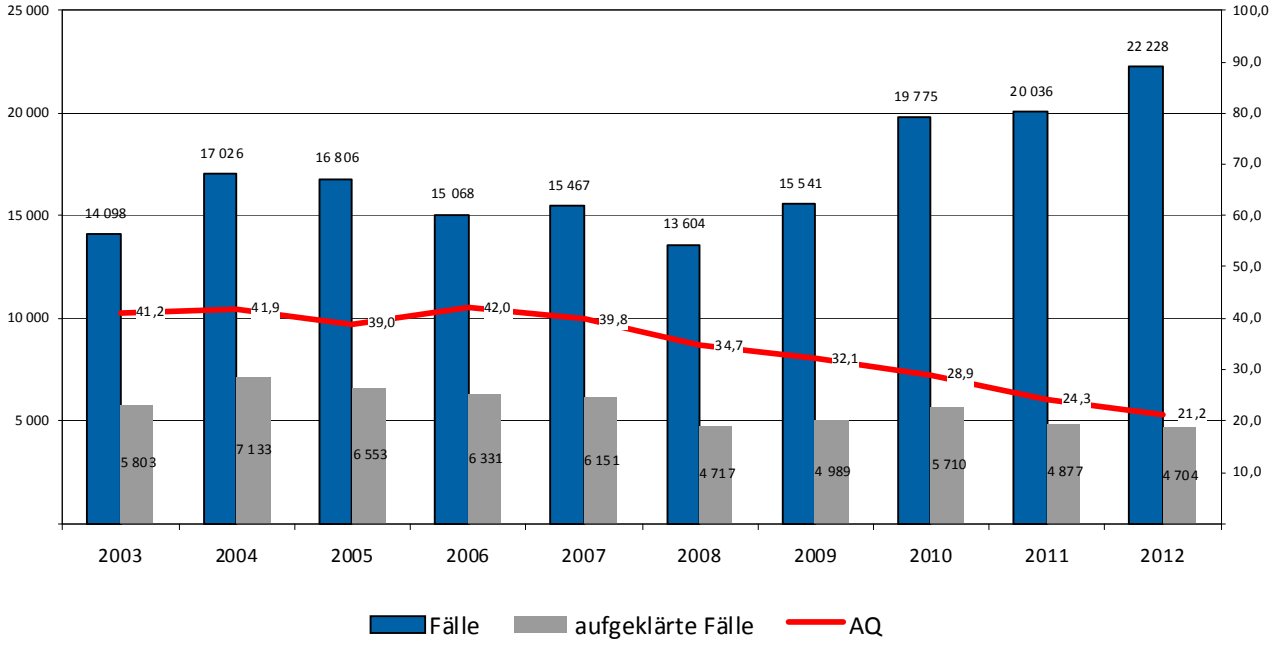
[7] Zahlungskarten, deren Einsatz unmittelbar zur Kontobelastung führt - girocard oder so genannte ec-Karte; PIN = Persönliche Geheimzahl („**P**ersonal **I**dentification **N**umber“)

durch betrügerischen Vertragsabschluss mit missbräuchlich genutzten Identitäten) und Zugangskennungen für Kommunikationsdienste sowie die Manipulation von Telekommunikationsanlagen sind die wesentlichen Phänomene, die hier erfasst werden.

1.4 Aufklärungsquote

Die Aufklärungsquote der Cybercrime im engeren Sinne ist im Jahr 2012 mit 21,2 % gegenüber den Jahren 2011 (24,3 %) und 2010 (28,9 %) erneut gesunken. Damit setzt sich die Tendenz der letzten zehn Jahre fort. Die Fallzahlen steigen bereits seit dem Jahr 2008 kontinuierlich an.

Vergleich Fallzahlen und Aufklärungsquote



Grafik: LKA NRW 2012
Datenquelle: PKS 2012

Diagramm 3: Darstellung von erfassten und aufgeklärten Fällen der Cybercrime im engeren Sinne

Aus der Polizeilichen Kriminalstatistik kann bereits ein Faktor für die sinkende Aufklärungsquote unmittelbar abgelesen werden: Die Quote sinkt selbst bei steigender Aufklärungsleistung (Anzahl der aufgeklärten Fälle) durch den Anstieg der Fallzahlen. Andere wesentliche Ursachen für diese Entwicklung werden unter 2. „Ermittlungshemmnisse“ gesondert beleuchtet.

1.5 Schaden

Im Jahr 2012 wurde in der Polizeilichen Kriminalstatistik für die Delikte der Cybercrime im engeren Sinne eine Gesamtschadenssumme von 12.227.294 Euro (2011: 16.173.242) erfasst. Gegenüber dem Vorjahr ist die Gesamtschadenssumme abermals reduziert. Die gestiegenen Fallzahlen der Cybercrime im engeren Sinne sind ausschließlich auf die Steigerung bei den Deliktsarten „Datenveränderung“ und „Compu-

tersabotage“ (+ 174,9 %) zurückzuführen[8]. Bei diesen Delikten werden keine Schäden erfasst. Dagegen gingen die Fallzahlen der Delikte mit Schadenserfassung deutlich zurück.

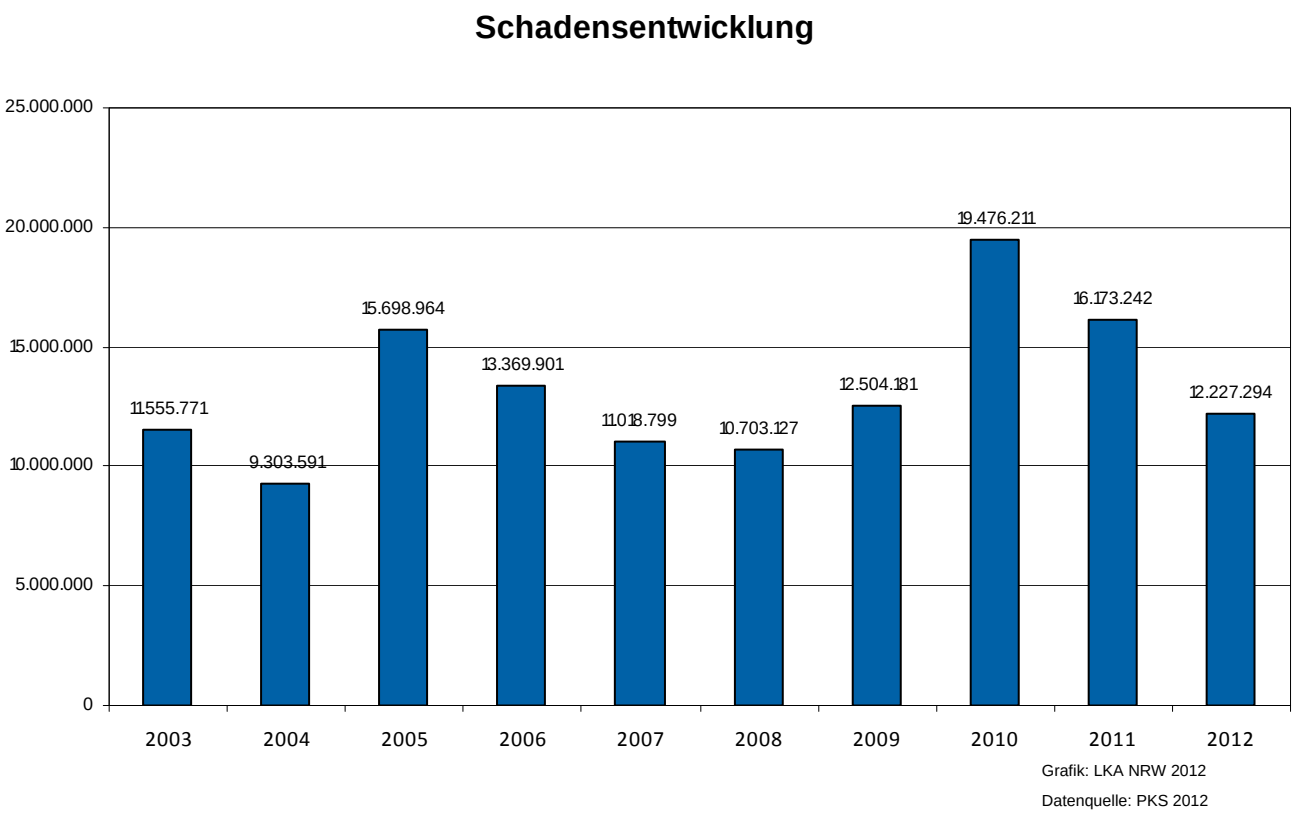


Diagramm 4: Entwicklung der Schadenssummen zur Cybercrime im engeren Sinne

1.6 Tatmittel Internet

Straftaten, bei denen das Internet als Tatmittel verwendet wird, werden in der Polizeilichen Kriminalstatistik mit der Sonderkennung „Tatmittel Internet“ erfasst.

Es kommen sowohl Straftaten in Betracht, bei denen das bloße Einstellen von Informationen in das Internet bereits Straftatbestände erfüllt (so genannte Äußerungs- bzw. Verbreitungsdelikte) als auch solche Delikte, bei denen das Internet als Kommunikationsmedium bei der Tatbestandsverwirklichung eingesetzt wird. Spielt das Internet im Hinblick auf die Tatverwirklichung eine untergeordnete Rolle, beispielsweise wenn Kontakte mittels Internet zwischen Täter und Opfer lediglich der eigentlichen Tat vorgelagert sind, wird die Sonderkennung „Tatmittel Internet“ nicht verwendet.[9]

Im Jahr 2012 wurden insgesamt 54.339 Straftaten (2011: 47.992 und 2010: 48.411 Straftaten) unter der Sonderkennung „Tatmittel Internet“ erfasst. Das sind 3,6 % der Gesamtkriminalität. Mit einer Differenz von 6.347 Straftaten ist eine Zunahme von 13,2 % zu verzeichnen.

Bemerkenswert ist zudem die hohe Anzahl (2.731 = 48,5 %) von Erpressungsfällen mit der Sonderkennung „Tatmittel Internet“. Die Täter setzen dabei neben Ransomware auch DDoS-Angriffe (vgl. 3.4) ein.

[8] Mögliche Folgeschäden und Verwertungshandlungen werden jedoch bei den Straftatbeständen für diese Handlungen (z. B. Betrug) erfasst.

[9] Quelle: RdErl. IM NRW vom 01.01.2003 – 42 – 6410 „Richtlinien für die Führung der Polizeilichen Kriminalstatistik“, (SMBl. NRW. 293) i. d. F. vom 01.01.2012

Kinderpornografie

Die Fallzahlen einzelner Delikte im Bereich der Kinderpornografie sind mitunter großen jährlichen Schwankungen unterworfen. Dies ist insbesondere auf den Abschluss von Umfangsverfahren mit einer Vielzahl von Einzeltaten zurückzuführen. Eine hohe Anzahl von Verbreitungshandlungen über das Internet findet dabei keinen Eingang in die Polizeiliche Kriminalstatistik. Straftaten mit ausländischem Tatort werden derzeit nicht in der Polizeilichen Kriminalstatistik erfasst. Die Anzahl der Fälle “Verbreitung von Kinderpornografie“ stieg von 562 im Jahr 2011 um 275 oder 48,9 % auf 837 Fälle im Jahr 2012. Der Rückgang der Aufklärungsquote von 64,2 % auf 49,1 % ist nicht plausibel zu erklären. Diese Entwicklung gilt es weiter zu beobachten. Die Anzahl der Fälle von Besitz oder Verschaffung von Kinderpornografie nahm von 737 erfassten Fällen im Jahr 2011 um 218 Fälle oder 29,6 % auf 519 Fälle ab. 90,4 % dieser Fälle konnten aufgeklärt werden. Darüber hinaus weist die Polizeiliche Kriminalstatistik 18 Fälle von gewerbs- bzw. bandenmäßiger Verbreitung von Kinderpornografie aus. Dies entspricht dem Mittelwert der letzten Jahre.

Die Tatverdächtigen in diesem Deliktsbereich sind - wie in den Vorjahren - fast ausschließlich männlich (97,3 %). Nichtdeutsche Tatverdächtige sind mit einem Anteil von 3,6 % im Vergleich zum Bevölkerungsanteil regelmäßig unterdurchschnittlich beteiligt. Die Verbreitung pornografischer Erzeugnisse wurde mit 1.780 (2011: 1.800) erfassten Delikten im Jahr 2012 in 78,9 % der Fälle über das Internet verwirklicht. Besitz und Verschaffen von Kinderpornografie wurde in 400 Fällen oder zu 77,1 % über das Internet verwirklicht; bei der Verbreitung von Kinderpornografie waren es 723 Fälle (86,4 %). Das Internet stellt damit das maßgebliche Verbreitungsmedium dar.

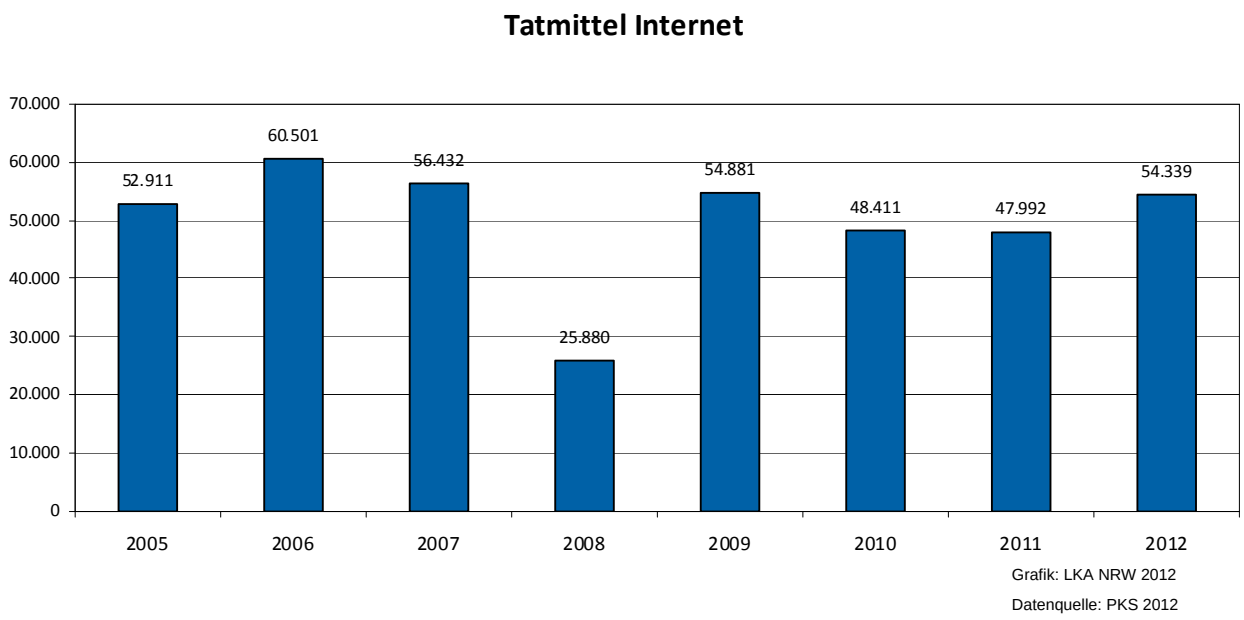


Diagramm 5: Entwicklung der Fallzahlen bei Delikten mit Sonderkennung „Tatmittel Internet“

2 Ermittlungshemmnisse

Die sinkende Aufklärungsquote der Cybercrime im engeren Sinne lässt sich mit den in der Polizeilichen Kriminalstatistik erfassten Daten nur unvollständig mit einer weitgehend korrelierenden Entwicklung der steigenden Fallzahlen erklären (vgl. 1.4). Obwohl die Polizei NRW seit Jahren die personellen und sächlichen Ressourcen stetig erhöht hat und ein als vorbildlich geltendes Fortbildungswesen betreibt, sinken die Aufklärungsquoten. Die Ursachen hierfür erscheinen vielfältig und werden nachfolgend beleuchtet.

2.1 Mindestdatenspeicherfrist

Die fehlenden Mindestdatenspeicherfristen von Internetverkehrsdaten und die daraus resultierenden Ermittlungshemmnisse tragen auch weiterhin maßgeblich zur negativen Entwicklung der Aufklärungsquote bei. Während die relevanten Daten von einigen Unternehmen für wenige Tage gespeichert werden, wird von anderen auf die Speicherung völlig verzichtet. Da elektronische Kommunikationsmittel in annähernd sämtlichen Bereichen der Cybercrime eingesetzt werden, stehen die für die Ermittlungen erforderlichen Daten als oftmals einzige Ermittlungsansätze in vielen Fällen nicht zur Verfügung.

Die Geschädigten bemerken den finanziellen Schaden meist erst nach einer Rechnungsstellung oder Prüfung von Kontoübersichten. Dies führt dazu, dass die Ermittlungen auf Grund fehlender Speicherfristen ergebnislos verlaufen.

2.2 Fortentwicklung des materiellen Rechts

Die Straftatbestände der Cybercrime im engeren Sinne und die darin enthaltenen Strafrahmen werden der veränderten Sozialschädlichkeit bestimmter Phänomene nur noch bedingt gerecht. Durch DDoS-Angriffe auf international agierende Konzerne waren z. B. über mehrere Tage die gesamte Kommunikation und deren Online-Abrechnungssystem weltweit betroffen. Es wurden enorme Schäden und Umsatzeinbußen verursacht. Bei den einschlägigen Straftatbeständen handelt es sich jedoch um Antragsdelikte mit Strafandrohungen, die einen Täter auch bei einer einfachen Sachbeschädigung erwarten würden. Da es keine Qualifikationen der Cybercrimedelikte im engeren Sinne gibt (vergleichbar der gemeinschädlichen Sachbeschädigung), welche in einem besonders schweren Fall zu einer erhöhten Strafandrohung führen würden, bleibt der Strafrahmen oft hinter dem Unrechtsgehalt zurück und die strafprozessualen Instrumentarien der §§ 100a ff. StPO werden nicht eröffnet[10]. Dies wirkt sich unmittelbar negativ auch auf die Chancen aus, Ermittlungsverfahren von besonderer Bedeutung erfolgreich abzuschließen.

[10] Vgl. *Ulrich Sieber*, Gutachten C zum 69. Deutschen Juristentag, 2012, C.H.Beck-Verlag, C 43

Marco Gercke

„Das materielle Strafrecht weist trotz mehrerer Gesetzesreformen im Hinblick auf die Internetkriminalität weiterhin erhebliche Gesetzeslücken auf. Dabei handelt es sich nicht um eine bewusste Entkriminalisierung durch den Gesetzgeber, sondern vorrangig um Regelungslücken, die durch geänderte technische Rahmenbedingungen oder Entwicklungsprozesse entstanden sind. Während beispielsweise unstreitig ist, dass das Herunterladen von kinderpornographischen Filmen und Videos strafbar ist, bereitet die Anwendung des Pornographiestrafrechts auf so genannte streaming-Dienste ganz erhebliche Probleme. Viele typische Internetdelikte, wie beispielsweise der Identitätsdiebstahl oder die Vervielfältigung und Entwendung von Daten durch Insider, sind seit Jahren Gegenstand wissenschaftlicher Diskussion, aber vom deutschen Strafrecht nur in Ansätzen erfasst. Während Deutschland in den 80er Jahren mit der Integration von Delikten zur Erfassung der Cybercrime im StGB eine weltweit führende Rolle einnahm und zum Modell für andere Länder wurde, stellt sich die Situation heute anders dar. Aufgrund unterbliebener Reformen und einer Fokussierung auf die zwölf Jahre alte Cybercrime Konvention des Europarates bleibt die Gesetzgebung in Deutschland heute bisweilen deutlich hinter den Standards einiger Entwicklungsländer zurück. Das gilt nicht nur im Bereich des materiellen Strafrechts, sondern auch wenn es um den Schutz grundlegender Freiheitsrechte im Internet geht."

Prof. Dr. Marco Gercke, Direktor des Cybercrime Research Institute mit Sitz in Köln.

2.3 Internationalisierung

Trotz der weltumspannenden Funktionsweise des Internets war in zurück liegender Zeit eine zumindest am jeweiligen Sprachraum, oft an den nationalen Grenzen orientierte Präferenz im Hinblick auf die Zielsysteme der Cyberkriminellen zu beobachten: Deutsche Hacker griffen meist auch deutsche Server an. Zwischenzeitlich haben insbesondere organisierte Tätergruppierungen mit kommerziellen Zielen sowie Online-Communities (z. B. Anonymous) diese Perseveranz aufgegeben. Zudem nutzen viele Täter Anonymisierungsmethoden, die auf der Weiterleitung über im Ausland befindliche Server basieren. Damit führen Ermittlungen immer häufiger und schneller zu Spuren, die nur noch im Ausland weiter verfolgt werden können. Der weitere Erfolg hängt dann von vielen Faktoren ab. In einigen Fällen können die erforderlichen Daten internationaler Konzerne von ausländischen Niederlassungen rechtmäßig auch ins Inland übermittelt werden, wo ein Zugriff mittels eines deutschen richterlichen Beschlusses möglich ist. In anderen Fällen bleibt lediglich der Weg über polizeiliche oder justizielle Rechtshilfeersuchen. Die Erfolgsaussichten richten sich dann nicht nur nach den jeweiligen Rechtshilfeabkommen, sondern auch nach der Leistungsfähigkeit und -willigkeit der dortigen Ermittlungsbehörden. Die Ermittlungschancen erhöhen sich gelegentlich sogar durch eine solche Konstellation, nämlich dann, wenn Rechtshilfeabkommen existieren und organisatorisch schnell und kompetent umgesetzt werden. Dann profitieren deutsche Ermittlungsbehörden von der in nahezu allen Staaten geregelten Speicherung so genannter Vorratsdaten, während umgekehrt Rechtshilfeersuchen an deutsche Ermittlungsbehörden wegen der zu kurzen oder nicht vorhandenen Speicherung von Verbindungsdaten ins Leere laufen. In vielen Ermittlungsverfahren werden Rechtshilfeersuchen jedoch nicht oder zu spät beantwortet oder Rechtshilfeabkommen bestehen nicht.

Marco Gercke

"Internetkriminalität hat in vielen Fällen eine transnationale Dimension. Die Bekämpfung setzt dabei grundsätzlich eine enge Zusammenarbeit von Strafverfolgungsbehörden über die Landesgrenzen hinaus voraus. Deutschland setzt zur Verbesserung der Zusammenarbeit der Strafverfolgungsbehörden auf die Cybercrime Konvention des Europarates. Diese enthält zahlreiche Normen, die mit dem Ziel eingeführt wurden, die grenzüberschreitende Zusammenarbeit zu verbessern. Zwölf Jahre nach der Unterzeichnung der Konvention durch Deutschland ist aber Ernüchterung eingetreten. Die Instrumente der Konvention werden nach eigenen Untersuchungen des Europarates selbst von den Mitgliedstaaten teilweise kaum genutzt. Darüber hinaus liegt die Zahl der Staaten, die die Konvention ratifiziert haben und mit denen Deutschland bei transnationalen Internetstraftaten beschleunigt zusammenarbeiten könnte, bei gerade einmal 38. Nur drei Nichtmitglieder des Europarates (USA, Japan und Australien) haben die Konvention ratifiziert. Die Länder, mit denen eine einfachere Kooperation hilfreich wäre, wie China, die Länder der Lateinamerikas, Zentralafrika oder Südasiens wurden vom Europarat weder eingeladen, an der Verhandlung der Konvention teilzunehmen, noch sind sie der Konvention beigetreten. Im Interesse der Strafverfolgungsbehörden und unter Berücksichtigung ihrer Bedürfnisse wäre es wünschenswert, dass sich Deutschland stärker für einen internationalen Lösungsansatz zur Verbesserung der internationalen Zusammenarbeit – beispielsweise unter dem Dach der Vereinten Nationen in einer der UN Konvention zur Bekämpfung transnationaler organisierter Kriminalität (UNTOC) vergleichbaren Form – einsetzt."

Prof. Dr. Marco Gercke, Direktor des Cybercrime Research Institute mit Sitz in Köln.

2.4 Anonymisierungspotenziale

Den im Internet agierenden Tätern ist häufig bewusst, dass sie über ihre IP-Adresse identifiziert werden können. Um dies zu vermeiden, nutzen sie verschiedene Möglichkeiten der Anonymisierung, beispielsweise durch Umleitung des Datenverkehrs über zwischengeschaltete Server[11]. Anbieter so genannter VPN-Dienste[12] werben damit, die Datenübertragung zwischen dem Computer des Benutzers und dem jeweiligen Ziel im Internet verschlüsselt über ihre im Ausland befindlichen Server umzuleiten und keine eigene Protokollierung vorzunehmen.

Eine darüber hinaus häufig genutzte Form der Anonymisierung erfolgt über das TOR-Netzwerk[13]. Dieser kostenlose Dienst besteht aus einer Vielzahl von weltweit verteilten Servern, über die die Datenpakete geleitet werden. Beim Verbindungsaufbau wird durch das Programm eine zufällige Route über einen Teil dieser Server festgelegt. Die Server führen keine Protokollierung über Herkunft oder Ziel der Daten. Die Notwendigkeit des TOR-Projekts wird mit der Möglichkeit begründet, unabhängig von Zensur oder politischer Verfolgung über etwaige Missstände berichten zu können. Als weiterer Grund für die Nutzung wird die durch TOR erhöhte Privatsphäre, zum Schutz vor der Analyse des Surfverhaltens der Nutzer durch Firmen oder den Staat, angegeben. Ein nicht unwesentlicher Anteil liegt jedoch nach kriminalpolizeilicher

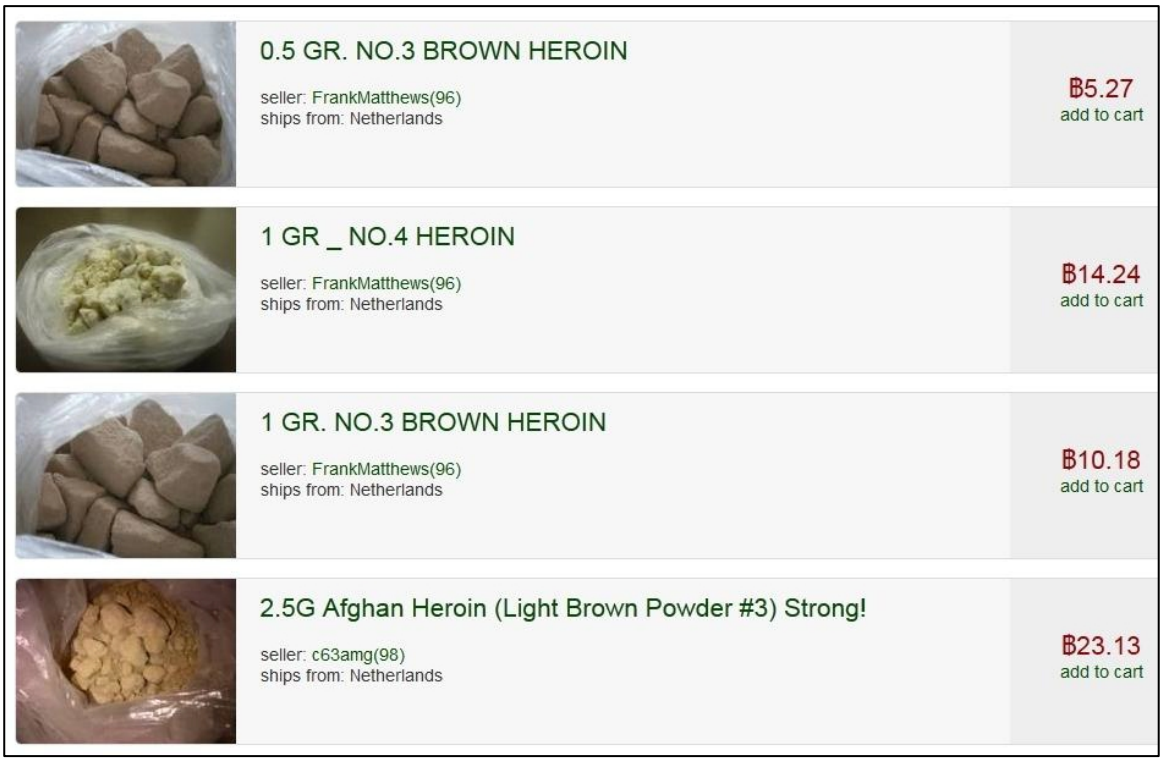
[11] z. B. Proxy-Server

[12] VPN = Virtual Private Network

[13] TOR = The Onion Router, mehrschichtiges Servernetzwerk

Erfahrung in der Nutzung des Netzwerks für kriminelle Zwecke. Über das TOR-Netzwerk erfolgt z. B. der Zugang zu dem so genannten Darknet[14]. Das Darknet bietet Kriminellen die Möglichkeit, innerhalb anonymer Serverstrukturen wie des TOR-Netzwerks Internetseiten zu betreiben, deren Inhalte angezeigt, deren tatsächlicher Standort jedoch nicht über die IP-Adresse ermittelt werden kann. Diese Möglichkeit nutzen Kriminelle, um z. B. illegalen Handel mit Drogen zu betreiben oder für die Verbreitung kinderpornografischen Materials. Dies führt dazu, dass die polizeilichen Ermittlungen nicht oder nur mit einem erheblich höheren Aufwand durchgeführt werden können.

Beispiel aus einem Darknet-Webshop für den Handel mit Drogen:



Quelle: G Data Software AG

2.5 Innovationen und zunehmende technische Komplexität

BigData

Unter Big Data versteht man vielfältige und unterschiedlich strukturierte Informationen, verbunden mit den Methoden und Technologien, diese umfangreichen Massendaten wirtschaftlich sinnvoll zu gewinnen und zu nutzen. Die wirtschaftliche Vernetzung von Unternehmen und die mobile soziale Vernetzung steigen zunehmend. Die hierbei exponentiell ansteigende Datenmenge[15] ist nicht nur ein Problem für die Internetwirtschaft sondern auch für Ermittlungsbehörden. Zur schieren Datenmenge kommt die ungleichartige Beschaffenheit (Heterogenität) dieser Daten hinzu. Dabei ist die für erfolgreiche Ermittlungen notwendige

[14] Darknet oder Hidden Services = versteckte Subnetze des Internet, die die Identität des Nutzers verbergen

[15] Bericht der IEEE 802.3 Ethernet Working Group

http://www.ieee802.org/3/ad_hoc/bwa/BWA_Report.pdf , Seite 8 vom 19.07.2012, abgerufen am 25.03.2013

Feststellung und Filterung der Daten sowie die Normalisierung und Auswertung durch eine rein personelle oder materielle Aufrüstung der Polizei kaum mehr zu bewältigen. Nur neue, innovative Analysemethoden werden die kriminalistische IuK-Forensik auch zukünftig ermöglichen (vgl. 4.1).

Implikationen von IPv6 für Ermittlungsbehörden

Bei IPv6 handelt es sich um die Weiterentwicklung des derzeitigen Übertragungsstandards IPv4, welcher in Rechnernetzen und somit auch im Internet verwendet wird. Mit dem neuen Standard steht ein deutlich größerer IP-Adressraum als bisher zur Verfügung. Im Jahr 2012 wurde damit begonnen, den neuen Standard einzuführen. Die Polizei muss sich seitdem auf die neue Technologie einstellen.

Alexander Bluhm

Implikationen von IPv6 für Ermittlungsbehörden

"Durch die Einführung von IPv6 wird die Ermittlungstätigkeit der Polizei erschwert. Während des Übergangs von IPv4 zu IPv6 müssen immer beide Übertragungswege untersucht werden. Kriminelle können sich das bereits heute zunutze machen. Während der Migrationsphase werden die beiden Protokolle übereinander getunnelt. Das versperrt den Blick auf die tatsächlichen Kommunikationsbeziehungen. Durch Tunnelverfahren wie Teredo kann dies auch vom Nutzer unbemerkt geschehen. Die IPv6 Privacy-Extensions und dynamische Praefixe, welche zur Wahrung der Privatsphäre der Nutzer eingeführt wurden, erzeugen die gleichen Schwierigkeiten bei der Ermittlung der Täter wie heutzutage dynamische IPv4 Adressen. Die Abfrage der Inhaber von Adressbereichen mittels whois funktioniert bei IPv4 und IPv6 gleich.

Durch den Wegfall von NAT (Network-Address-Translation) wird das Identifizieren von Endgeräten einfacher. Einige Nutzer fordern allerdings die Einführung von NAT auch bei IPv6 aus falsch verstandenen Sicherheitsbedenken. Das Internet wird sich dahingehend verändern, dass viel mehr Geräte global routebare Adressen bekommen. Das können persönliche Computer, eingebettete Systeme oder Steuerungsanlagen sein. Das eröffnet Kriminellen viele neue Möglichkeiten."

Dip.-Math. Alexander Bluhm, Product Owner genugate, genua Gesellschaft für Netzwerk und Unix-Administration mbh, Kirchheim bei München, Mitglied des BITKOM

IP-Sharing, Port Address Translation (PAT)

Ein Problem der Identifizierbarkeit tritt gegebenenfalls bei der mobilen Internetnutzung auf. Hier wird die Mehrfachnutzung einer einzelnen IP-Adresse durch die Nutzung unterschiedlicher Ports geregelt. Bis zu 40.000 Mobilgeräte können zeitgleich über eine einzige IP-Adresse eine Internetverbindung herstellen.
Eine gesetzliche Pflicht im Telekommunikationsgesetz (TKG) zur Erfassung der Ports besteht nicht. Eine eindeutige Identifizierung ist ohne Port-Angabe nicht möglich. Hinzu kommt noch, dass Provider aufgrund von nicht ausreichenden IP-Kontingenten auf Zweit- oder Drittanbieter zurückgreifen. Die dadurch entstehenden Verzögerungen können die Ermittlungserfolge wesentlich erschweren.

IP-basierte Sprachkommunikation und andere Kommunikationsprogramme

Michael Bartsch

IP-basierte Sprachkommunikation und andere Kommunikationsprogramme

"Telekommunikation ist heute nicht mehr alleine das Telefonieren im klassischen Sinne. Durch das Internet und neue Applikationen findet Telekommunikation auf unterschiedlichen Kanälen statt. WhatsApp, GoogleTalk, Skype, ICQ, Facebook und Co., um nur einige zu nennen, stellen die Telekommunikationsinfrastruktur zur Verfügung, die benötigt wird, um immer und überall erreichbar zu sein und das auf allen erdenklichen Endgeräten wie Telefonen, Smartphones, Spielkonsolen, Tablets und Pads und Computern. Voice-Over-IP ist der Oberbegriff für alle möglichen Arten, Sprache zu übertragen. Dabei spielt die Privatsphäre eine immer größere Rolle. Die Frage nach der „Sicherheit“ von solchen Systemen fordert von den Anbietern und Herstellern immer bessere Sicherheitsmechanismen. Die Verschlüsselung der Daten und der Gespräche ist hierbei die wichtigste Sicherheitseigenschaft. Für die Polizeiarbeit wird es dadurch immer schwieriger, heraus zu finden, welche Kommunikationsart stattfindet, und durch die Verschlüsselung ist Telekommunikationsüberwachung nicht in Echtzeit oder gar nicht durchführbar."

Michael Bartsch, Leiter BITKOM Arbeitskreis Öffentliche Sicherheit, T-Systems International GmbH

2.6 Ubiquität des Internets und steigende Qualitätsanforderungen

In nahezu allen Bevölkerungsschichten ist die Nutzung des Internets zum selbstverständlichen Bestandteil des Alltags geworden. Die Miniaturisierung der erforderlichen Geräte fördert diese Entwicklung noch. Potenzielle Opfer wie Täter führen jederzeit komplexe IT-Systeme im Westentaschenformat mit sich und nutzen diese. Daher wird das Internet nicht nur immer häufiger unmittelbar zur Begehung von Straftaten genutzt, sondern die damit verbundenen Kommunikationsabläufe bilden zunehmend auch wichtige Ermittlungsansätze in allen klassischen Kriminalitätsphänomenen ab, vom Betrug bis zum Tötungsdelikt. Dies führt dazu, dass die Ermittlungskräfte in diesen Bereichen technische Ermittlungsmaßnahmen durchführen oder initiieren müssen, die noch vor wenigen Jahren ausschließlich den hoch spezialisierten Cyberkriminalisten und Kräften der IuK-Ermittlungsunterstützung vorbehalten waren. Auch die Anforderungen an diese Spezialisten steigen durch die beschriebene Entwicklung qualitativ und quantitativ stetig an. Sie leisten zudem mit einem wesentlichen Anteil der zur Verfügung stehenden Arbeitszeit auch ermittlungsunterstützende Hilfe in anderen, teilweise hoch priorisierten Kriminalitätsbereichen, wie z. B. bei Produkterpressungen. Eine weitere Folge dieser Entwicklung ist, dass der Fortbildungs-, Informations- und der Vernetzungsbedarf der Spezialisten in den letzten Jahren enorm gestiegen sind.

3 Darstellung und Bewertung ausgewählter Phänomene

3.1 Identitätsdiebstahl/Phishing

Der Identitätsdiebstahl umfasst die unrechtmäßige Erlangung und den Einsatz der erlangten Daten, um damit rechtswidrige Aktivitäten über das Internet durchzuführen. Datenerlangung und Verwertung erfolgen über Phänomene wie beispielweise Phishing und Carding.

Der Identitätsdiebstahl bildet bei den Fallzahlen der Cybercrimedelikte den Schwerpunkt (11.500 Fälle). Die Auswertung der Datensätze des polizeilichen Vorgangsbearbeitungssystems weist eine Gesamtzahl von 4.966 Phishing-Fällen aus. Das Ziel der Täter ist das Erlangen von Zugangsdaten, beispielsweise für Online-Banking, Web-Shops und Packstationen. Einen erheblichen Anteil daran (2.071 Fälle) haben auch so genannte Carding[16]-Fälle als Verwertungstat. Die hieraus erlangten Daten werden vielfach zur illegalen Zahlungsabwicklung verwendet. Für die Opfer entstehen daraus erhebliche Nachteile, z. B. Inkassoforderungen, Mahnschreiben von Händlern und Rechtsanwaltskanzleien.

Um Zugangsdaten zu erlangen, bringen die Täter Schadsoftware auf den jeweiligen Nutzer-PC auf, wodurch Zugangsdaten ohne die Mitwirkung des Nutzers abgefangen werden können. Diese Daten werden durch „man-in-the-middle“[17] oder „man-in-the-browser“[18]-Angriffe innerhalb von Transaktionsvorgängen derart manipuliert, dass schließlich Geldbeträge unbemerkt auf Täterkonten umgeleitet werden können. Darüber hinaus nutzen Täter manipulierte Webseiten und verfälschte E-Mails, um Opfer zur Preisgabe ihrer persönlichen Daten zu bewegen. Als Reaktion auf die Verbesserung der technischen Sicherheitsstandards (insbesondere beim Online-Banking) setzen die Täter Social Engineering[19] ein.

Firmen haben sich auf diese Entwicklungen eingestellt und mit häufigeren Aktualisierungen ihrer Anwendungen sowie dem Anbieten von Patches zur Behebung von Sicherheitslücken reagiert. Bei Online-Dienstleistungen, insbesondere Online-Banking, wurde die Sicherheit durch neuere TAN-Verfahren, so genannte Multifaktorielle Authentifizierungsverfahren, verbessert. Die dabei angewandte Kanaltrennung führt zu einer deutlichen Verbesserung der Sicherheit im Online-Banking.

Fallbeispiel Identitätsdiebstahl

Über Facebook erhielt der Geschädigte eine Nachricht von einem vermeintlich befreundeten Mitglied. In dieser Nachricht wurde er gebeten, seine Mobilfunknummer zu übermitteln. Die anschließend auf dem Mobiltelefon des Geschädigten per SMS eingehenden Codes sollten an das vermeintlich befreundete Facebook-Mitglied weitergeleitet werden. Der Geschädigte leitete die Codes arglos weiter, ohne zu bemerken, dass es sich bei den Codes um TAN-Nummern eines SMS-Bezahldienstes handelte. Die nächste Mobilfunkrechnung des Geschädigten enthielt die dadurch entstandenen Kosten des SMS-Bezahldienstes. Ermittlungen ergaben, dass nicht die befreundete Person selbst die Nachrichten geschickt hatte. Vielmehr war der Facebook-Account des befreundeten Mitglieds durch einen unbekannten Täter gehackt worden. Der Täter nutzte die Facebook-Identität, um damit das Opfer zu täuschen.

[16] Missbräuchliche Einsatz von illegal erlangten Kreditkartendaten im Internet

[17] Bei dieser Angriffsform sitzt der Angreifer zwischen zwei Kommunikationsendpunkten und kann den Datenverkehr manipulieren.

[18] Hier werden Manipulationen von Darstellungen und Transaktionen direkt im Webbrowser vorgenommen.

[19] Einflussnahme auf Personen, um diese zu einer Handlung, beispielsweise zur Preisgabe vertraulicher Informationen oder Öffnen eines E-Mail-Anhangs, zu veranlassen.

Im Jahr 2012 konnten neue Varianten des Phishing festgestellt werden:

Bei einem als „Spear-Phishing“ (engl. Speer – gezielter Angriff) bezeichneten Angriff verschaffen sich Täter zielgerichtet interne Informationen einer Organisation oder eines Unternehmens. Für die Täter sind insbesondere E-Mail-Adressen und organisations- oder geschäftsrelevante Informationen von Interesse. Die Zielpersonen werden unter Verwendung dieser Informationen vor einem augenscheinlich authentischen Hintergrund kontaktiert und veranlasst, sensible Daten preiszugeben oder Schadsoftware zu installieren. Eine Variante des Spear-Phishing ist das „Whaling“, bei dem die Täter gezielt Führungskräfte und Entscheidungsträger eines Unternehmens angehen. Dabei ist der Aufwand für vertrauenschaffende Maßnahmen, z. B. Beschaffung entsprechender Firmeninterna wie Organisations- und Personalstruktur mit dem jeweiligen Verantwortungsbereich, hoch.

Dr. Elmar

Gerhardts-Padilla

„Auch 2012 war wieder ein Anstieg beim Gesamtaufkommen von Schadsoftware und der Zahl neuer, eindeutiger Schadsoftwareexemplare zu beobachten. Es existieren mittlerweile diverse Schadsoftwarevarianten, die Kriminelle bei Informations- und Identitätsdiebstahl unterstützen. Dabei kommen Methoden wie Webinjects, Ändern von DNS–Einträgen, Keylogger oder Webcam aktivieren zum Einsatz. Über Webinjects ist es Kriminellen möglich, eigenen Code in die Darstellung legitimer Webseiten zu injizieren. So kann z. B. bei Anzeige einer legitimen Webseite ein zusätzliches Pop-up mit der Aufforderung zur Eingabe von persönlichen Daten auf dem infizierten Rechner geöffnet werden. Das Ändern von DNS–Einträgen ist eine andere Möglichkeit, Informationsdiebstahl zu unterstützen. Dabei werden die lokalen DNS–Einstellungen auf einem Rechner geändert. Dadurch können Nutzer gezielt auf bösartige DNS–Server umgelenkt werden. Keylogger sind eine weitere Möglichkeit für Informationsdiebstahl. Dies sind Programme, die Tastatureingaben mitprotokollieren. Dadurch können Kriminelle vertrauliche Daten wie z. B. Logins und Passwörter ausspionieren. Auch Webcams können zur Spionage eingesetzt werden. Einige Schadsoftware bietet die Funktionalität, an Rechner angeschlossene oder in Rechner eingebaute Webcams zu aktivieren. Die aufgenommenen Bilder können dann von Kriminellen mittels der Schadsoftware extrahiert werden.“

Dr. Elmar Gerhards-Padilla, Leiter Schadsoftwareanalyse/-bekämpfung, Fraunhofer FKIE

Der Gesamtschaden aus den Phänomenen Phishing beim Online-Banking und Carding beträgt für NRW im Jahr 2012 nach Auswertung der Daten aus dem polizeilichen Vorgangsbearbeitungssystem ca. 5.500.000 Euro.

Fallbeispiel Phishing

Die Geschädigte erhielt beim Online-Banking über ein Popup-Fenster die Nachricht, dass aus Sicherheitsgründen dort eine TAN eingegeben werden müsse. Nachdem sie dies getan hatte, wurde mittels Echtzeittrojaner im Hintergrund eine Auslandsüberweisung durchgeführt. Der Schaden betrug 2.600 Euro.

3.2 Carding

Durch Phishing, insbesondere über Schadsoftware oder gezielte Angriffe auf Firmendatenbanken, gelangen Kreditkartendaten in die Hände von Kriminellen. In der Regel nutzen diese die Daten nicht selbst, sondern veräußern die Kreditkartendaten in eCrime-Foren[20]. Der Preis je Datensatz wird abhängig von der Deckungssumme der Kreditkarte festgesetzt und beginnt schon bei wenigen Euro. Die Käufer nutzen die Kreditkartendaten zum Erwerb von Waren über Onlineshops oder Internet-Auktionshäuser. Um anonym zu bleiben, nutzen die Täter für den Empfang der Waren Packstationen, leer stehende Wohnungen oder werben Helfer als Paketagenten an. Die Waren werden für den Eigengebrauch verwendet oder weiterveräußert. Der im polizeilichen Vorgangsbearbeitungssystem registrierte Schaden betrug im Jahr 2012 für die 2.071 in der Recherchedatenbank identifizierten Fälle über 1.000.000 Euro.

3.3 Ransomware

Unter dem Begriff „Ransomware“ wird eine Vielzahl von Schadprogrammen erfasst, die Computersysteme sperren oder Daten verschlüsseln und die Nutzer wegen vermeintlich illegaler Aktivitäten über ein Popup-Fenster zur Zahlung eines Lösegeldes (engl. ransom) über elektronische Zahlungssysteme auffordern. Während anfänglich der deutschsprachige Raum das primäre Ziel dieser Kriminalitätsform war, sind inzwischen auch der gesamte europäische Raum und die USA betroffen. Die klassischen Varianten erwecken den Anschein, von einer Behörde (BKA, Bundespolizei) zu stammen und den Computer wegen des Besitzes von kinderpornografischem Material, wegen illegaler Downloads oder eines Verstoßes gegen Lizenz- und Urheberrechte zu sperren. Es existieren zahlreiche Abwandlungen. Einige Varianten geben vor, den Facebook-Account zu blockieren, sofern nicht 20 Euro überwiesen würden.

Die Schadprogramme werden über massenhaft versandte E-Mails im Dateianhang und manipulierte Webseiten verbreitet. Mit Schadcode versehene Werbebanner, die auf vielen bekannten und vertrauenswürdigen Webseiten eingeblendet werden, können ohne Wissen des Seitenbetreibers durch so genannte Drive-By-Downloads[21] Computersysteme kompromittieren. Das polizeiliche Vorgangsbearbeitungssystem verzeichnet hierzu insgesamt 8.170 Fälle.

Wie in vielen anderen Phänomenen im Bereich Cybercrime machen sich die Cyberkriminellen auch bei der Ransomware Techniken des Social-Engineering zunutze. Die Opfer werden gezielt unter Druck gesetzt und so zu einer Zahlung veranlasst. So ist der im Popup-Fenster aufgeführte Vorwurf mittlerweile nicht mehr zufällig gewählt, sondern steht im Kontext zu den vom Internetnutzer zuvor aufgerufenen Webseiten. Bei einem infizierten System erscheint nach dem Besuch von Webseiten mit pornografischen Inhalten der Hinweis, der Computer sei im Zusammenhang mit Kinderpornografie aufgefallen. Auch die eingeblendeten Texte und Behördenlogos werden nach einer Geolokalisierung über die IP-Adresse des Internetanschlusses an das jeweilige Land angepasst.

[20] Nichtöffentliche Internetforen, in denen Handel mit Kreditkartendaten, Schadsoftware, Zugangsdaten zu E-Commerce-Dienstleistern und Drogen betrieben wird.

[21] auch: Drive-by-Infection – Schadsoftware gelangt beim Surfen unbemerkt und ohne Zutun des Nutzers auf den Computer

Candid Wuest

„Erpressungstrojaner haben auch in 2012 weiter stark zugenommen. Einzelne Angreifer infizieren mehr als 25.000 Computer von Privatpersonen täglich mit solcher Malware. Ermittlungen haben gezeigt, dass ca. 2,9% der Opfer bezahlen, was einzelnen Gruppen Einnahmen von bis zu 300.000 Euro pro Monat beschert. Der Rechner wird natürlich nur in den seltensten Fällen frei geschaltet, so dass einige Opfer sogar mehrfach bezahlen. Weil derartige Angriffe so rentabel und einfach durchzuführen sind, erwarten wir, dass auch in 2013 die Erpressungstrojaner-Vorfälle weiter steigen werden."

Candid Wuest, Symantec Deutschland GmbH, Mitglied des BITKOM

3.4 DDoS-Angriffe

„We were attacking your website in the last days. We will continue to take your site down in the next weeks, if you don't pay 10.000 $..."

Wortlaut eines Erpresserschreibens nach einem DDoS-Angriff

Bei DDos-Angriffen werden IT-Infrastrukturen von Unternehmen mittels gezielter Massenabfragen so belastet, dass diese für ihre ursprünglichen Aufgaben nicht mehr zur Verfügung stehen. Hackergruppen wie Anonymous nutzen dies zur Durchsetzung ihrer ideologischen Ziele[22]. Gewinnorientierte Kriminelle nutzen darüber hinaus DDoS-Angriffe für Erpressungen. Für die Beendigung der Angriffe forderten die Täter bis zu 10.000 US Dollar. Die durch den DDoS-Angriff unmittelbar verursachten Schäden übertreffen die Täterforderungen häufig um ein Vielfaches. Ein geschädigtes Unternehmen der Mobilfunkbranche bezifferte den durch einen zwei Tage andauernden DDoS-Angriff verursachten Schaden auf 300.000 bis 500.000 Euro. Die Angriffe werden über ein Netz von mit Schadsoftware infizierten Rechnern (Bot-Netze, vgl. 6.1) durchgeführt. Kriminelle können Bot-Netze ohne großen Aufwand in eCrime-Foren bedarfsgerecht buchen und nutzen, ohne über eigene Infrastruktur oder besondere Kenntnisse verfügen zu müssen. Dabei können sie bei Bedarf auf eine rund um die Uhr erreichbare Service-Hotline in Landessprache zurückgreifen.

3.5 Smartphones - neue Risiken

Mit zunehmender Verbreitung von Smartphones und entsprechenden Angeboten an Applikationen (Apps) in den virtuellen Märkten haben auch die Einsatzmöglichkeiten stetig zugenommen. Über spezielle Applikationen und eigene Webbrowser können Online-Banking, E-Commerce-Transaktionen (z. B. eBay, Amazon) und Aktivitäten in Sozialen Netzwerken über die mobilen Endgeräte abgewickelt werden. Die erforderlichen Zugangsdaten zu diesen Diensten und Zahlungssystemen, aber auch andere sensible Nutzerdaten wie Fotos, Kontakte, E-Mails und GPS-Daten sind häufig auf den Geräten gespeichert und machen sie somit zum attraktiven Ziel von Cyberkriminellen.

Über manipulierte Applikationen, Webseiten und Dateien können Schadprogramme auf den Smartphones installiert und Daten abgegriffen werden. Darüber hinaus stehen die mobilen Mini-Computer den Kriminel-

[22] Beispiel: Anonymous' Angriffe auf Kommunikationskanäle und Webserver eines Konzerns

len nach der Installation des Schadcodes als Bestandteil großer Netzstrukturen (sog. Bot-Netzen) für eine Vielzahl von Einsatzmöglichkeiten (z. B. DDoS-Angriffe) zur Verfügung.

Neben den fremdverursachten Eingriffen in die Sicherheitsmechanismen von Smartphones gewinnt die Modifikation der unterschiedlichen Betriebssysteme durch die Nutzer selbst immer mehr an Bedeutung. Durch das so genannte jailbreaken oder rooten[23] werden bestehende Sicherheitslücken in der Gerätesoftware ausgenutzt, um die systemimmanenten Herstellerrestriktionen zu entfernen und den Zugriff auf das Dateisystem und die Installation von ungeprüfter Software zu ermöglichen. Durch diese Manipulation können gewöhnlich kostenpflichtige Applikationen und Programme unbekannter Quellen, welche auf den zahlreichen Warez[24]-Seiten zum kostenlosen Download angeboten werden und oftmals Schadcode enthalten, installiert werden. Der vermeintliche Zugewinn an Funktionalitäten des Gerätes geht mit unvermeidlichen Sicherheitsrisiken und oftmals dem Verlust persönlicher Daten einher.

Thomas Tschersich

„Beim mobilen Surfen zeigen sich viele Nutzer eher unbesorgt: Nur etwa die Hälfte führt regelmäßig Aktualisierungen des Betriebssystems durch und schließt damit bekannte Sicherheitslücken. Das zeigt eine Befragung, die die TNS-Infratest im Auftrag der Deutschen Telekom im vergangenen Jahr durchgeführt hat. Zu viele betrachten ihr Smartphone als ein einfaches Telefon und nicht als einen Hochleistungsrechner, was es tatsächlich ist. Die Telekom beobachtet die Gefahrenlage im Netz kontinuierlich und hat ein Frühwarnsystem aufgebaut. Dazu gehören 97 weltweit eingesetzte Locksysteme - so genannte Honeypots. Wir simulieren damit unter anderem auch leicht angreifbare Smartphones. Die Anzahl der Angriffe ist frappierend: Ein einzelnes Gerät wurde innerhalb eines Jahres über 100.000 mal attackiert; mehr als 330 dieser Angriffe waren erfolgreich, also fast jeden Tag einer. Mit den Honeypots können wir das Verhalten von Angreifern analysieren und neue Trends identifizieren. Unsere Erkenntnisse teilen wir dann beispielsweise mit den Herstellern von Schutzsoftware, so dass sie ihre Programme entsprechend anpassen können. Die Cyberkriminellen haben längst erkannt, dass Smartphones ein leichtes Ziel sind. Dabei geben sie sich noch nicht einmal besonders viel Mühe: Die Schadprogramme sind bisher keine anderen als für PC und Laptop. Für den Nutzer bedeutet das wiederum: Die meisten Angriffe lassen sich leicht verhindern beziehungsweise abwehren. Grundsätzlich sollten Nutzer darauf achten, ihr Smartphone über Updates auf dem aktuellen Stand zu halten. Einige Hersteller bieten zudem spezielle Sicherheitslösungen an. Vor allem für Geräte, die auf dem relativ offenen Betriebssystem Android basieren, sind zusätzliche Sicherheitsprodukte zu empfehlen. Und schließlich sollten Nutzer nur Apps herunterladen, die vertrauenswürdig sind. Dafür sollten sie auf die offiziellen Marktplätze zurückgreifen und sich die Beschreibungen und Bewertungen der Programme genau durchlesen, bevor sie sie installieren. Besonders gefährdet sind zudem Smartphones, bei denen die Nutzer die Betriebssoftware selbst modifizieren, etwa durch einen so genannten Jailbreak beim iPhone. Dieses Risiko sollten sicherheitsbewusste Nutzer nicht eingehen. Aber auch die Hersteller der Endgeräte müssen mehr Verantwortung für die Sicherheit ihrer Kunden übernehmen. Einige Hersteller sind bei Softwareupdates zu zögerlich, während beim PC umgehend Anpassungen erfolgen.“

Thomas Tschersich

Vorsitzender BITKOM LA Sicherheit; Leiter IT-Sicherheit Deutsche Telekom AG

[23] jailbreak/rooten = bezeichnet Entsperren von Computersoftware, um die eigenen Rechte und technischen Möglichkeiten zu erhöhen.

[24] Warez bezeichnet im Computerjargon illegal beschaffte oder verbreitete Software.

3.6 Skimming/PoS-Terminals

Das Kriminalitätsphänomen „Skimming“[25] wurde bereits im Lagebild „IuK-Kriminalität in NRW“ des Jahres 2011 dargestellt. Hinsichtlich der Manipulationen an Geldautomaten mittels so genannter Vorsatzgeräte hat sich der erstmalige Rückgang der Fallzahlen im Jahr 2011 (im Vergleich zum Höchststand in 2010) weiterhin fortgesetzt. Mit 212[26] identifizierten Skimming-Angriffen im Jahr 2012 gingen die Fallzahlen im Vergleich zum Vorjahr erneut merklich zurück. Die Entwicklung zeigt, dass die Sicherungsmaßnahmen der Kreditwirtschaft an Geldautomaten (z. B. Austausch veralteter Modelle) sowie die Veränderung der Sicherheitsarchitektur bei Zahlungskartenprodukten (z. B. flächendeckende EMV-Chip[27]-Prüfung in Europa) zunehmend greifen.

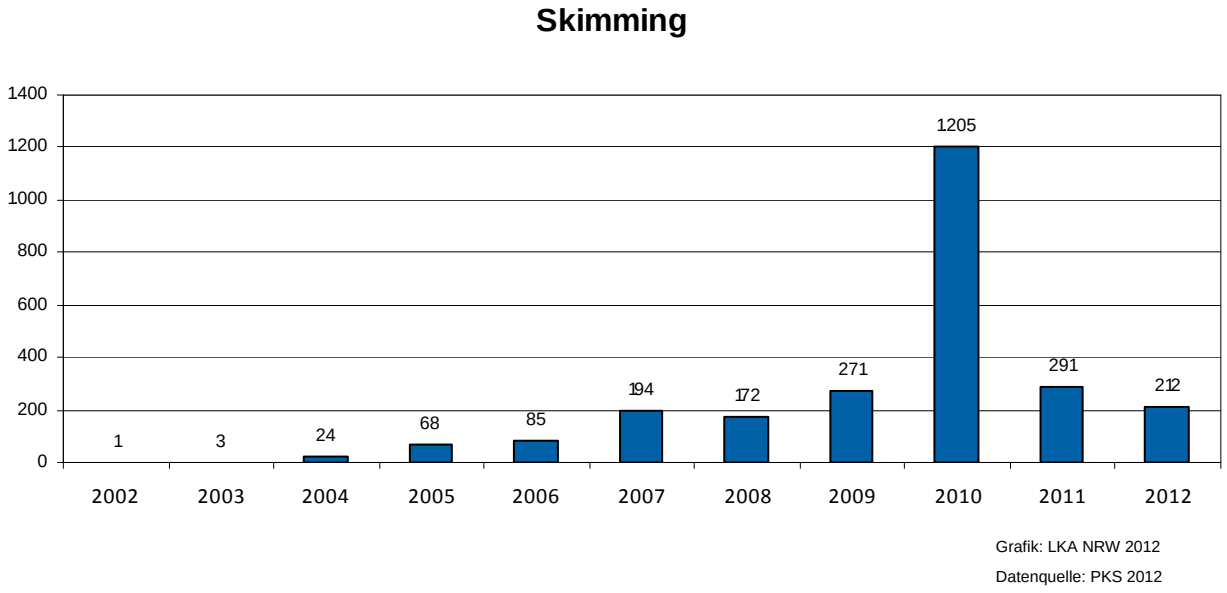


Diagramm 6: 10-Jahres-Entwicklung - Skimming an Geldautomaten in NRW

Die Cashing-Taten[28] konzentrierten sich - wie im Vorjahr - überwiegend auf Länder Süd-, Mittel- und Nordamerikas sowie den asiatischen Raum. Dort sind nach wie vor Zahlungskartentransaktionen unter Nutzung der Magnetstreifentechnologie möglich. Jedoch gewinnt auch dort die EMV-Chip-Technologie an Bedeutung und wird in immer mehr Ländern umgesetzt.

Bezüglich einer weiteren Verlagerung des „Skimming“ hin zu Zahlterminals hat sich die letztjährige Lagebildeinschätzung als zutreffend erwiesen. PoS-Terminals[29] des Handels haben sich dabei als Hauptangriffsziel herausgestellt. Fälle manipulierter Fahrscheinautomaten oder kundenbedienter Tankterminals wurden hingegen nicht registriert. Zur Manipulation von PoS-Terminals wurden bevorzugt Geschäfte mit hoher Kundenfrequenz wie Lebensmitteldiscounter oder Bau- und Gartenmärkte als Angriffsziel gewählt.

[25] Skimming = Unrechtmäßige Erlangung von Zahlungskartendaten (PIN [persönliche Geheimnummer] und Magnetstreifendaten) zur Herstellung eigener Zahlungskartenfälschungen (white plastics)

[26] Zahlenbasis = Auswertung des polizeilichen Vorgangsbearbeitungssystems

[27] EMV-Chip = technischer Standard für die Kommunikation zwischen Chipkarte und Terminal

[28] Verwertungstat beim Skimming. Die erlangten Daten werden an Geldautomaten im Ausland eingesetzt

[29] PoS = Point of Sale, PoS-Terminals sind Kartenzahlterminals im Handel

Mit insgesamt 47 Fällen (davon 29 Fälle mit nachfolgendem Cashing) wurden 2012 in NRW deutlich mehr Manipulationen von PoS-Terminals als 2011 (neun Fälle) registriert.

Sachverhalt Skimming/PoS-Terminals

Unbekannte Täter drangen im Juni in einen Agrarhandel ein und manipulierten ein PoS-Terminal. Über einen Zeitraum von drei Monaten wurden schließlich unbemerkt die Zahlungskartendaten der Kunden ausgespäht. Die Kartendaten wurden später auf Kartenrohlinge übertragen. Im Oktober kam es schließlich zu ersten Verwertungstaten in den USA. Der Gesamtschaden beläuft sich auf über 380.000 Euro.

Neben dem bekannten Einbau der Skimming-Technik innerhalb der Terminals kam es im Jahr 2012 erstmals zum Einsatz von so genannten Hauben. Hierbei handelt es sich um täuschend echt aussehende Aufsätze mit Karteneinzugschlitz, Sichtschutz und Tastaturfeld.

Die Hauptgefahr liegt unverändert in der Tatsache, dass die Manipulationen äußerlich nicht oder nur schwer feststellbar sind. Die Magnetstreifendaten können dadurch über längere Zeiträume unentdeckt abgeschöpft werden. Jeder PoS-Manipulationsfall mit nachfolgendem Cashing zieht durchschnittlich Schäden im sechsstelligen Euro-Bereich nach sich.

3.7 Telekommunikationsanlagenmanipulation

Das Vorgangsbearbeitungssystem der Polizei NRW weist für das Jahr 2012 insgesamt 103 Fälle der „Manipulation von Telekommunikationsanlagen“ (TK-Anlagen) aus. Bei diesem Kriminalitätsphänomen werden innerhalb kürzester Zeit teure Auslandstelefonverbindungen generiert, welche Schäden im fünfstelligen Euro-Bereich verursachen. In 58 der mit Schadenssumme registrierten Fälle lag der Gesamtschaden bei mehr als 325.000 Euro. Ein Einzelfall erreichte eine Schadenshöhe von ca. 32.500 Euro.

Sachverhalt TK-Anlagen

Die Telekommunikationsanlage einer Gemeinschaftspraxis wurde manipuliert. Dabei erlangten die Täter Zugriff über die nicht geänderte (Standard-) PIN der Anlage. Anschließend wurden Auslandsgespräche geführt. Es entstand ein Schaden von 5.000 Euro.

Die Virtualisierung und Auslagerung der TK-Dienste in die „Cloud“[30] bietet inzwischen weitere Angriffspotenziale. Mit der erfolgreichen Erlangung des Administratoren-Status haben Täter dieselben Möglichkeiten wie in den anderen Bereichen der „virtuellen Welt“. Neben dieser Vorgehensweise kommen aber auch die bereits bekannten Angriffe auf TK-Anlagen zum Einsatz. Ziel sind hierbei unverändert Nebenstellen-, Wartungs- und Rufumleitungsfunktionen.

Gerade an arbeitsfreien Wochenenden, an denen erfahrungsgemäß die meisten Angriffe drohen, sollte durch die Anlagenbetreiber die Möglichkeit einer Zugriffseinschränkung geprüft werden. Grundsätzlich sollte bei der Rechtevergabe ohnehin abgewogen werden, inwieweit Mitarbeitern ein - für die Aufgabenerledigung ggf. entbehrlicher - uneingeschränkter Nutzungsumfang eingeräumt wird. Angesichts eines Falles, in dem eine TK-Anlage mit einer zwei Jahre alten Firmware betrieben wurde, stellt die Beauftragung eines professionellen Supports eine weitere sinnvolle Lösung dar. Der in diesem Fall entstandene Schaden von ca. 6.000 Euro hätte so vielleicht verhindert werden können. Ungeachtet dessen sollte eine TK-

[30] Cloud Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen. (Quelle: Bundesamt für Sicherheit in der Informationstechnik)

Anlage immer auf dem aktuellen technischen Stand und mit der neuesten Software betrieben werden. Die Vergabe eines individuellen, starken Zugangscodes („Passwort“) wird dringend empfohlen.

Martin

Bürstenbinder

„Manipulation von TK-Anlagen

Mit einfachen Maßnahmen Schutz gegen Gebührenbetrug erhöhen

Nach unseren Erkenntnissen ist das Ziel der Manipulation von TK-Anlagen ganz überwiegend Gebührenbetrug durch Rufweiterleitung an horrend teure Rufnummern in variierenden Zielländern. Angriffe erfolgen in der Regel am Wochenende, wenn niemand im Betrieb ist. Inzwischen warnen manche Anschlussnetzbetreiber ihre Kunden, wenn sie Auffälligkeiten im Verbindungsprofil entdecken. Doch dann ist in der Regel schon ein relevanter und manchmal auch drastischer finanzieller Schaden entstanden. Besonderes Augenmerk sollte darum auf der Vorbeugung liegen: bewusster Umgang mit sämtlichen Passwörtern, die Sprachboxen an Nebenstellen einer TK-Anlage und Zugänge zur Anlage selbst schützen. Nicht benötigte Auslandsvorwahlen können bei professionellen Anlagen in Sperrlisten eingetragen werden. Ebenso empfiehlt sich zeitnahes Einspielen von freigegebenen Software-Patches. Das sind einfache Maßnahmen, die bei konsequenter Anwendung in vielen Fällen schon das Schutzniveau deutlich erhöhen.“

Martin Bürstenbinder, Geschäftsführer, VAF Bundesverband Telekommunikation e.V.

3.8 Web 2.0/Soziale Netzwerke als neue Kriminalitätsbrennpunkte

Das Internet hat mit „Web 2.0“ eine Entwicklung vollzogen, bei der die Nutzer - statt vornehmlich Inhalte zu konsumieren - vermehrt selbst gestalten können. Aus diesem Grundgedanken entstanden neue Netz-Gemeinschaften (Social Media), u. a. 2004 der heutige Marktführer „Facebook“, bei dem im Oktober 2012 mehr als eine Milliarde[31] monatlich aktive Nutzer angemeldet waren oder 2005 das Videoportal „Youtube“ und 2006 „Twitter“.

Soziale Netzwerke sind Teilmenge der Social Media. In den Sozialen Netzwerken steht nicht wie bei den Themenforen ein bestimmter gemeinsamer Interessenschwerpunkt im Vordergrund. Vielmehr bieten sie eine Plattform, über die sich die Benutzer selbst darstellen, Ansprechpartner suchen und zu allen möglichen Themen kommunizieren können. Soziale Netzwerke sind insofern Kombinationen aus Homepages, Kontaktbörsen, öffentlichen Tagebüchern, Diskussionsrunden und Ähnlichem.

Sie verfügen üblicherweise über Standardfunktionen:

- Persönliches Profil mit Angaben zur Person und Fotos, Einstellungen zur Einsichtnahme der Profilangaben
- Kontaktliste oder Adressbuch mit Verwaltungsfunktionen, Importfunktionen aus anderen Adressbüchern
- Empfang und Versand von persönlichen Nachrichten an andere Mitglieder, Gruppen

[31] Quelle: heise.de;, http://www.heise.de/newsticker/meldung/Facebook-hat-eine-Milliarde-aktive-Nutzer-1723387.html, 25.01.2013

- Empfang und automatisierter Versand von Benachrichtigungen über Ereignisse (Profiländerungen, eingestellte Bilder, Videos, Kritiken etc.)
- Blogs[32] oder Mikroblogging-Funktionen
- Spiele, insbesondere zum Aufbau von sozialen Kontakten
- Suchfunktion über Mitglieder oder Einträge

Im Internet haben sich gerade im Bereich der Sozialen Medien Sonderformen von Kriminalität ausgebildet.

Beim Cybermobbing werden Personen mit Hilfe von Internetmedien, insbesondere auch Soziale Netzwerke, diffamiert, beleidigt, belästigt oder genötigt. Während verbale Angriffe, wie bei einem Streit auf dem Schulhof, zumindest für umstehende Personen schnell vergessen sind, bleibt ein Beitrag im Internet lange veröffentlicht und geht weit über die Wahrnehmbarkeitsgrenzen der Schule hinaus. Täter sind Erwachsene und Jugendliche beiderlei Geschlechts. Opfer werden neben Erwachsenen und Jugendlichen auch Kinder. Die Situation ist für die Opfer belastend.

Michael

Kranawetter

„Cybermobbing wird zunehmend ein Thema unter Jugendlichen, in einer global durchgeführten Studie zum Thema Onlinemobbing in 2012 wurde für Deutschland festgestellt, dass mittlerweile 39% der Jugendlichen zwischen 8 und 17 Jahren Opfer von Verunglimpfung, Schikanen und Hänseleien durch Online Aktivitäten wurden; damit ist Deutschland weltweit auf Platz 11. Dagegen steht, dass lediglich 18% der Schulen Richtlinien und Sanktionen vorweisen und nur 28% der Schulen ihre Schüler aufklären oder beraten können. Für Interessierte, die das Thema aktiv angehen wollen, steht auf www.sicherheit-macht-schule.de Informationsmaterial für Schulen bereit.

Die Studie zeigt insbesondere für Deutschland auch auf, dass Onlinemobbing ab einem Alter von 13 Jahren zunimmt, davor wird eher offline, also traditionell gemobbt, wovon 79% der Jugendlichen betroffen sind. Zudem werden eher Mädchen online gemobbt und mobben auch eher online. Jungen werden stärker kontrolliert und dürfen weniger Zeit im Internet verbringen. Somit sind im Täter und Opferbereich Mädchen zwischen 13 und 17 besonders in den Fokus zu nehmen.

Um dieser Entwicklung entgegen zu wirken, sollten folgende Punkte beachtet werden:

- Lassen Sie Ihre Kinder online nicht allein. Achten Sie darauf, wie Ihre Kinder das Internet nutzen und wo sie sich bewegen. Hören Sie zu und ermuntern Sie Ihre Kinder, Ihre Erfahrungen zu teilen.

- Ermutigen Sie Ihre Kinder, sich anders zu verhalten und mit gutem Beispiel voranzugehen. Denken Sie aber daran, dass Ihre Kinder dabei Ihre Unterstützung benötigen.

- Wenn Ihr Kind betroffen ist, warten Sie nicht, bis sich das Problem von selbst erledigt. Greifen Sie aktiv ein und fragen Sie, wie Sie helfen können.

[32] zumeist öffentlich geführtes Tagebuch oder Journal

	- Sollten Sie feststellen, dass Ihr Kind andere Kinder mobbt, stellen Sie klar, dass dies nicht ok ist. Aber versuchen Sie auch, die Hintergründe herauszufinden. Greifen Sie bei Bedarf auf professionelle Hilfe zurück. - Vermitteln Sie Ihren Kindern, dass sich Konflikte auch anders lösen lassen.“ Michael Kranawetter, Chief Security Advisor, Microsoft Deutschland GmbH, Mitglied des BITKOM

Das Cyber-Grooming bezeichnet eine Vorgehensweise von Tätern, bei der Kinder und Jugendliche im Internet zur Anbahnung sexueller Handlungen kontaktiert werden. Dies gelingt Tätern insbesondere in Sozialen Netzwerken, die auf diese Opfergruppen ausgerichtet sind. Darüber hinaus erfolgen über Soziale Medien Absprachen zwischen Tatbeteiligten, die Abwicklung von Drogengeschäften oder die Verbreitung strafrechtlich relevanter Inhalte politischer Extremisten.

Neben den „Global Playern“ gibt es Soziale Netzwerke, die für einen regionalen Nutzerkreis bedeutsam sind. Für Russland und die Ukraine sind das „Odnoklassniki“ und „Vkontakte“. In China werden aufgrund der staatlichen Restriktionen gegen ausländische Anbieter insbesondere die Sozialen Netzwerke „Qzone“ und „Renren“ genutzt. Einwohner mit Migrationshintergrund nutzen diese Netzwerke von Deutschland aus, um beispielsweise mit Angehörigen oder Freunden in Kontakt zu bleiben. Für polizeiliche Ermittler ergibt sich daraus u. a. ein sprachliches Problem. Darüber hinaus nutzen deutsche Straftäter ausländische Kommunikationsplattformen, da sie davon ausgehen, dort sicherer vor dem Zugriff deutscher Strafverfolgungsbehörden zu sein.

3.9 Kinderpornografie

Kinderpornografische Schriften - d. h. insbesondere Bild- und Videomaterial - beinhalten die Dokumentationen von sexuellen Missbrauchshandlungen zum Nachteil von Kindern und sind gemäß § 184 b StGB mit einem Herstellungs-, Besitz-, Beschaffungs- und Verbreitungsverbot belegt. Aufgrund der bevorzugten Verbreitungswege dieses Materials werden diese Delikte der Cybercrime (Tatmittel Internet) zugerechnet.

Bei der Verbreitung von Kinderpornografie spielt der kommerzielle Markt eine untergeordnete Rolle; überwiegend wird einschlägiges Material getauscht.

Missbrauchsabbildungen von Kindern findet man in nahezu allen Diensten des Internet. Wurde der Tausch vor Jahren noch überwiegend per E-Mail abgewickelt, geht der Trend in den letzten Jahren hin zur Verbreitung über sog. Tauschbörsen und über Messenger-Programme. Darüber hinaus nutzen viele Täter anonymisierte Dienste wie z. B. das TOR-Netzwerk[33] zum Tausch der Missbrauchsabbildungen. Das anonymisierte Tauschen und das Fehlen einer Mindestdatenspeicherfrist stellen die Polizei vor besondere Herausforderungen. Es müssen zeitaufwändige Anstrengungen unternommen werden, um mit alternativen Ermittlungsmethoden die Täter zu identifizieren. Da Verbreiter von Kinderpornografie auch immer potenzielle sexuelle Missbraucher sind[34], gehen dadurch oft wertvolle Hinweise zur Ermittlung und Verfolgung eines sexuellen Kindesmissbrauchs verloren.

[33] Siehe 2.4 Anonymisierungspotentiale

[34] Quelle: Child Pornography Offenses Are a Valid Diagnostic Indicator of Pedophilia”, Journal of Abnormal Psychology, 2006 (Seto & Cantor, Universität Toronto)

4 Initiativen

Die beschriebenen technischen, rechtlichen und phänomenologischen Anforderungen an die Polizei sind enorm. Es ist nicht zu erwarten, dass diese allein durch die weitere quantitative Verbesserung der personellen und technischen Bedingungen zu bewältigen sein werden. Es ist erforderlich, neue Wege zu gehen. Die Polizei NRW setzt auf die kooperative Bewältigung dieser Herausforderungen und optimiert die internen Prozesse. Dabei zeigt sich, dass durch Einbindung aller wesentlichen Akteure und durch schnellere und vereinfachte interne Abläufe eine erfolgreichere, aber auch effizientere Aufgabenwahrnehmung ermöglicht wird. Die folgenden Beispiele sollen dies verdeutlichen.

4.1 Sicherheitskooperation Cybercrime - Landeskriminalamt NRW und BITKOM

„Gemeinsam gegen Cybercrime“

Die seit 2011 bestehende Kooperation will in Wirtschaft und Sicherheitsbehörden den gegenseitigen Informationsaustausch und Wissenstransfer über technologische Entwicklungen und aktuelle Kriminalitätsphänomene nachhaltig fördern, Präventionsmaßnahmen entwickeln und umsetzen sowie frühzeitig neuen Erscheinungsformen der Cybercrime begegnen. Der Erreichung dieser Ziele dienen gemeinsame Aktivitäten in den Kooperationsfeldern:

- Informationsaustausch und Wissenstransfer
- gegenseitige Hospitationen
- Dunkelfeldforschung
- Reduzierung des Dunkelfeldes durch die Verbesserung des Anzeigeverhaltens
- Konzeption und Durchführung von Präventionsmaßnahmen
- Vermitteln von Experten in konkreten Einzelfällen

Im Jahr 2012 wurden in diesen Handlungsfeldern die folgenden Aktivitäten entwickelt:

- IuK-Kriminalität Lagebild 2011 des Landeskriminalamts NRW unter der Beteiligung des BITKOM erstellt
- Durchführung einer Vielzahl von Awareness-Veranstaltungen
- BITKOM und Landeskriminalamt NRW sind im Landespräventionsrat NRW aktiv
- Einrichtung einer Expertenhotline zwischen Landeskriminalamt NRW und BITKOM
- Hospitationen mehrerer Firmen beim Landeskriminalamt NRW
- Strategische Zusammenarbeit mit dem SPIK e.V. (Schweizer Polizei Informatik Kongress)

Ein konkretes Beispiel

Ein wesentliches Kooperationsfeld stellen die gegenseitigen Hospitationen dar. Hier begegnen sich Experten aus Wirtschaft und Polizei bei der Bewältigung einer gemeinsamen Aufgabe. Neben der Optimierung von Arbeitsabläufen und dem gegenseitigen Kennenlernen können durch Hospitationsprojekte auch innovative, praxisbezogene Lösungen entstehen. Beispielsweise erfolgte eine dreiwöchige Hospitation von Mitarbeitern eines weltweit agierenden IT-Konzerns beim Landeskriminalamt NRW. Gemeinsames Thema der Hospitation war die „Semantische Analyse unstrukturierter Massendaten“. Die derzeit und

zukünftig anfallenden enormen und heterogenen Datenmengen stellen für Wirtschaft und Strafverfolgungsbehörden gleichermaßen eine große Herausforderung dar und erfordern Lösungsansätze, die eine zeit- und ressourcensparende, effiziente Auswertung gewährleisten. Gemeinsam wurde an einem bereits abgeschlossenen Ermittlungsvorgang nochmals eine Auswertung durchgeführt. Dazu wurden in technischem und kriminalfachlichem Austausch Wissensbausteine erarbeitet, implementiert und auf den aufbereiteten Datenbestand angewandt. Der Vergleich zwischen der klassischen und der neuen, innovativen Analysemethode führte zu wertvollen Erkenntnissen bei Polizei und Wirtschaftsunternehmen.

4.2 Filmprojekt

Das Landeskriminalamt NRW ist Mitglied der Arbeitsgruppe Prävention von Internet- und Computerkriminalität des Landespräventionsrats NRW, welcher Mitglieder aus verschiedenen Fachrichtungen, wie beispielsweise der Handwerkskammer, der Verbraucherzentrale NRW und des Schulministeriums angehören. Der Landespräventionsrat berät die Landesregierung in allen Fragen der Kriminalprävention. In diesem Rahmen entstanden unter Koordination des Landeskriminalamts NRW im Jahr 2012 unter dem Titel „Sichere Netzwelten“ sechs Kurzfilme zur Prävention von Cybercrime sowie ein Making-of. Durch die Einbeziehung leistungsstarker Kooperationspartner, wie das Institut für Internetsicherheit der Westfälischen Hochschule in Gelsenkirchen und den Autor und Regisseur Oliver Köhler, konnte der jeweilige Erstellungsprozess besonders effizient und kostengünstig gestaltet werden.

Nach der Festlegung von Themen innerhalb der Arbeitsgruppe erfolgt die Produktion in Zusammenarbeit mit dem Institut für Internetsicherheit der Westfälischen Hochschule Gelsenkirchen und einem professionellen Filmteam. Bemerkenswert sind die enge Verzahnung der beteiligten Stellen sowie die unbürokratische Bereitstellung von Mitteln. Diese Konstellation ermöglicht es, unmittelbar auf aktuelle Phänomene einzugehen. Die filmische Umsetzung dauert in Folge dessen nur wenige Wochen und ermöglicht damit eine bislang nur schwer erreichbare Aktualität im Hinblick auf die dargestellten Cybercrime-Phänomene sowie die technischen Hintergründe. Durch die Creative Commons Lizenz dürfen die Filme beliebig vervielfältigt und eingesetzt werden. Die Präventionsfilme wurden auf zahlreichen Veranstaltungen vorgestellt und stießen auch im benachbarten Ausland (Niederlande und Schweiz) auf großes Interesse. Die mittlerweile 3. Staffel mit vier Filmen wurde erstmals Ende April 2013 auf dem Deutschen Präventionstag in Bielefeld öffentlich gezeigt. Mit der Produktion einer neuen Staffel soll im Jahr 2013 begonnen werden. Weitere Projekte sehen z. B. die Einbettung der Filme in ein Schulstundenkonzept sowie Veranstaltungen zur Prävention von Cybercrime in kleinen und mittelständischen Unternehmen vor.

Die Filme können kostenlos heruntergeladen und genutzt werden:

http://www.justiz.nrw.de/BS/praevention/zwischentext_internet_praevention/index.php

Screenshot aus dem Awarenessfilm „Passwortsicherheit“

4.3 Single Point of Contact

Eine wesentliche Erkenntnis aus dem intensiven Austausch mit Wirtschaftsunternehmen ist deren Erwartung an eine professionelle und angemessen handelnde Polizei. Das Management der Firmen befürchtet Reputationsverlust und erfolglose Ermittlungen der Polizei und verzichtet daher häufig auf die Einbindung der Strafverfolgungsorgane. Stattdessen werden immer häufiger private Sicherheitsunternehmen mit Ermittlungen betraut. Um dem zu begegnen, hat das Landeskriminalamt NRW in seinem Cybercrime-Kompetenzzentrum einen so genannten Single Point of Contact eingerichtet. Hier stehen unter einer Telefonnummer und einer E-Mail-Adresse rund um die Uhr polizeiliche Experten zur Verfügung und beantworten dringende Fragen aus Wirtschaft, Politik sowie Forschung und Lehre. Unternehmen können auch Strafanzeige erstatten und aktuelle Cyber-Angriffe melden. Ein besonderer Geschäftsprozess, der jeweils eigene Kommunikationsstränge zur IT-Abteilung sowie zum Management bzw. zur Rechtsabteilung des betroffenen Unternehmens unterhält, sorgt für einen ebenengerechten, gezielten Informationsfluss. Sofern das Landeskriminalamt NRW die Ermittlungsverfahren nicht in eigener Zuständigkeit bearbeitet, wird eine kontrollierte Übergabe an eine zuständige und leistungsfähige Kreispolizeibehörde sichergestellt. Die

positiven Erfahrungen mit dieser Service-Einrichtung haben dazu geführt, dass sich im Jahr 2012 bereits in 150 Fällen Firmen und Organisationen an das Cybercrime-Kompetenzzentrum wandten, darunter börsennotierte Konzerne, die Angriffe gegen deren IT-Systeme beim Landeskriminalamt NRW zur Anzeige bringen.

4.4 Kooperation des Landeskriminalamts NRW mit der Fachhochschule Aachen

Zwischen der Fachhochschule Aachen, Fachbereich Elektrotechnik und Informationstechnik, und dem Landeskriminalamt NRW wurde ein Kooperationsvertrag unterzeichnet. Die Initiative hat sich die Ziele gesetzt, das allgemeinen Bewusstsein um die Gefahren von Cybercrime zu verbessern, die technischen Kompetenzen beider Kooperationspartner zu verbessern, neue Technologien zur Prävention und Strafverfolgung zu entwickeln und schließlich den Wissenstransfer zwischen den Kooperationspartnern zu intensivieren.

Im Rahmen der Kooperation wurden Themenschwerpunkte ausgearbeitet, welche Aufgabenstellungen für Praktikumssemester und Bachelorarbeiten ermöglichten und gleichzeitig das Landeskriminalamt NRW bei seiner Aufgabenerfüllung unterstützen.

Eines dieser Themen war der Aufbau einer Mobilfunkzelle. Zur Analyse von Schadsoftware wird in der Netzwerkforensik üblicherweise der Netzwerkverkehr des vermeintlich infizierten Computers analysiert. Hier wird beispielsweise untersucht, welche Internetadressen der Rechner zu welchen Zeitpunkten aufsucht oder ob dieser Spam versendet. Ein solcher Ansatz ist auch für das Erkennen von Schadsoftware in Handys und Smartphones denkbar. Mit diesem Projekt wurde eine Infrastruktur geschaffen, die die Beobachtung des Verhaltens eines Mobiltelefons ermöglicht. Dazu wird in einer abgeschirmten Umgebung eine Mobilfunkzelle inklusive Vermittlungssoftware installiert. Eine Überwachungseinheit protokolliert die Aktivitäten des in der Testzelle eingebuchten Mobiltelefons. Einer der in diesem Projekt im Rahmen seines Praktikumssemesters tätigen Studenten fertigte seine Bachelorarbeit zu diesem Thema und schloss diese mit Bestnote ab. Er konnte im Anschluss an sein Studium unmittelbar als Mitarbeiter für das Landeskriminalamt NRW gewonnen werden.

4.5 Prävention

Die Prävention von Cybercrime obliegt den sachlich und örtlich zuständigen Kreispolizeibehörden. Das Landeskriminalamt unterstützt die Kreispolizeibehörden insbesondere durch

- Erhebung des kriminalpräventiven Handlungsbedarfs
- Fortschreiben von Standards und Entwickeln von Medien
- Initiieren und Koordinieren von überregionalen Präventionsmaßnahmen

Die Prävention von Cybercrime wird im Landeskriminalamt vom Cybercrime-Kompetenzzentrum wahrgenommen. Zu den durchgeführten Präventionsmaßnahmen gehören Informationsveranstaltungen und Vortragstätigkeiten bei Behörden und in der Wirtschaft, die aus der Zusammenarbeit mit unterschiedlichen Institutionen oder Verbänden hervorgehen. Für die Industrie- und Handelskammern werden beispielsweise Referate zum Thema Cybercrime für kleine und mittelständische Unternehmen angeboten.

Die Präventionsarbeit in den Kreispolizeipolizeibehörden zeichnet sich durch vielfältige Aktivitäten aus. Im Vordergrund stehen verhaltensorientierte Ansätze, die durch Vorträge, Workshops oder Multiplikatorenschulungen verfolgt werden. Aktuelle Themen wie etwa „Gefahren durch neue Medien“ werden insbesondere für Lehrerkollegien, Studienseminare, Erzieherinnen oder andere Berufsgruppen mit pädagogischem Hintergrund angeboten.

Prävention von Cybercrime beginnt bereits im Grundschulalter. Eltern und Pädagogen werden die Gefahren erläutert und entsprechende Verhaltenshinweise gegeben. Weiterführende Schulen oder Berufskollegs passen die Themen altersgerecht an und informieren die Heranwachsenden über Gefahren, Opfer oder Täter zu werden.

Informationsstände und Vorträge auf Großveranstaltungen wie der Security-Messe 2012 in Essen oder dem Deutschen Präventionstag 2012 in München werden genutzt, um die breite Öffentlichkeit zu erreichen.

Der demografische Wandel führt dazu, dass die Zahl der Internetnutzer in der Generation 60+ stetig wächst. Immer mehr Kreispolizeibehörden führen daher Präventionsveranstaltungen in Seniorenunterkünften durch. Welches Alter die Zielgruppe der Präventionsarbeit auch hat, die enge Zusammenarbeit mit anderen Behörden und Verbänden wie etwa Schulämtern, Sozialverbänden oder Medienzentren fördert den Informations- und Wissenstransfer. Einige Kommunen vernetzen sich unter Einbeziehung der Polizei in Arbeitskreisen, um durch die Zusammenarbeit von Experten unterschiedlichster Fachrichtungen eine flächendeckende und ressortübergreifende Präventionsarbeit zu forcieren. Diese Form der Kooperationsarbeit ermöglicht die kostengünstige und effiziente Umsetzung von Präventionsmaßnahmen und aktiviert alle wichtigen Akteure.

Neben den bereits im Lagebild IuK-kriminalität 2011 vorgestellten Informationen bietet das Programm Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK) unter www.polizei-beratung.de weitere Angebote rund um das Thema Cybercrime und Mediensicherheit.

5 Fazit

Obwohl die Cybercrimebekämpfung der Polizei NRW noch nie besser aufgestellt war, ist die Aufklärungsquote im Bereich der Cybercrime im engeren Sinne erneut gesunken!

Im Abschnitt „Ermittlungshemmnisse“ wurden im multifaktoriellen Ansatz einige Ursachen für den stetigen Rückgang der Aufklärungsquote beleuchtet. Ein wesentlicher Faktor ist die quantitative Entwicklung der Fallzahlen der Cybercrime. Je mehr Ermittlungsverfahren durch die polizeilichen Experten in den Polizeibehörden zu bearbeiten sind, desto weniger Zeit steht ihnen zur Klärung der einzelnen Straftaten zur Verfügung. Die Polizei NRW hat daher die Anzahl der Experten, darunter auch Informatiker, im Jahr 2012 erneut erhöht. Die Verbesserung des Personaleinsatzes allein wird jedoch nicht alle Ursachen der aufgezeigten Entwicklung beseitigen können, denn auch andere Rahmenbedingungen beeinflussen die Erfolgsaussichten der Cyberkriminalisten.

Cybercrime ist bereits technisch bedingt ein internationales Phänomen ohne Grenzen - jedenfalls für die Straftäter. Die Strafverfolgung hingegen bewegt sich nach wie vor in den durch nationales Recht geprägten Grenzen und kann diese meist nur unter Anwendung der mit einzelnen Staaten vereinbarten Abkommen sowie anderen binationalen Verträgen, die beispielsweise auf den so genannten Prümer Verträgen basieren, überwinden (vgl. 2.3). Langfristig bedarf es jedoch einer internationalen Vereinbarung, die über die europäischen Grenzen hinaus eine zuverlässige Basis für die justizielle Rechtshilfe schafft.

Zu den wesentlichen Ermittlungshemmnissen zählen auch die immer weiter verbreiteten Anonymisierungsmöglichkeiten des Internets. Kostenlose Dienste, die es einerseits dem Bürger in einem Unrechtsstaat erlauben sollen, ohne staatliche Sanktionierung sein Recht auf Meinungsäußerung wahrzunehmen, stehen auf der anderen Seite aber auch Straftätern in demokratisch legitimierten und organisierten Gesellschaften zur Verfügung. Für den Täter bedeutet dies eine einfache und kostenlose Möglichkeit, sich der Strafverfolgung zu entziehen. Die Polizei kann diesen Vorsprung nicht oder nur mit erheblich höherem Ermittlungsaufwand kompensieren und ist dabei darauf angewiesen, aus anderen rechtmäßig zugänglichen Quellen verwertbare Informationen zu erschließen. Bei allen bereits bestehenden Möglichkeiten der Straftäter sollte dieses Ungleichgewicht nicht noch vergrößert werden. Das Fehlen einer angemessenen Mindestdatenspeicherfrist ist dabei ein herausragendes Ermittlungshemmnis, das nicht nur die Terrorismusbekämpfung und die Aufklärung von Kapitalverbrechen erschwert. Auch die Aufklärung vieler Delikte der Massenkriminalität wird vereitelt. Sowohl die datenschutzrechtlichen Rahmenbedingungen als auch die strafprozessualen Ermächtigungen der Polizei müssen daher stetig an der raschen Entwicklung der Cybercrimephänome gemessen und – falls erforderlich – fortentwickelt werden.

Der Cybersicherheit haben sich mittlerweile viele wesentliche Institutionen und Akteure aus Politik, Justiz, Wirtschaft, Forschung und Lehre verschrieben. In den intensiven, teilweise schon strukturierten Informationsaustauschen auf nationalen und internationalen Plattformen ist die polizeiliche Cybercrimebekämpfung eng eingebunden. Die Vernetzung steigert allseits die Kompetenzen. Im Sinne dieser Strategie hat das Landeskriminalamt NRW bereits im Jahr 2011 eine Kooperationsvereinbarung mit dem Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) geschlossen. Die vielen gemeinsamen Aktivitäten im Jahr 2012 (vgl. 4 Initiativen) standen unter dem Motto:

Gemeinsam gegen Cybercrime

Die ersten Erfahrungen haben bestätigt, dass sowohl bei Strafverfolgungsbehörden als auch bei den übrigen Kooperationspartnern ein großer Bedarf nach einem qualifizierten Informations- und Know-how-Transfer besteht. Dabei handelt es sich um einen Austausch von Erfahrungen und Wissen, der allen Beteiligten zugute kommt. Die Polizei NRW hat damit im Jahr 2012 wichtige Schritte auf dem Weg zu einer noch professionelleren und kooperativen Cybercrimebekämpfung unternommen.

6 Begriffsbestimmungen und Anlagen

6.1 Definitionen

Cybercrime

Cybercrime umfasst die Straftaten, die sich gegen das Internet, weitere Datennetze und informationstechnische Systeme oder deren Daten richten. Cybercrime umfasst auch solche Straftaten, die mittels dieser Informationstechnik begangen werden.

Diese Definition berücksichtigt sowohl nationale als auch internationale Sicherheitsstrategien. Dabei steht sie im Einklang mit internationalen Begriffsbestimmungen wie der European Cyber Crime Convention[35] der United Nations.

Cybercrime im engeren Sinne

Die Cybercrime im engeren Sinne umfasst Straftaten, bei denen Elemente der elektronischen Datenverarbeitung in den Tatbestandsmerkmalen enthalten sind (Computerkriminalität). 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. Vorbereitungshandlungen gem. §§ 202 a, 202 b und 202 c StGB[36]
- Softwarepiraterie (privates Handeln)
- Softwarepiraterie (gewerbsmäßiges Handeln)
- Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten

Bot-Netz

Der Begriff ist die Kurzform von Roboter-Netzwerk. Darunter versteht man ein fernsteuerbares Netzwerk mit spezieller Schadsoftware infizierter Computer. Gesteuert werden die Botnetze über Command&Control-Server. Bot-Netze können für die Verbreitung von Spam- oder Phishing-E-Mails oder Denial-of-Service-Attacken verwendet werden. In der Regel bemerken die Nutzer der betroffenen Computer die Kompromittierung ihrer Systeme nicht.

6.2 Auftrag „Lagebild“

Mit Erlass MIK NRW vom 29.02.2012 - 423-62.18.09 „Bekämpfung der Kriminalität unter Nutzung von Informations- und Kommunikationstechnik durch die Polizei des Landes Nordrhein-Westfalen“ wurde das Landeskriminalamt NRW beauftragt, ein spezifisches jährliches Lagebild zu erstellen.

[35] Convention on Cybercrime, Budapest, 23.11.2011 (CETS No. 185)

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

6.3 Datenbasis

Grundlage dieses Lagebildes sind Daten aus der Polizeilichen Kriminalstatistik, Sachverhalte aus dem polizeilichen Vorgangsbearbeitungssystem und dem Kriminalpolizeilichen Sondermeldedienst IuK-Kriminalität. In der Polizeilichen Kriminalstatistik werden unter dem Summenschlüssel 897000 nur die Delikte der Cybercrime im engeren Sinne zusammengefasst (siehe Nr. 5.1).

Im Kriminalpolizeilichen Sondermeldedienst Cybercrime melden die Polizeibehörden folgende Straftaten der Cybercrime im engeren Sinne:

- § 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, Falschbeurkundung/Urkundenunterdrückung,
  § 348 StGB im Zusammenhang mit Datenverarbeitung
- § 303 a StGB Datenveränderung
- § 303 b StGB Computersabotage

Während sich aus der Polizeilichen Kriminalstatistik nicht alle Informationen zu den einzelnen Straftaten entnehmen lassen, bietet der Kriminalpolizeiliche Sondermeldedienst IuK-Kriminalität eine zusätzliche Möglichkeit einer differenzierten Auswertung von Informationen zur Phänomenologie einzelner Delikte.

Um neue Tatbegehungsformen der Cybercrime zeitnah erkennen zu können, bietet der Kriminalpolizeiliche Sondermeldedienst Cybercrime den sachbearbeitenden Dienststellen auch die Möglichkeit, Straftaten über den Katalog hinaus zu melden, wenn

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

Zur umfassenden Darstellung der Cybercrime wurde eine ergänzende Auswertung der im polizeilichen Vorgangsbearbeitungssystem erfassten Datensätze vorgenommen.

6.4 Tabellen - PKS

Tabelle 1: Fallzahlen in einzelnen Deliktsfeldern der IuK-Kriminalität im engeren Sinne bei Deliktsgruppen

	Delikte		Zu- bzw. Abnahme			
	2011	2012				in %
Computerbetrug	6.277	6.087	-	190	-	3,0
Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung	1.994	2.278	+	284	+	14,2
Datenveränderung/ Computersabotage	1.498	4.118	+	2.620	+	174,9
Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen	3.257	4.373	+	1.116	+	34,3
Betrug mittels rechtswidrig erlangter Debitkarte mit PIN	6.108	4.880	-	1.228	-	20,1
Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten	881	491	-	390	-	52,4
Softwarepiraterie private Anwendung	12	25	+	13	+	108,3
Softwarepiraterie gewerbsmäßiges Handeln	9	48	+	39	+	433,3
Computerkriminalität insgesamt	20.036	22.228	+	2.192	+	10,9

Tabelle 2: Aufklärungsquoten

	aufgeklärte Fälle		Aufklärungsquote %		Zu- bzw. Abnahme	
	2011	2012	2011	2012	% - Punkte	
Computerbetrug	1.369	1.555	21,8	25,6	+	3,8
Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung	740	617	37,1	27,1	-	10,0
Datenveränderung / Computersabotage	224	252	15,0	6,1	-	8,9
Ausspähen, Abfangen von Daten einsch Vorbereitungshandlungen	456	570	14,0	13,0	-	1,0
Betrug mittels rechtswidrig erlangter Debitkarte mit PIN	1.884	1.516	30,2	31,1	+	0,9
Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten	227	127	25,8	30,3	+	4,5
Softwarepiraterie private Anwendung	11	21	91,7	84,0	-	7,7
Softwarepiraterie gewerbsmäßiges Handeln	6	46	66,7	95,8	+	29,1
Computerkriminalität insgesamt	4.877	4.704	24,3	21,2	-	3,1

Tabelle 3: Entwicklung der Fallzahlen und der Aufklärungsquoten

	bekannt gewordene Fälle			Aufklärung	
	erfasste Fälle	Zu- bzw Abnahme		aufgeklärte	Aufklärungs-
Jahr	insgesamt	%		Fälle	quote %
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
2010	19.775	+	27,2	5.710	28,9
2011	20.036	+	1,3	4.877	24,3
2012	22.228	+	10,9	4.704	21,2

Tabelle 4: Entwicklung der Altersverteilung der Tatverdächtigen

Tatverdächtige											
			14		18		unter		ab		
	bis unter		bis unter		bis unter		21		21		insge-
	14		18		21		insgesamt		insgesamt		samt
Jahr	absolut	Anteil %	absolut	Anteil %	absolut	Anteil %	absolut	Anteil %	absolut	Anteil %	
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	2.741	76,3	3.591
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
2010	87	1,8	472	9,7	636	13,1	1.195	24,6	3.671	75,4	4.866
2011	50	1,2	379	9,0	447	10,6	876	20,8	3.326	79,2	4.202
2012	126	3,4	284	7,6	362	9,6	772	20,6	2.981	79,4	3.753

Tabelle 5: Tatmittel Internet

Tatmittel Internet			
	erfasste Fälle insgesamt	darunter Tatmittel Internet	
	2012	absolut	Anteil %
Straftaten insgesamt	**1.518.363**	**54.339**	**3,6**
Straftaten gegen die sexuelle Selbstbestimmung	10.498	1.632	15,5
- Verbreitung pornografischer Erzeugnisse	1.780	1.404	78,9
darunter:			
- Besitz/Verschaffen von Kinderpornografie	519	400	77,1
- Verbreitung von Kinderpornografie	837	723	86,4
Betrug	263.992	35.987	13,6
darunter:			
- Waren- und Warenkreditbetrug	70.895	20.010	28,2
- Computerbetrug	6.087	5.052	83,0
- Betrug mit Zugangsdaten zu			
Kommunikationsdiensten	419	182	43,4
Fälschung beweiserheblicher Daten,	2.278	1.782	78,2
Täuschung im Rechtsverkehr bei Datenverarbeitung			
Datenveränderung, Computersabotage	4.118	3.940	95,7
Ausspähen, Abfangen von Daten einschl.	4373	3798	86,9
Vorbereitungshandlungen			
Erpressung	2.731	1.324	48,5

6.5 Ansprechpartner/ergänzende Hinweise

Landeskriminalamt Nordrhein-Westfalen

Abteilung 4

Cybercrime-Kompetenzzentrum

Dezernat 41

0211-939-4110

cybercrime.lka@polizei.nrw.de

Weitere Informationen für Polizeibedienstete im Intrapol NRW:

http://intrapol.polizei.nrw.de/Kriminalitaet/Delikte/IuKKrim/Seiten/default.aspx

Notizen

Herausgeber

Landeskriminalamt Nordrhein Westfalen
Völklinger Str. 49
40221 Düsseldorf

Dezernat 41
Redaktion: KR Helmut Picko
Tel.: 0211-939-4100 oder Polizeinetz 07-224-4100
Fax: 0211-939-194100 oder Polizeinetz 07-224-194100

Dez41.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

Titelbild: Landeskriminalamt NRW, Dezernat 41, Fotograf: S. Becker