POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

IuK-Kriminalität in NRW – Entwicklung und Bewertung

Lagebild 2011

POLIZEI Nordrhein-Westfalen Landeskriminalamt

Kriminalitätsentwicklung im Überblick

IuK-Kriminalität[1] in NRW – Entwicklung und Bewertung

- Fallzahlen der IuK-Kriminalität im engeren Sinne[2] (oder Computerkriminalität) steigen erstmals seit 2001 wieder über 20.000
- Starke Zunahme der Erpressungen mit Tatmittel Internet bei großem Dunkelfeld
- Skimming - Fallzahlen stark rückläufig
- Datenveränderung und Computersabotage - Fallzahlen nahezu verdoppelt
- Niedrigste Aufklärungsquote seit Erfassung der IuK-Kriminalität im engeren Sinne (1987)

	2010	2011		in %	Tendenz[3]
IuK-Kriminalität im engeren Sinne	**19.775**	**20.036**	+	**1,3**	
Computerbetrug	7.406	6.277	-	15,2	
Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung	1.442	1.994	+	38,3	
Datenveränderung/Computersabotage	783	1.498	+	91,3	
Ausspähen; Abfangen von Daten einschl. Vorbereitungshandlungen gem. §§ 202 a, 202 b, 202 c StGB	3.954	3.257	-	17,6	
Betrug mittels rechtswidrig erlangter Debitkarte mit PIN	5.511	6.108	+	10,8	
Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten	637	881	+	38,3	
Straftaten mit Tatmittel Internet	**48.411**	**47.992**	**-**	**0,9**	
Betrug mit Tatmittel Internet	39.060	37.923	-	2,9	
Erpressung mit Tatmittel Internet	26	336	+	1192,3	

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

[2] Informationen zur Definition und Abgrenzung unter 5.1

[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 IuK-Kriminalität stellt phänomenspezifisch und phänomenübergreifend die Entwicklung der IuK-Kriminalität im Land Nordrhein-Westfalen dar. Die Daten[4] basieren auf Meldungen zu Verfahren der Polizeibehörden in NRW, die nach einem bundesweit einheitlichen 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

Von den insgesamt 1.511.469 in NRW polizeilich bekannt gewordenen Straftaten im Jahr 2011 sind laut Polizeilicher Kriminalstatistik 20.036 (1,3 %) der IuK-Kriminalität im engeren Sinne zuzuordnen. Dies entspricht einer Zunahme um 261 Fälle (1,3 %) gegenüber dem Vorjahr (19.775 Fälle).

Damit übersteigt die Anzahl in diesem Jahr erstmals seit 2001 wieder 20.000 Fälle. In den vergangenen Jahren waren die Fallzahlen schwankend, wiesen aber insgesamt eine zunehmende Tendenz auf. Im Jahr 2010 ergab sich eine Steigerung um mehr als 27 % im Vergleich zum Jahr 2009. 2011 wurden 2.471 Fälle der Datenveränderung bzw. Computersabotage (so genannte Ransomware vgl. 2.3) in der Polizeilichen Kriminalstatistik nicht erfasst, da deren Aufklärung durch deutsche Ermittlungsbehörden zur Feststellung aus dem Ausland agierender ausländischer Tatverdächtiger führte. Unter Berücksichtigung dieser - als so genannte Auslandsstraftaten nicht in die Polizeiliche Kriminalstatistik eingehenden - Fälle, würde der seit 2008 steigende Trend fortgesetzt.

1.3 Einzelne Deliktsfelder

Betrug mittels rechtswidrig erlangter Debitkarten[5] mit PIN

Der Anstieg der Fallzahlen um 10,8 % (+ 597 Fälle) korreliert mit dem Anstieg der Taschendiebstahlsdelikte. Der häufig leichtfertige Umgang der Geschädigten mit ihrer PIN[6], die in vielen Fällen als Notiz in der Geldbörse oder Handtasche mitgeführt wird, ermöglicht den Tätern den rechtswidrigen Einsatz erbeuteter Debitkarten.

Computerbetrug

Von 2008 bis 2010 stiegen die Fallzahlen in diesem Deliktsfeld erheblich. Im Jahr 2011 ergab sich mit 6.277 Fällen im Vergleich zu 2010 ein Rückgang um 1.129 Fälle (- 15,2 %). Ob dies mit den zunehmend wirksamen technischen Sicherungen, z.B. chipTAN und smsTAN, oder mit dem Abschluss der flächendeckenden Einführung des EMV-Chips[7] in Europa in Zusammenhang steht, lässt sich mit Gewissheit noch nicht feststellen[8]. In die Polizeiliche Kriminalstatistik des Jahres 2010 flossen zudem einige Umfangsver-

[4] Erläuterungen zu den Datenquellen unter 5
[5] Zahlungskarten deren Einsatz unmittelbar zur Kontobelastung führt - girocard oder so genannte ec-Karte
[6] PIN = Persönliche Geheimzahl („**P**ersonal **I**dentification **N**umber“)
[7] Mit EMV wird ein technischer Standard für die Kommunikation zwischen Chipkarte und Terminal zur Abwicklung von girocard-(ehemals ec-Karte) oder Kreditkarten-Transaktionen bezeichnet.
Auf Grundlage dieses Standards lässt sich eine Multiapplikations-Chipkarte erstellen, die die im Chip gespeicherten Daten gegen Verfälschung und auch gegen Kopieren schützt und dem Karteninhaber den Zugang zu einem breiten Spektrum unterschiedlicher Anwendungen und Dienstleistungen ermöglicht.
Der EMV-Standard ist seit dem 01.01.2011 in Europa verpflichtend.
(Quelle: https://www.kartensicherheit.de/de/pub/oeffentlich/sicherheitsprodukte/emv_chip.php)
[8] siehe dazu auch die Einschätzung des Experten der EURO Kartensysteme GmbH – Gemeinschaftsunternehmen der deutschen Kreditwirtschaft unter 2.5

fahren ein, die für die hohe Fallzahl von 7.406 mit ursächlich sein dürften. Im Langzeitvergleich der Daten ergibt sich eine Fortsetzung des steigenden Trends.

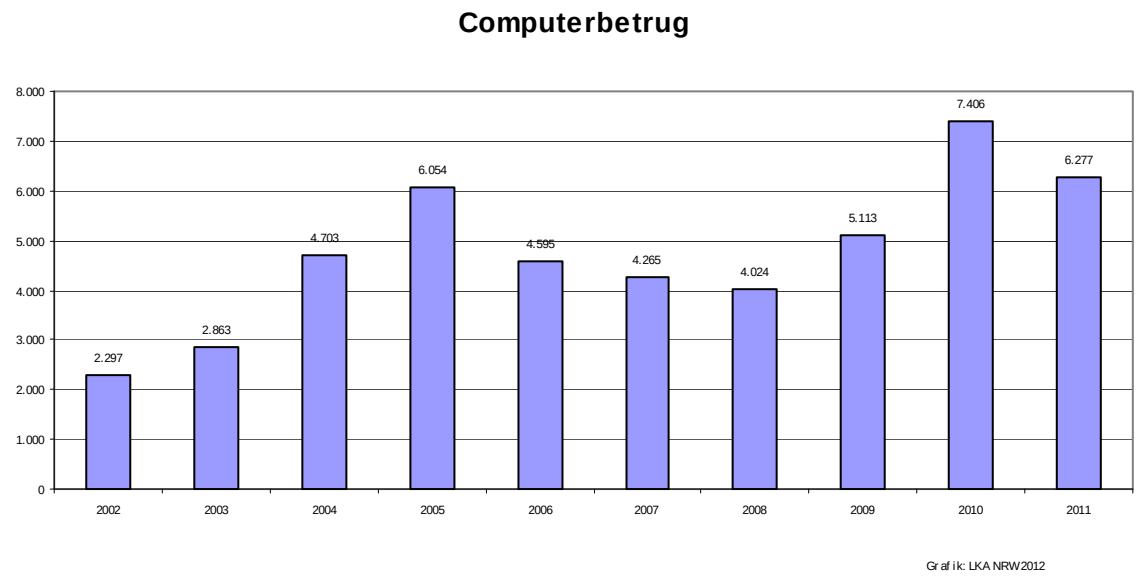

Diagramm 1: Entwicklung der Fallzahlen des Computerbetrugs

Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten

Hier sind überwiegend Fälle der Telekommunikationsanlagen-Manipulation erfasst worden. So z.B. Eindringen über Fernwartungsoptionen mit anschließenden Gesprächsvermittlungen ins Ausland oder dem Generieren von Umsätzen auf so genannte Premiumdienste, z.B. 0900-Rufnummern, zu Gunsten der Täter. Die für 2011 erfassten 881 (637) Fälle und die damit verbundene Zunahme stellt im längerfristigen Vergleich keine Auffälligkeit dar. In diesem Betrugsbereich schwanken die jährlichen Fallzahlen seit 2002 zwischen 491 Fällen (2006) und 917 Fällen (2004).

Telekommunikationsanlagen-Manipulationen werden bereits seit Jahrzehnten festgestellt. Durch neue technische Anwendungsoptionen, z.B. durch das Betreiben einer Telefonanlage in einer so genannten Cloud, könnten die Fallzahlen in diesem Phänomen weiter ansteigen. Der Trend zur Virtualisierung und Auslagerung solcher Anlagen setzt sich fort. Den Straftätern bieten sich damit neue technische Angriffsziele, verbunden mit neuen Modi Operandi und hohen illegalen Gewinnmöglichkeiten. Hiergegen müssen insbesondere die Anbieter moderner Telekommunikationsanlagen ihre Vorkehrungen ständig anpassen. Verbesserte Sicherheitssysteme und die Schulung der Administratoren oder Kunden sind die Voraussetzungen, um die weitere Entwicklung positiv zu beeinflussen.

Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei der Datenverarbeitung

Die Zunahme von 38,3 % (552 Fälle) kann auf Basis der vorliegenden Daten und Auswerteerkenntnisse nicht hinreichend erklärt werden. Eine Ursache könnte in den zunehmend greifenden Schutz- und Verhaltensmaßnahmen zur Verhinderung von erfolgreichen Phishing-Taten liegen. Sofern dadurch eine schädigende Vermögensverfügung verhindert wird, ergibt sich auch eine geänderte Erfassung in der Polizeilichen Kriminalstatistik. Statt eines erfolgreichen Computerbetrugs wird die Tat als Fälschung beweiserheblicher Daten registriert. Zu einer abschließenden Bewertung bedarf es jedoch der weiteren Beobachtung dieses Trends.

Datenveränderung, Computersabotage

Für das Jahr 2011 ist nahezu eine Verdopplung der Fallzahlen im Vergleich zum Vorjahr festzustellen (+ 715 Fälle oder 91,3 %). Hierbei spielen Angriffe mittels Schadsoftware eine zunehmende Rolle, aber auch DDoS-Angriffe[9] auf Webpräsenzen und Onlineshops haben zugenommen. Die Angriffe können durch die einfache Verfügbarkeit benutzerfreundlicher Angriffswerkzeuge auch von wenig versierten Tätern durchgeführt werden. Daneben existieren bereits ganze Angriffsnetzwerke (so genannte Bot-Netze), die von professionellen Tätergruppierungen vermietet werden. Es ist daher zu vermuten, dass diese Fälle künftig noch häufiger auftreten. Es ist von einem großen Dunkelfeld auszugehen, da betroffene Firmen Reputationsverluste befürchten und deshalb auf die Erstattung einer Strafanzeige verzichten.

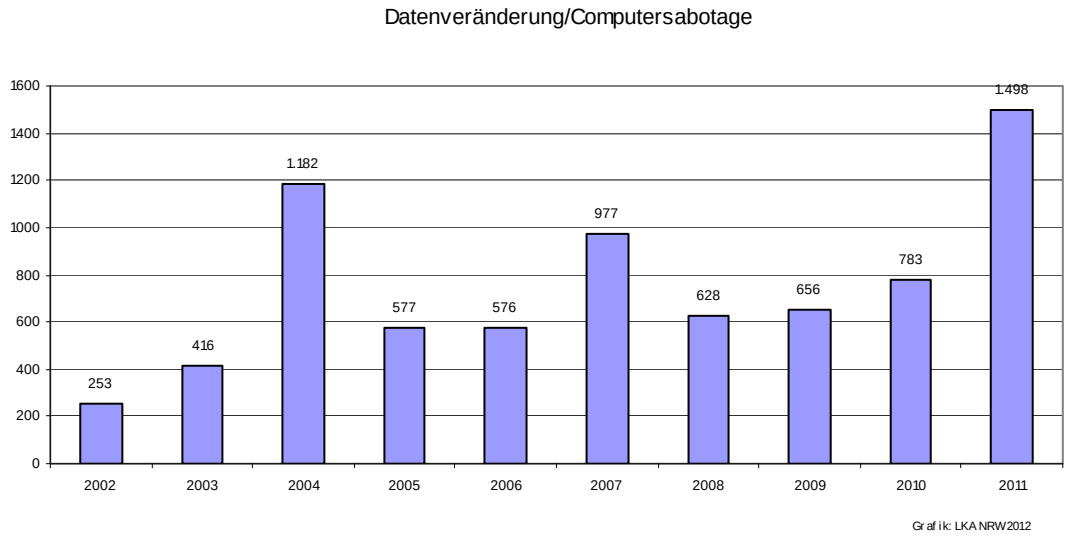

Diagramm 2: Entwicklungen der Fallzahlen der Datenveränderung/Computersabotage

Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen

Das Ausspähen von Daten (z.B. Accounts, Kreditkartendaten, Kontoinformationen) bildet den Schwerpunkt der Fallzahlen. Ursächlich für den Rückgang der Fälle im Vergleich zum Vorjahr (- 17,6 %) ist nach hiesiger Einschätzung die seit 2010 geänderte Rechtsprechung des BGH, wonach das Anbringen und der Einsatz von Skimming[10]-Technik strafrechtlich als Vorbereitung der Geld- und Wertzeichenfälschung und nicht mehr als Ausspähen von Daten zu werten ist. Dies führte zu einer veränderten Erfassung in der Polizeilichen Kriminalstatistik 2011.

Die Fallzahlen beim Skimming sind nach einem starken Anstieg im Vorjahr (von 271 in 2009 auf 1205 in 2010) deutlich rückläufig (291 Fälle in 2011). Der Austausch und die Aufrüstung der Geldautomaten mit besserer Sicherheitstechnik sowie Ermittlungserfolge (z.B. Umfangsverfahren wegen gewerbs- und bandenmäßiger Fälschung von Zahlungskarten in den Polizeipräsidien Bochum und Wuppertal) dürften dazu beigetragen haben.

[9] Distributed Denial of Service: Absichtlich herbeigeführte Serverüberlastung
[10] Skimming = englisch für „Abschöpfen“ bzw. „Absahnen“. Das Phänomen wird unter 2.5 dargestellt.

1.4 Aufklärungsquote

Die Aufklärungsquote der IuK-Kriminalität im engeren Sinne insgesamt ist im Jahr 2011 mit 24,3 % gegenüber 2010 (28,9 %) erneut gesunken. Damit setzt sich die Tendenz der sinkenden Aufklärungsquote fort. Im Jahr 2011 wurde die niedrigste Aufklärungsquote der letzten zehn Jahre erzielt.

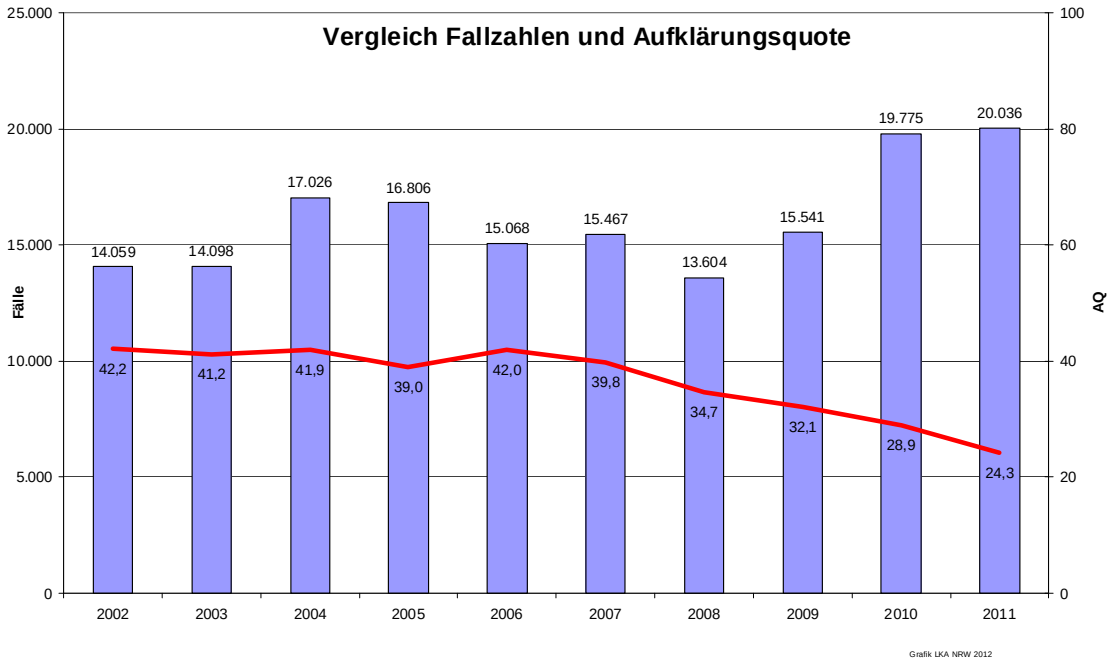

Diagramm 3: Darstellung von erfassten und aufgeklärten Fällen der IuK-Kriminalität im engeren Sinne

Die Entwicklung der Aufklärungsquote wird von verschiedenen Faktoren beeinflusst. Die registrierten Fallzahlen steigen seit 2008 stetig. Die kriminalistische Beherrschbarkeit der technischen Entwicklungssprünge mit hohen Innovationsschüben und immer kürzeren Entwicklungszyklen wird zunehmend anspruchsvoller. Die Internationalisierung und Professionalisierung der Täter hat zusätzliche Auswirkungen auf die Komplexität der Ermittlungsverfahren.

Neben diesen Faktoren wirkt sich die **fehlende Mindestdatenspeicherung** negativ auf die Aufklärungsquote aus. Für erfolgreiche Ermittlungen müssen in der Regel Verkehrsdaten vorliegen. Die Rückmeldungen aus den Polizeibehörden besagen, dass die derzeit fehlenden gesetzlichen Regelungen ein herausragendes Ermittlungshindernis bei der Bekämpfung der IuK-Kriminalität darstellen. Fehlen die Verkehrsdaten, stehen häufig keine weiteren Ermittlungsansätze zur Verfügung oder ergeben sich nur aus aufwändigen Ermittlungsprozessen. Sofern sich damit die fehlenden Verkehrsdaten überhaupt kompensieren lassen, erfordert dies doch einen erheblich höheren Zeit- und Personalansatz.

Die kriminalistischen und technischen Anforderungen an die Ermittlungsführung sind erheblich gestiegen und steigen weiter an. Polizei und Justiz müssen ihre Strategien und Prozesse sowie ihre Organisation und die Fortbildungskonzepte hierauf anpassen. Die rasante Entwicklung einer „grenzenlosen IuK-Kriminalität“ erfordert enge Kooperationen und neue Zusammenarbeitsmechanismen zwischen den Strafverfolgungsbehörden und beispielsweise der Internetwirtschaft. Die Polizei NRW hat 2011 mit der Einrichtung des IuK-Kompetenzzentrums beim LKA NRW einen erheblichen, qualitativen und personellen Schritt getan (siehe 3.3 – Organisationsentwicklung bei der Polizei NRW).

1.5 Schaden

2011 beträgt die Gesamtschadenssumme aller in der Polizeilichen Kriminalstatistik erfassten Delikte der IuK-Kriminalität im engeren Sinne 16.173.242 (19.476.211) Euro. Gegenüber dem Vorjahr ist die Gesamtschadenssumme damit um 17,0 % reduziert. Die Anzahl der Delikte, die in der Statistik mit Schadenssummen erfasst werden (Computerbetrug etc.) hat abgenommen. Delikte bei denen keine Schadenssummen erfasst werden (Datenveränderung, Computersabotage) weisen hingegen Zuwächse auf.

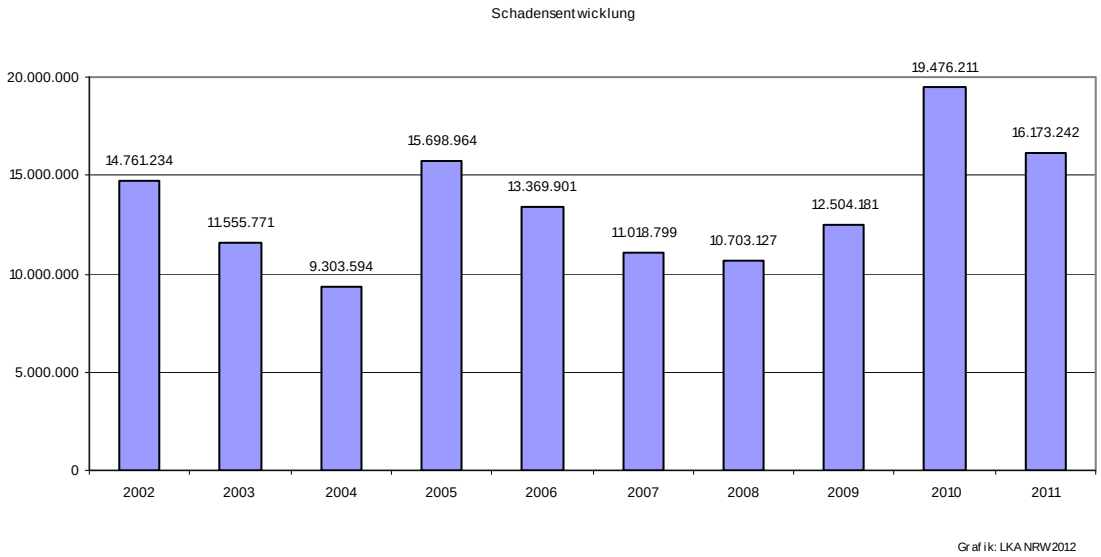

Diagramm 4: Entwicklung der Schadenssummen zur IuK-Kriminalität im engeren Sinne

1.6 Tatmittel Internet

Seit 2004 werden in der Polizeilichen Kriminalstatistik grundsätzlich alle Delikte, bei denen das Internet als Tatmittel verwendet wird, mit der Sonderkennung „Tatmittel Internet“ registriert.

Es kommen sowohl Straftaten in Betracht, in deren Zusammenhang das bloße Einstellen von Informationen in das Internet bereits Straftatbestände erfüllt (so genannte Veräußerungs- 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.[11]

Im Jahr 2011 wurden insgesamt 47.992 Straftaten unter der Sonderkennung „Tatmittel Internet“ erfasst. Das sind 3,2 % der Gesamtkriminalität (2010: 48.411 Straftaten mit einem Anteil an der Gesamtkriminalität von 3,4 %). Im Vergleich zum Vorjahr stellt dies eine Abnahme um 419 Fälle oder 0,9 % dar.

[11] 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

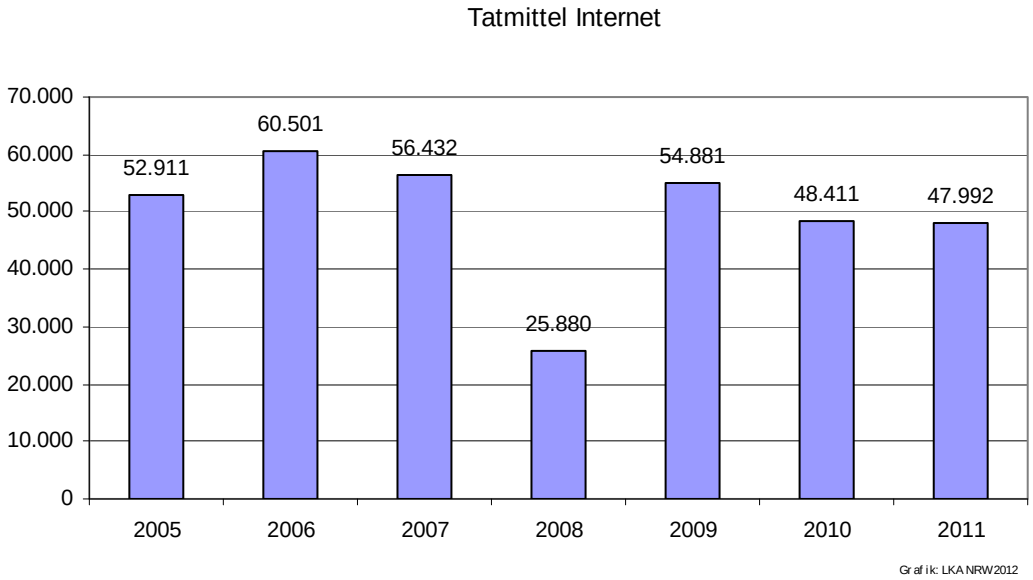

Diagramm 5: Entwicklung der Fallzahlen bei Delikten mit Sonderkennung „Tatmittel Internet“

In den vergangenen Jahren unterlag die Zahl der erfassten Fälle erheblichen Schwankungen (zwischen 25.880 Fällen im Jahr 2008 und 60.501 Fällen im Jahr 2006).

2 Darstellung und Bewertung ausgewählter Phänomene

2.1 Phishing/Identitätsdiebstahl

Phishing setzt sich aus den Begriffen password, harvesting und fishing (Passwort, abernten und fischen) zusammen. Unter Phishing versteht man eine Vielzahl möglicher technischer Angriffe und unterschiedlicher Modi Operandi. Ziel ist es, unberechtigt Passwörter und Zugangsdaten zu beispielsweise Internetauktionshäusern, -kaufhäusern, Bankkonten und Kreditkartennummern zu erlangen. Dies erfolgt häufig über Phishing-Mails, die mit plausiblen Inhalten und gelegentlich überzeugend imitierten Webseiten Vertrauen erwecken und zur Eingabe der eigenen Daten verleiten sollen.

Darüber hinaus kann über entsprechend präparierte Webseiten auch ohne eigenes Zutun Schadsoftware auf den heimischen PC geladen werden, so genannte „Drive-by-Infection“. Auf diesem Weg geben viele Rechner fortlaufend Zugangs- und Nutzungsdaten preis, ohne dass die Nutzer etwas ahnen. Nicht selten wird der infizierte Rechner oder das Smartphone damit zum Teil eines Bot-Netzes. Mit den ausgespähten Daten werden illegale Kontobewegungen und Onlinebestellungen durchgeführt sowie fremde Packstationen für illegale Warensendungen missbraucht. Kriminelle Gruppierungen entwickeln eine unüberschaubare Anzahl von neuen Schadprogrammen. Unerfahrene Täter können sich Viren und Trojaner aus Online-Baukastensystemen zusammenstellen. Daher verhindert selbst der Einsatz aktueller Antiviren-Software nicht immer den Befall des eigenen Rechners.

Thorsten Kraft

„Die deutsche Internetwirtschaft investiert jährlich Millionen für den Schutz Ihrer Kunden und den von diesen verwalteten 'Digitalen Identitäten'. Trotz dieser Anstrengungen gelingt es Cyberkriminellen jedoch immer wieder diese Sicherheitsmechanismen zu unterwandern - Cyberkriminelle sind eben immer einen Schritt voraus! Daher halten wir Aufklärungskampagnen, wie botfrei.de und DSiN (Deutschland sicher im Netz) für wichtige Ansätze um den Endkunden abzuholen und zu dem Thema Sicherheit zu sensibilisieren."

Thorsten Kraft, Senior Technical Project Manager - Anti-Botnet Beratungszentrum (eco - Verband der deutschen Internetwirtschaft e.V.)

Phishing wird häufig von professionellen, international agierenden Tätergruppen betrieben. Die Ermittlungen gestalten sich aufwändig und technisch sowie rechtlich anspruchsvoll.

Ein Beispiel – Ermittlungskommission „Katusha“

Eine internationale Bande installierte weltweit Echtzeit-Trojaner auf den PC tausender Opfer, um deren Online-Bankgeschäfte zu manipulieren. Sie führten mindestens 260 illegale Überweisungen mit einem Gesamtvolumen von 1,65 Millionen Euro aus, wovon durch eine gemeinsame Ermittlungskommission der Landeskriminalämter Nordrhein-Westfalen und Baden-Württemberg Transaktionen in Höhe von 1,2 Millionen Euro verhindert werden konnten. Alle Hauptakteure und Hintermänner wurden identifiziert und mit Unterstützung der estnischen und britischen Behörden verhaftet.

Überwachungsmaßnahmen deckten die Identität von 470 so genannten Finanzagenten auf, die sich bei Schein-Firmen als „Finanzmanager“ beworben hatten. Sie eröffneten bei unterschiedlichen Banken Konten, um eingehende Gelder abzuheben und weiterzuleiten. Gegen diese Finanzagenten wurden Strafverfahren wegen Verdachts der Geldwäsche eingeleitet. Die sechs Haupttäter aus Deutschland und Estland wurden 2011 zu mehrjährigen Haftstrafen verurteilt.

Je nach Schwerpunkt der Tat und der Tatausführung erfolgt die Erfassung von Phishing-Straftaten in der Polizeilichen Kriminalstatistik unterschiedlich, so z.B. als Ausspähen von Daten, Computerbetrug, unterschiedlichen anderen Betrugsformen oder Geldwäsche. Auf der Datenbasis des Vorgangsbearbeitungssystems der Polizei NRW ergeben sich für das vergangene Jahr 3.448 (2.056) Fälle. Seit 2005 steigen die Fallzahlen kontinuierlich.

2.2 Fake-Shops

Mit Fake-Shops werden Internetseiten bezeichnet, die einen seriösen Online-Shop vortäuschen. Die Seiten sind in der Regel professionell gestaltet, so dass die Täuschung auf den ersten Blick nicht erkennbar ist. Die Firmen bzw. im Impressum angegebene Personen sind entweder frei erfunden oder es werden Daten von ahnungslosen Personen oder Firmen missbraucht. Die in den Fake-Shops angebotenen Produkte, über die die Täter nicht verfügen, werden zumeist unterhalb des marktüblichen Preises angeboten. Die getäuschten Käufer zahlen, ohne die Ware zu erhalten. Die Täter verwenden zudem häufig die bei der Transaktion vom Käufer übermittelten Zahlungskartendaten, um damit weitere unberechtigte Verfügungen vorzunehmen, beispielsweise um Waren auf Kosten des Opfers zu bestellen.

Die Tat wird als Warenbetrug mit Tatmittel Internet erfasst und floss im Jahr 2011 mit 15.433 Fällen in die Polizeiliche Kriminalstatistik NRW ein. Wie viele Verfahren davon Fake-Shops zuzuordnen sind, lässt sich aufgrund fehlender Differenzierung in der statistischen Erfassung nicht feststellen. Gleichwohl ergeben sich Hinweise auf dieses Phänomen aus den Kriminalpolizeilichen Meldediensten und dem Vorgangsbearbeitungssystem der Polizei NRW. In einigen Fällen diente die Internetpräsenz ausschließlich dazu, unrechtmäßig Zahlungskartendaten zu erlangen. Diese sind den Straftaten Abfangen von Daten bzw. Vorbereiten des Ausspähens und Abfangens von Daten zuzuordnen. Insbesondere ausländische Täter bedienen sich so genannter Finanzagenten (vgl. „Katusha“), deren Tatbeiträge häufig als Geldwäsche gesondert in der Polizeilichen Kriminalstatistik erfasst werden.

Michael Barth

„Die Verfolgbarkeit der Täter ist sehr schwer bis nahezu unmöglich. Die ITK-Branche bewertet die Vorgänge als organisierte Kriminalität in einer Form, die die derzeit existierenden grenzüberschreitenden Prozesse der Polizeikooperation bewusst nutzt und sich zu Nutze macht. Gefasst werden aus Sicht der IT-Branche oft nur unwichtige Mittelsmänner, die sich von den Drahtziehern ausnutzen ließen.“

Michael Barth, Geschäftsführer Arbeitskreis Öffentliche Sicherheit - BITKOM

Das Internet bietet Möglichkeiten[12], die das Risiko, Opfer eines Fake-Shop Anbieters zu werden, reduzieren können. Bezahlungen per Vorkasse oder Nachnahme[13] sind dabei aus Sicht des Käufers besonders risikoreich. Der Verbraucher sollte den Onlineshop in einer Suchmaschine eingeben. Häufig verweisen im Internet andere User oder so genannte Blacklists auf einen betrügerischen Shop.

2.3 Ransomware/BKA-Trojaner

Ransomware setzt sich aus den englischen Begriffen für Lösegeld, Loskauf (Ransom) und Malware für Schadprogramm zusammen. Bei Ransomware handelt es sich um Schadprogramme. Diese verändern die Daten auf dem PC, so dass der Berechtigte nicht mehr auf diesen zugreifen kann. Eine Texteinblendung verspricht die Freigabe der Daten, sofern ein Entgelt entrichtet werde.

Eine Variante der Ransomware ist der so genannte BKA-Trojaner. Er installiert sich selbständig und vom Computernutzer zunächst unbemerkt. Insbesondere über Seiten mit pornografischen Inhalten, zum illegalen Download sowie über vermeintlich harmlose Homepages mit Kochrezepten und sozialen Netzwerken gelangt der Trojaner auf den PC. In einem Pop-Up-Fenster wird dem Anwender unterstellt, strafbare Handlungen, wie die Verbreitung kinderpornografischen Materials, begangen zu haben. Aufgrund dieser vorgeblichen Straftat sei der PC durch die Polizei gesperrt bzw. verschlüsselt worden. Nur durch eine einmalige Zahlung von z.B. 100 Euro über einen digitalen Bezahldienst wie uKash oder PaySafe[14] könne dieser wieder freigeschaltet werden. Dabei nutzen die Täter die Logos des Bundeskriminalamtes und der Bundespolizei sowie verschiedener Antiviren-Hersteller, um glaubhaft zu wirken. Trotz der Zahlung des geforderten Betrages ist eine Freigabe bisher in keinem Fall erfolgt. Der „BKA-Trojaner“ ist seit mindestens Ende März 2011 in verschiedenen Varianten bzw. Wellen eingesetzt worden. Bis zum Jahresende 2011 wurden 23 Wellen bekannt.

Bild 1: Bildschirmfoto eines Trojaners

[12] Unter dem Link http://www.kaufenmitverstand.de gibt es -7- goldene Regeln für den Online-Einkauf.

[13] Häufig erhalten die Opfer zwar ein Paket, darin befindet sich aber nicht die bestellte oder sogar gar keine Ware. Dies kann erst überprüft werden, wenn das Paket bereits angenommen und bezahlt wurde.

[14] Es handelt sich um Gutscheine, die als Prepaid-Bezahlsystem im Internet dienen und anonym im Internet eingelöst werden können.

Neben dem hier beschriebenen „BKA-Trojaner“ sind so genannte GEMA-Trojaner sowie viele weitere Varianten dieses Trojaners bekannt.

Aus der Polizeilichen Kriminalstatistik ergeben sich keine eindeutigen Fallzahlen, weil diese Straftaten überwiegend als Erpressung erfasst werden. Ein großer Anteil der Delikte (2.471 Fälle) wurde durch einen ermittelten Täter im Ausland begangen und als so genannte Auslandsstraftat nicht erfasst. Die Polizeiliche Kriminalstatistik weist daher lediglich 336 Fälle der Erpressung mit dem Tatmittel Internet aus.

Im Vorgangsbearbeitungssystem der Polizei NRW sind 5.758 Treffer erfasst[15]. Darüber hinaus gehen die Ermittlungsdienststellen von einem großen Dunkelfeld aus, da viele Opfer auf die Erstattung einer Strafanzeige verzichten.

2.4 DDoS-Angriffe

Bei einem Denial of Service-Angriff (DoS-Angriff) wird ein Server mit gezielten Anfragen regelrecht „bombardiert“. Er steht so für reguläre Anfragen nicht mehr zur Verfügung. Wird ein DoS-Angriff koordiniert und von einer größeren Anzahl anderer Systeme ausgeführt, so spricht man von einem DDoS-Angriff (Distributed Denial of Service) oder von einer verteilten Dienstblockade. Der DDoS-Angriff wird auch als Nötigungsmittel eingesetzt. Bei diesem Phänomen werden Betreiber von Online-Geschäften oder gewerblichen Internetauftritten per E-Mail aufgefordert, einen vergleichsweise geringen Betrag (150, 200, 300 bis zu 2.500 Euro) mittels eines unbaren Internetzahlungsmittels (uKash oder PaySafe) an die Täter zu zahlen. Erfolgt die Zahlung nicht bis zu einem bestimmten Zeitpunkt, wird der Internetauftritt/das Online-Geschäft angegriffen. Dies kann in kurzer Zeit zu hohen Umsatzverlusten bei den Betreibern der Internetauftritte führen, so dass einzelne Geschädigte bereit sind, das vergleichsweise geringe „Schutzgeld“ zu zahlen.

Wie beim Phänomen Phishing handelt es sich beim DoS- bzw. DDoS-Angriff nicht immer um eine eigenständige Straftat, sondern in vielen Fällen um eine Komponente einer strafbaren Handlung (z.B. Erpressung). Bei dem Angriff an sich handelt es sich strafrechtlich um eine Datenveränderung bzw. Computersabotage. Im Jahr 2011 wurden unter dem Schlagwort „DDoS“ in polizeilichen Vorgangsbearbeitungssystem 41 Fälle erfasst. Auch die DDoS-Angriffe dürften für die Steigerung der Erpressungsfälle mit Tatmittel Internet verantwortlich sein (siehe 2.3).

2.5 Angriffe durch Online-Communities

Zunehmend kam es im Jahr 2011 zu IT-Angriffen durch so genannte Online-Communities, wie z.B. der Hackergruppierung „Anonymous“ oder der „No Name Crew“. Die Communities bewerten dabei nach eigenen moralischen, ethischen oder politischen Maßstäben die Handlungen von Einzelpersonen, Behörden, Firmen oder Organisationen. Anschließend analysieren Sie deren IT-Systeme und führen Angriffe durch, um die Verfügbarkeit der Systeme einzuschränken oder Daten auszuspähen. Die Täter bemühen sich um maximale Öffentlichkeitswirksamkeit und Anerkennung. Vereinzelt kommt es auch zu so genannten Defacements, bei denen die Opfer durch Veränderungen der Webpräsenzen verunglimpft werden sollen. In einigen Fällen boten die Communities unbeteiligten Usern weltweit an, sich an den Aktionen zu beteiligen. Dazu stellten sie beispielsweise das Tool „Low Orbit Ion Canon“[16] zur Verfügung, das die Sympathisanten auf dem eigenen Rechner installieren. Die Angriffe aller beteiligten Rechner wurden dann durch Mitglieder der Community gesteuert. Die Communities kritisieren die nach ihrer Auffassung illegitime Machtausübung ihrer Opfer.

[15] Quelle: Recherche im polizeilichen Vorgangsbearbeitungssystem

[16] Im Internet verfügbare und einfach zu bedienende Software zur Teilnahme an einem DDoS-Angriff. Aktuelle Versionen lassen sich über die die Text-basierte Kommunikationsplattform „Internet Relay Chat“ (IRC) zentral steuern.

Ein Beispiel - „Operation Payback“

Als verschiedene Bezahldienste die Zusammenarbeit mit Wikileaks kündigten, rief die Gruppe „Anonymous“ zum Angriff auf deren Firmennetze auf, um die Erreichbarkeit der Internetpräsenzen einzuschränken und deren Geldfluss zu stoppen. Ein Server zur zentralen Steuerung der Angriffe befand sich in NRW. Das Landeskriminalamt NRW ermittelte wichtige Erkenntnisse über den Angriff und die Angreifer. Diese wurden den amerikanischen Ermittlungsbehörden übermittelt und führten im Anschluss zur Festnahme mehrerer Täter in den USA.

Das Landeskriminalamt NRW ermittelte im Jahr 2011 in vier derartigen Fällen. Es handelt sich um die Operationen „Servergate“, „Payback“ und „Green Rights“ der internationalen Gruppierung „Anonymous“ sowie um die Angriffe gegen das polizeiliche Ortungssystem „Patras“ durch die nationale Gruppierung „No Name Crew“. In allen Verfahren konnten Täter ermittelt werden. Im Fall der „No Name Crew“ wurden nahezu alle führenden Mitglieder identifiziert.

2.6 Skimming

Skimming steht als Synonym für das unrechtmäßige Erlangen von Zahlungskartendaten (PIN und Magnetstreifendaten) und die Herstellung eigener Zahlungskartenfälschungen für anschließende Verwertungstaten (Cashing) an ausländischen Geldautomaten. Die Täter bedienen sich unterschiedlicher Methoden. Beim „klassischen“ Skimming bringen sie eine technische Vorrichtung zum Auslesen von Magnetstreifendaten und PIN an Geldautomaten an. Vorsatzgeräte werden dabei unmittelbar vor dem Karteneinzugschlitz des Automaten befestigt, so dass beim Karteneinzug die Magnetstreifendaten unbemerkt aufgezeichnet und der eigentliche Auszahlungsvorgang nicht unterbrochen wird. Zeitgleich erfolgt die Ausspähung und Aufzeichnung der PIN-Eingabe z.B. durch Kameraleisten oberhalb des Tastaturfeldes oder über präparierte PIN-Eingabetastaturen.

Seit ca. zehn Jahren ist das Kriminalitätsphänomen Skimming bekannt. Waren es zu Beginn noch Einzelfälle, so erreichten die Skimming-Angriffe auf Geldautomaten im Jahr 2010 mit 1.205 in NRW festgestellten Fällen[17] ihren bisherigen Höchststand. Die positiven Auswirkungen eines umfangreichen Maßnahmenpakets der Zahlungskartenindustrie und der Kreditwirtschaft trugen 2011 erstmals dazu bei, den jahrelangen Negativtrend zu durchbrechen. Mit einem Rückgang der Fallzahlen um 76 Prozent im Vergleich zum Vorjahr sind für 2011 lediglich noch 291 Skimming-Angriffe auf Geldautomaten zu verzeichnen. Nach fachlicher Bewertung wird sich dieser Umkehrtrend auch 2012 weiter fortsetzen.

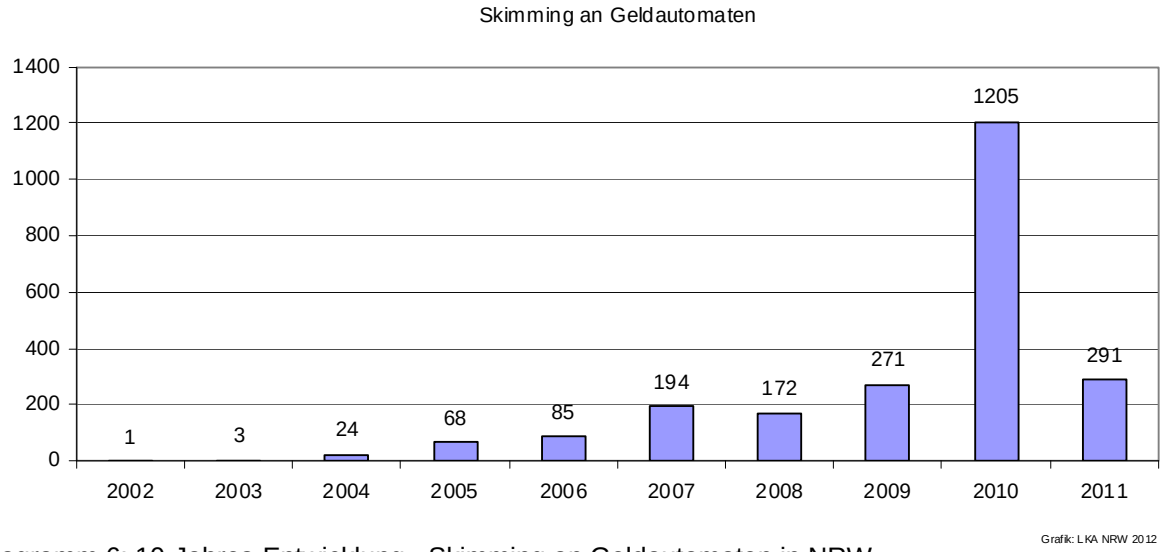

Diagramm 6: 10-Jahres-Entwicklung - Skimming an Geldautomaten in NRW

[17] Zahlenbasis = Auswertung des polizeilichen Vorgangsbearbeitungssystems

Zu den erfolgreichen Maßnahmen zählen die europaweite Umsetzung der EMV-Chip-Prüfung beim „girocard"-Einsatz an Geldautomaten und PoS-Terminals[18] sowie der Austausch oder die technische Aufrüstung veralteter Geldautomatenmodelle. Folge der EMV-Chip-Prüfung ist seit Anfang 2011 eine deutliche Verlagerung der Cashing-Taten nach Süd-, Mittel- und Nordamerika. In diesen Ländern erfolgt nach wie vor eine PIN-gestützte Zahlungskartentransaktion unter Verwendung der Magnetstreifendaten.

Hans-Werner Niklasch

„Neueste Technologiestandards und die effektive Prävention garantieren die hohe Sicherheit der deutschen Geldautomaten. Besonders erfreulich war 2011 der Rückgang der Geldautomatenmanipulationen im Inland.

Diesen Erfolg führen wir auf die flächendeckende Einführung des EMV-Standards zum 1. Januar 2011 und das massive Aufrüsten der deutschen Geldautomaten mit neuester Technik zurück. Aber auch der beschleunigte Informationsaustausch nach Feststellung einer Manipulation zwischen den beteiligten Polizeibehörden, den Banken und Sparkassen und der EURO Kartensysteme trug mit dazu bei. Eine weitere Rolle beim Rückgang der Manipulationen im Inland spielten jedoch auch zusätzliche Videoüberwachungssysteme, Aufklärungsmaßnahmen, die Außerbetriebnahme von Zugangskontrolllesern zu Foyers sowie die gezielt verstärkten Überwachungs- und Kontrollmaßnahmen innerhalb der Banken und Sparkassen, auch außerhalb der Geschäftszeiten, durch entsprechende Sicherheitsunternehmen. Hierdurch konnten Geldautomaten-Angriffe schneller erkannt und Folgemaßnahmen, wie die Übersendung der Geldautomaten-Journale zu Auswertungszwecken und die Einleitung von Sperren potenziell gefährdeter Karten, zügig veranlasst werden."

Hans-Werner Niklasch, Geschäftsführer der EURO Kartensysteme GmbH

Die Täter reagieren auf die Modernisierung der Geldautomaten mit angepassten Skimming-Geräten oder der Verlagerung zu anderen Geldautomatenmodellen. So löste die Erschwerung von Skimming an Geldautomaten im Jahr 2011 erstmals wieder ein verstärktes Interesse an alternativen Techniken PIN-basierter Debitkartenzahlungen aus. Zu den Angriffszielen zählten kundenbediente SB-Tankanlagen von Verbrauchermärkten, Fahrscheinautomaten sowie PoS-Terminals im Handel.

> Die Skimming-Angriffe auf Fahrscheinautomaten verliefen nach klassischem Muster: Zur Erlangung der Magnetstreifendaten wurde in acht bekannt gewordenen Fällen ein Vorsatzgerät am Karteneinzugsschacht angebracht und gleichzeitig die PIN mit einer Kameraleiste aufgezeichnet.
> Anders hingegen verlief die Manipulation von zwei Tankautomaten sowie von acht PoS-Terminals im Handel. Beide Systeme wurden im Innenbereich - von außen nicht erkennbar - so präpariert, dass sowohl Magnetstreifendaten wie auch PIN gespeichert wurden. Sofern nicht auf Grund technischer Störungen oder eher zufällig erkannt, ermöglichte dies den Tätern einen teils mehrwöchigen Zeitraum zur Datenerlangung. Erst mit dem plötzlichen Einsatz zahlreicher Zahlungskartendubletten an ausländischen Geldautomaten wurden diese Taten schließlich bekannt. Allein die Bilanz einer einzigen manipulierten Tankanlage im Ruhrgebiet ergab mehr als 900 Strafanzeigen sowie eine Cashing-Schadensumme von insgesamt 1,3 Mio. Euro.

Dieses Gewinnpotenzial lässt den Schluss zu, dass das Phänomen Skimming allein mit der Sicherung von Geldautomaten nicht zu beenden sein wird. Daher bedarf es auch hier einer Sensibilisierung aller Beteiligten (Betreiber und Nutzer), wie sie im Umgang mit Geldautomaten gelungen ist.
Bei den kundenbedienten Terminals des Handels (z.B. Tankanlagen oder PoS-Terminals) sind in erster Linie die Betreiber gefordert, denn für Kunden sind Manipulationen im Inneren der Geräte nicht erkennbar. Daher ist - neben regelmäßigen Sichtkontrollen - anzuraten, technische Möglichkeiten zur Störungs-

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

detektion einzusetzen. Diese sind bereits verfügbar. Zur Verhinderung von Cashing erscheint nur ein dauerhafter Verzicht auf den Magnetstreifen erfolgversprechend. Die Möglichkeiten reichen über eine vollständige Debitkarten-Transaktionssperre für Länder ohne EMV-Chip-Prüfung bis zur temporären Sperrung/Freischaltung mit oder ohne Verfügungslimit.

2.7 Cybermobbing

Unter Cybermobbing (hier wird der Begriff synonym zu Cyberbullying, E-Mobbing usw. verwendet) versteht man das Beleidigen, Bedrohen, Bloßstellen oder Belästigen anderer mit Hilfe moderner Kommunikationsmittel – meist über einen längeren Zeitraum. [19]

Diese Handlungen können in die folgenden Kategorien[20] eingeteilt werden:

- **Flaming** (Beleidigung, Beschimpfung)
- **Harassment** (Belästigung)
- **Denigration** (Anschwärzen, Gerüchte verbreiten)
- **Impersonation** (Auftreten unter falscher Identität)
- **Outing and Trickery** (Bloßstellen und Betrügerei)
- **Exclusion** (Ausschluss)
- **Cyberstalking** (fortwährende Belästigung und Verfolgung)
- **Cyberthreats** (offene Androhung von Gewalt)

Folgende Straftatbestände können erfüllt sein: Beleidigung, üble Nachrede, Verleumdung, Verletzung der Vertraulichkeit des Wortes, Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen, Nachstellen, Nötigung, Bedrohung, Erpressung, Datenveränderung und das Recht am eigenen Bild. Neben der Vielzahl möglicher Einzeldelikte erschwert die nicht einheitliche Erfassung der Sachverhalte in der Polizeilichen Kriminalstatistik eine vollständige und verlässliche Darstellung der Fallzahlen. Weitere Unschärfen entstehen auch hier durch die geringe Anzeigenbereitschaft der Opfer und das daraus resultierende Dunkelfeld. Eine Einschätzung des Dunkelfeldes lässt die Studie „Cybermobbing – definitorische Grauzone und kriminalistisches Dunkelfeld“ der Universität Münster zu (siehe auch den Expertenbeitrag weiter unten). Anlässe und Ursachen sind in der Regel im sozialen Umfeld der Täter und Opfer zu suchen. Hierbei spielen soziale Aspekte in einer Gruppe (Anerkennung; Stärkung des Gemeinschaftsgefühls; Rivalitäten), aber auch persönliche Beziehungen (Konflikte in der Klassengemeinschaft; Interkulturelle Konflikte; zerbrochene Freundschaften) und psychische Gründe (Entlastung/Ventil für Aggressionen; Reaktion aus Angst, selbst Opfer zu werden; Machtdemonstration) eine Rolle. Zudem bietet das Internet Anonymität und Sicherheit für den Täter.

[19] Quelle: http://www.klicksafe.de/themen/kommunizieren/cyber-mobbing/cyber-mobbing-was-ist-das/

[20] Willard (2007) unterscheidet acht verschiedene Ausprägungen des Cybermobbing *(aus: Gewalt im Web 2.0; Grimm, P./Rhein, S./Clausen-Muradian, E.; Hrsg: NLM, 2008)*:

Dr. Stephanie Pieschl und Dr. Torsten Porsch

Cybermobbing – definitorische Grauzone und kriminalstatistisches Dunkelfeld

Dr. Stephanie Pieschl & Dr. Torsten Porsch

„An dieser Stelle berichten wir über ausgewählte Ergebnisse (nur ein Bundesland, nur einzelne Fragen) einer unserer Studien: Im Frühjahr 2011 haben sich 1000 repräsentativ ausgewählte Schülerinnen und Schüler aus NRW im Alter von 14 bis 20 Jahren mittels strukturiertem Fragebogen telefonisch zum Thema befragen lassen (Techniker Krankenkasse, 2011). Neben demografischen Informationen und Mediennutzung wurden insbesondere ihre Erfahrungen mit Cybermobbing erfasst.

Erstens zeigt diese Studie, dass Cybermobbing ein relevantes Thema für Schülerinnen und Schüler ist. Einem Großteil der befragten Schülerinnen und Schüler (77%) ist der Begriff Cybermobbing bekannt und 57% geben an, dass Cybermobbing an ihrer Schule offiziell angesprochen wird, z.B. im Unterricht, in Workshops oder durch klare Verhaltensregeln. Mit ihren Eltern haben bereits 37% der Befragten über Cybermobbing gesprochen.

Zweitens zeigt diese Studie, dass sich zwar wenige Schülerinnen und Schüler explizit als Opfer (6 %) oder Täter (8 %) von Cybermobbing bezeichnen, dass Fragen nach konkreten Erlebnissen im Internet oder mit dem Handy aber zeigen, dass viele von ihnen (36 %) schon Aspekte von Cybermobbing erlebt haben: Es berichteten 22% der Befragten von Beleidigungen und Drohungen (Harassment), unter der Verbreitung von Gerüchten und übler Nachrede litten 15% (Denigration), 11% berichteten Identitätsmissbrauch (Impersonation), 6% wurden aus Onlinegruppen (Spiele und Chats) ausgeschlossen (Exclusion) und von 4% der Betroffenen wurden gegen Ihren Willen Informationen (Bilder, Videos, etc.) an andere weitergegeben, um Ihnen zu schaden (Outing).

Drittens zeigt diese Studie, dass die Folgen von Cybermobbing unterschiedlich ausfallen. Viele Schülerinnen und Schüler berichten von emotionalen Folgen, sie fühlen sich beispielsweise wütend, verletzt, verzweifelt oder hilflos. Schwere Fälle können eine Reihe von weiteren Folgen wie zum Beispiel schulische Probleme nach sich ziehen (Porsch & Pieschl, 2012).“

www.medienkompetenz-praevention.de

Westfälische Wilhelms-Universität Münster

Beispiele aus den erfassten Ermittlungsvorgängen:

Sacherhalt 1:

Zwei 12- und 13-jährige Jungen kopierten das Profil eines Klassenkameraden beim sozialen Netzwerk SchülerVZ. Dieses Profil nutzten die beiden, um Schul- und Klassenkameraden des Geschädigten Nachrichten mit beleidigendem Inhalt zu senden.

Sachverhalt 2:

Der jugendliche Geschädigte wurde von einem Freund auf sein Fehlverhalten gegenüber dessen Freundin angesprochen. Angeblich hatte der Geschädigte die Freundin über ein Chat-Programm sexuell belästigt. Es stellte sich heraus, dass sein Nutzerkonto gehackt worden war. Der Täter nutzte das Konto um in Videokonferenzen mit weiteren Usern aus der Freundesliste des Geschädigten eine Videochat-Kommunikation einzugehen und sich dort bei sexuellen Handlungen zeigte. Weiterhin erpresste der Täter eine weitere Bekannte des Geschädigten um sie zu veranlassen, sich zunächst vor der Webcam in Unterwäsche zu zeigen. Nachdem sie der Aufforderung gefolgt

war, erpresste er sie zu weiteren Handlungen mit der Drohung, die dabei entstandenen Bilder in einem sozialen Netzwerk zu veröffentlichen.

Sachverhalt 3:

Der ehemalige Lebensgefährte der Geschädigten veränderte nach der Trennung die Daten ihres E-Mail-Accounts, erstellte hiermit Profile bei Partnerbörsen und veröffentlichte ihre Handynummer. Außerdem stellte der Beschuldigte ihr nach, indem er sie mittels einer Instant-Messenger-Software per Webcam überwachte. Eine forensische Untersuchung des Computers ergab, dass dort eine Fernwartungssoftware installiert war, über die der Beschuldigte vollen Zugriff auf den Computer der Geschädigten hatte.

Sachverhalt 4:

Die Geschädigte nahm drei Jahre nach der Trennung wieder Kontakt zu ihrem ehemaligen Lebensgefährten auf und mischte sich in einen ihn betreffenden Streit ein. Der Beschuldigte reagierte sofort mit Drohungen gegen die Geschädigte und erstellte mit ihren Daten und einem Foto ein Nutzerprofil in einem Portal für Sexualkontakte. Hierin veröffentlichte er intime Details über die Geschädigte, die er aus der vorausgegangenen Beziehung erlangt hatte.

2.8 Kinderpornografie

Kinderpornografie sind pornografische Schriften - d. h. insbesondere Bild- und Videomaterial – die ihren Ursprung in der Dokumentation von sexuellen Missbrauchshandlungen zum Nachteil von Kindern finden und gemäß § 184 b StGB mit einem Herstellungs-, Besitz-, Beschaffungs- und Verbreitungsverbot belegt sind. Aufgrund der bevorzugten Verbreitungswege dieses Materials über das Internet und andere digitale Kommunikationsmittel sowie dem Vorliegen in digitaler Form auf Datenträgern werden diese Delikte der IuK-Kriminalität im weiteren Sinne zugerechnet. Andere Trägermedien wie z.B. analoge und Printmedien werden zwar nach wie vor im Deliktsbereich bei strafprozessualen Maßnahmen sichergestellt, spielen aber keine übergeordnete Rolle in den Fallzahlen mehr.

Die Fallzahlen in diesem Deliktsbereich sind zum Teil großen jährlichen Schwankungen unterworfen, was insbesondere auf den Zeitpunkt des Abschlusses von Umfangsverfahren mit einer Vielzahl von Einzeltaten zurückzuführen ist. Die weltweite Kommunikationsmöglichkeit über das Internet führt dazu, dass eine Vielzahl von Verbreitungshandlungen keinen Eingang in die Polizeiliche Kriminalstatistik findet, da Straftaten mit erkennbarem ausländischen Tatort nicht in der Polizeilichen Kriminalstatistik erfasst werden. Die Anzahl der bekannt gewordenen Fälle der Verbreitung von Kinderpornografie sank von 815 im Jahr 2010 um 78 oder 9,6 % auf 737 Fälle im Jahr 2011. Die international geführte Diskussion um Websperren gegen kinderpornografische Webangebote und die Bemühungen um Löschung entsprechender Inhalte könnten zu einem Verdrängungseffekt hin zu anderen Diensten des Internet bzw. Verbreitungswegen (z.B. über Handy) geführt haben.

Die Aufklärungsquote bei der Verbreitung von Kinderpornografie lag mit 64,2 % geringfügig höher als im Vorjahr (60,8 %). Auch die Anzahl der Fälle von Besitz oder Verschaffung von Kinderpornografie nahm von 688 erfassten Fällen im Jahr 2010 um 126 Fälle oder 18,3 % auf 562 Fälle ab.

Die Polizeiliche Kriminalstatistik weist darüber hinaus 13 Fälle von gewerbs- beziehungsweise bandenmäßiger Verbreitung von Kinderpornografie aus (2010: 20).

Die Tatverdächtigen in diesem Deliktsbereich sind - wie in den Vorjahren - nahezu ausschließlich männlich (96,6 %). Von den insgesamt ermittelten 954 Tatverdächtigen waren 65 (6,8 %) unter 21-Jährige (2010: 13,6 %) und 889 (93,2 %) Erwachsene (2010: 86,4 %).

2.9 Server-Hacking/SQL-Injection

Das Phänomen SQL-Injection[21] ist eine Variante des Server-Hackings. Bei einer SQL-Injection werden Sicherheitslücken in SQL-Datenbanken ausgenutzt. Der Angreifer versucht dabei, eigene SQL-Befehle in einer Datenbank ausführen zu lassen, um Zugriffsrechte zu erlangen, Daten auszuspähen, zu verändern oder zu löschen. Eine SQL-Injection wird durch Fehler in der Konfiguration von Servern und Datenbanken, durch Programmierfehler in Webseiten aber auch durch fehlende Sicherheitsupdates der entsprechenden Anwendungen ermöglicht.

Olaf Siemens

„SQL-Injection ist nach unserer Erfahrung die häufigste Sicherheitslücke in Web-Anwendungen, die unmittelbar zum Verlust von vertraulichen oder personenbezogenen Informationen oder sogar zum Einbruch in ein System führen kann. SQL-Injection-Schwachstellen sind dabei fast immer mit gängigen Werkzeugen ausnutzbar, um an Daten aus der verwendeten Datenbank zu gelangen. Unternehmen sollten beteiligte Entwickler entsprechend schulen und das Thema Sicherheit und sichere Softwareentwicklung von Beginn an in Softwareprojekte einfließen lassen. Es muss sichergestellt werden, dass entsprechende Richtlinien bei der Programmierung (z.B. Eingabevalidierung und Verwendung von Prepared Statements) durchgängig von den Entwicklern angewendet werden."

Olaf Siemens, Geschäftsführer TÜV Rheinland i-sec GmbH

Zur Verhinderung von SQL-Injections müssen alle verfügbaren Sicherheitsupdates (Patches) installiert sein. Die Einhaltung der IT-Grundschutz-Kataloge des BSI[22] sollten als Mindeststandard beachtet werden.

SQL-Injections werden u. a. statistisch als Ausspähen von Daten, Datenveränderung/Computersabotage oder Erpressung erfasst. So können aus der Polizeilichen Kriminalstatistik keine konkreten Fallzahlen entnommen werden. Im Kriminalpolizeilichen Meldedienst sind für den gesamten Bereich Hacking 41 Fälle gemeldet. Es ist jedoch davon auszugehen, dass viele geschädigte Firmen und Behörden aus Sorge um eine Rufschädigung auf eine Anzeigenerstattung verzichtet haben. Aufgrund fehlender forensischer Auswertungen von betroffenen Systemen ist davon auszugehen, dass SQL-Injections häufig unbemerkt bleiben.

3 Initiativen

3.1 Organisationsentwicklung bei der Polizei NRW

Das Ministerium für Inneres und Kommunales hat auf die in diesem Lagebild beschriebenen veränderten Bedingungen mit einer Neuorganisation der IuK-Kriminalitätsbekämpfung durch die Einrichtung des IuK-Kompetenzzentrums beim Landeskriminalamt NRW reagiert und darüber hinaus am 29. Februar 2012 Zuständigkeiten und Abläufe in allen Kreispolizeibehörden angepasst.

Im IuK-Kompetenzzentrum sollen bis Ende 2012 mehr als 100 Spezialisten für die Bekämpfung der IuK-Kriminalität in einer Organisationseinheit wirken. Hier werden seit November 2011 komplexe Ermittlungsverfahren geführt, Präventionskonzepte sowie Kriminalitätsanalysen erstellt und die Kreispolizeibehörden in besonders komplexen Ermittlungsverfahren unterstützt. Das Landeskriminalamt NRW ist zudem als Single Point of Contact (SPoC) Ansprechpartner für Polizeibehörden, Justiz, Forschung und Lehre, die Wirtschaft sowie für die Bürger des Landes NRW. Für die kompetente Betreuung und die sofortige Einleitung komplexer Ermittlungsmaßnahmen ist der SPoC rund um die Uhr erreichbar.

[21] SQL - abgeleitet aus der Vorgängerbezeichnung SEQUEL - ist eine verbreitete Datenbanksprache zum Bearbeiten und Abfragen von Datenbeständen in relationalen Datenbanken.
[22] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html

In den Kreispolizeibehörden befassen sich in Nordrhein-Westfalen ca. 400 Spezialisten mit der Bekämpfung der IuK-Kriminalität. Zusätzlich werden im Jahr 2012 weitere Ingenieure und Informatiker eingestellt. Die Qualifizierung der Spezialisten erfolgt durch ein umfangreiches, zielgruppenorientiertes Fortbildungsangebot des Landesamtes für Aus- und Fortbildung und Personalangelegenheiten der Polizei (LAFP) NRW.

3.2 Kooperation LKA NRW und BITKOM

Am 8. November 2011 wurde ein Kooperationsvertrag zwischen dem Bundesverband Informationswirtschaft, Telekommunikation und Neue Medien (BITKOM) e.V. und dem LKA NRW unterzeichnet. Die Zusammenarbeit zielt darauf ab, in Wirtschaft und Sicherheitsbehörden den Informationsaustausch und Wissenstransfer über technologische Entwicklungen und aktuelle Kriminalitätsphänomene nachhaltig zu fördern, Präventionsmaßnahmen zu entwickeln und umzusetzen sowie frühzeitig neuen Erscheinungsformen der IuK-Kriminalität zu begegnen. Der Erreichung dieser Ziele dienen gemeinsame Aktivitäten in den Kooperationsfeldern:

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

3.3 Prävention

Polizeiliche Kriminalprävention im Zusammenhang mit IuK-Kriminalität konzentriert sich auf verhaltensorientierte Ansätze. Diese werden insbesondere in der Öffentlichkeitsarbeit und Multiplikatorenschulung vermittelt, um ein sicherheitsbewusstes Verhalten im Umgang mit Medien zu erreichen. Zielgruppen sind sowohl Kinder und Jugendliche (Jugendmedienschutz) als auch Erwachsene (z.B. Eltern, Lehrerinnen und Lehrer).

Die vorhandenen Kompetenzen sollen gebündelt, die Akzeptanz von Informationsangeboten staatlicher und privater Stellen mit Präventionsanliegen erhöht und Kooperationen zwischen unterschiedlichen Trägern angestrebt werden. Die Kommission Kriminalitätsbekämpfung[23] befasst sich seit 2009 mit dem Vorhaben, Kräfte wirkungsvoll und gezielt zu bündeln. Die Projektgruppe „Mediensicherheit“ der Kommission Polizeiliche Kriminalprävention (KPK) greift dieses Vorhaben seit 2010 auf. Vor diesem Hintergrund strebt die Projektgruppe eine Zusammenarbeit mit der EU-Initiative „klicksafe“ sowie dem Bundesamt für Sicherheit in der Informationstechnik (BSI) an.

Projekte und Netzwerke - Beispiele

„**Webrespect**“ ist eine seit April 2011 bestehende Präventionsinitiative des Kompetenzteams Köln und des Polizeipräsidiums Köln gegen „Cybermobbing/Cyberbullying“ und den daraus resultierenden rechtlichen, sozialen und persönlichen Problemstellungen.

„**CyberCops**“ ist ein 2007 gegründetes Kooperationsprojekt unter Beteiligung der Polizei Minden-Lübbecke, dem Kinderschutzbund, der örtlichen Drogenberatungsstelle und weiteren sozialen Partnern. Schülerinnen und Schüler im Kreisgebiet sollen nach einer ziel- und fachgerechten Schulung als Multiplikatoren in ihrer „Peer-Group“ Medienkompetenzen und präventive Ansätze bei der Nutzung der IuK-Technik, insbesondere des Internets, weitergeben.

In dem Netzwerk "**Surfen mit SIN(N) - Sicherheit im Netz**" arbeiten in Bielefeld unter der Federführung des Sozial- und Kriminalpräventiven Rates der Stadt Bielefeld (SKPR) mehrere Einrichtungen zusammen. Die Schirmherrschaft liegt beim Oberbürgermeister, der Polizeipräsidentin und einem Vertreter der Uni-

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

versität Bielefeld. Das Medienzentrum, das Kompetenzteam und das Kommissariat Kriminalprävention/Opferschutz arbeiten in drei Säulen mit Eltern, Lehrern und Schülern aller Bielefelder Schulen zum Thema "Chancen und Risiken des Internets" zusammen. Die Arbeit wird unterstützt von weiteren Netzwerkpartnern aus allen gesellschaftlichen Bereichen.

Wanderausstellung "**Internet – Ort der unbegrenzten Möglichkeiten!?**". Die von der Kreispolizeibehörde Paderborn und dem „Verein zur Förderung der kommunalen Kriminalprävention in Paderborn e.V." konzipierte Wanderausstellung richtet sich an den privaten IT-Nutzer. Neben den Möglichkeiten der technischen Absicherung stehen verhaltenspräventive Informationen im Vordergrund.

Das **IuK-Kompetenzzentrum** des Landeskriminalamts NRW unterstützt mit konkreten Maßnahmen den **Landespräventionsrat NRW**. Durch umfangreiche Vortragstätigkeiten vor Führungskräften und Entscheidungsträgern der Polizei, Justiz, Politik und Wirtschaft soll das Gefahrenbewusstsein verbessert werden. Eine erfolgreiche Bekämpfung der IuK-Kriminalität setzt die Unterstützung aller wesentlichen Akteure voraus. Dazu ist eine Grundlagenarbeit erforderlich, in die sich auch die Polizei NRW einbringt. Die Spezialisten beteiligen sich an nationalen und internationalen Forschungs-Projekten (z.B. Bildzuordnungstechnologien im Bereich der Kinderpornografie in den Projekten „INBEKI" und „ICOP"), um die präventiven und repressiven polizeilichen Potenziale zu optimieren.

Cybermobbing

Die Fähigkeit, Chancen und Risiken des Internets richtig einzuschätzen und verantwortungsbewusst damit umzugehen, wird neben anderen Aspekten unter der Bezeichnung „Medienkompetenz" erfasst.

Die Vermittlung von Medienkompetenz obliegt weitgehend den Pädagogen und wird von Seiten der Polizei durch Multiplikatorenschulungen unterstützt.

Ziele der Maßnahmen sind neben dem sicheren Umgang mit Medien:

- die allgemeine Stärkung des Selbstbewusstseins von Kindern und Jugendlichen
- die Schaffung eines Problembewusstseins bei den Tätern
- die Sensibilisierung der Gesellschaft
- die Steigerung der Selbstachtung, des Durchsetzungsvermögens sowie der Eigen- und Mitverantwortlichkeit.

Dr. Stephanie Pieschl und Dr. Torsten Porsch

„Kommt es zu Cybermobbing muss von den Betroffenen und deren Umfeld adäquat reagiert werden. Das zentrale Mittel zur Eindämmung muss, aus unserer Sicht, die Prävention sein. Neben allgemeiner Aufklärung über Gefahren im Internet ist es zweckmäßig, zielgruppengerechte Maßnahmen durchzuführen die speziell der Prävention von Cybermobbing dienen, beispielsweise indem sie die (kritische und ethische) Medienkompetenz der Schülerinnen und Schüler stärken. Dazu haben wir mit dem Programm „Surf-Fair" einen Vorschlag gemacht, der sich in der Präventionsarbeit mit Kindern und Jugendlichen einsetzen lässt und sich in der Praxis bewährt hat (Pieschl & Porsch, 2012)."

www.medienkompetenz-praevention.de

Westfälische Wilhelms-Universität Münster

Weitere empfehlenswerte Informationen

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 BSI www.bsi.de oder www.bsi-fuer-buerger.de, die Landesanstalt für Medien NRW www.lfm-nrw.de, die Initiativen „Schulen ans Netz e. V." www.schulen-ans-netz.de, „SCHAU-HIN" www.schau-hin.info und „klicksafe.de" www.klicksafe.de bieten empfehlenswerte Informationen und Angebote rund um das Thema IuK-Kriminalität und Mediensicherheit.

4 Fazit und Prognose

Die Polizeiliche Kriminalstatistik beantwortet nicht alle Fragen im Hinblick auf die Entwicklung der IuK-Kriminalität. Zu schnelllebig ist die Technik, zu vielfältig sind die Modi Operandi und die Phänomene, als dass sie sich statistisch eindeutig in die Kategorien des materiellen Rechts – also die Straftatbestände – einordnen ließen. Auch wenn ergänzend auf alle zur Verfügung stehenden Daten des Kriminalpolizeilichen Meldedienstes und der Vorgangsbearbeitungssysteme zurückgegriffen wird, bleibt das Bild nicht selten ungenau. Wie in anderen Kriminalitätsfeldern existiert auch bei der IuK-Kriminalität eine Differenz zwischen den polizeilich erfassten Fällen und dem tatsächlichen Kriminalitätsgeschehen. Die Erforschung und Reduzierung dieses Dunkelfelds hat sich u. a. die Kooperation zwischen dem BITKOM und dem Landeskriminalamt NRW zum Ziel gesetzt. Darüber hinaus hatten erstmalig externe Experten Gelegenheit, ergänzende Informationen und Bewertungen zum Lagebild IuK-Kriminalität beizutragen.

In einer Einschätzung sind sich alle Experten sicher: Die bisherigen Statistiken zeigen nur „die Spitze des Eisbergs“.

Dennoch lassen sich einige prägnante Aussagen treffen:

- Die Fallzahlen der registrierten IuK-Kriminalität im engeren Sinne[24] steigen erstmals seit 2002 wieder über 20.000.
- Erpressungen mit Tatmittel Internet nehmen bei kleiner Zahl, aber vermutetem großem Dunkelfeld, stark zu.
- Im Phänomen Skimming sind die Fallzahlen gegenüber dem Vorjahr stark rückläufig; technische Sicherungsmaßnahmen der Entwicklungs- und Vertriebsfirmen sowie Ermittlungserfolge der Polizei haben hierzu beigetragen.
- Die Polizei NRW verzeichnet die niedrigste Aufklärungsquote seit Erfassung der IuK-Kriminalität im engeren Sinne im Jahr 1987; darauf wurde bereits im Jahr 2011 mit verschiedenen Maßnahmen reagiert (z.B. IuK-Kompetenzzentrum; Erlass des Ministeriums für Inneres und Kommunales zur Bekämpfung der IuK-Kriminalität; Kooperation mit der IT-Wirtschaft).
- Die Fallzahlen bei den Straftaten Datenveränderung und Computersabotage haben sich nahezu verdoppelt.

Der Anwender wird trotz aller polizeilichen und gesellschaftlichen Maßnahmen auch in Zukunft den beschriebenen Gefahren ausgesetzt sein. Er muss damit rechnen, dass sein PC durch Schadsoftware infiziert wird und seine Daten ausgespäht werden. Er kann gemobbt und seine Konten können geplündert werden. In Fake-Shops wird er zur Kasse gebeten, ohne die Ware zu erhalten. Gegen viele Angriffe kann sich ein durchschnittlich informierter Anwender auch mit seiner folgsam installierten Firewall oder seinem Anti-Virenprogramm nur unzureichend schützen. Experteneinschätzungen gehen davon aus, dass mindestens 25 Prozent aller PC mit Schadsoftware verseucht sind.[25] Dennoch wiegen die Vorzüge und Vorteile des Internets diese Nachteile auf. Bisher denken nur wenige User ernsthaft darüber nach, auf das Internet zu verzichten.

Neben der Massenkriminalität im Internet sind neue, schwere Kriminalitätsformen entstanden, die spezifisches Know-how erfordern, z.B. Datenausspähung und Datensabotage, Computerbetrug, Identitätsdiebstahl oder digitale Schutzgelderpressung. Sie gehen einher mit Phänomenen wie Skimming, Phishing, Carding[26], dem massenhaften Einsatz von Schadsoftware, dem Aufbau sowie Betrieb von Botnetzen und

[24] Informationen zur Definition und Abgrenzung finden Sie unter 5.1
[25] Mit der Anwendung „QuickScan“ der Firma BitDefender sollen Anwender ihre Rechner online in knapp einer Minute kostenlos auf Schadsoftware prüfen können. Im Rahmen der Betatest-Phase wurden mit dem Tool rund 2,3 Millionen Computer überprüft. 30 Prozent davon waren mit Schadsoftware verseucht. Quelle: BitDefender GmbH
[26] Unter Carding versteht man den missbräuchlichen Einsatz von Zahlungskartendaten (überwiegend Kreditkartendaten)

der Ausführung von DDoS-Angriffen. Die Polizeiliche Kriminalstatistik gibt die Wachstumsraten auch hier nur unzureichend wieder.

Charakteristika dieser schweren Formen der profitorientierten Internetkriminalität sind die permanente Fortentwicklung krimineller Geschäftsideen, ausgerichtet an profitorientierten Marktmechanismen, eine hohe und wachsende Professionalität und Anonymität sowie ein internationales Zusammenwirken von Tatbeteiligten. Es hat sich eine ausgeprägte Underground-Economy entwickelt, in der man gleich einem Baukastensystem alles für die kriminelle Geschäftsidee kaufen oder mieten kann, z.B. Daten, Karten, Trojaner, Schadsoftware, IT-Infrastruktur und IT-Know-how sowie spezifische Service-Level. Dies verdeutlicht einen anderen, neuen Typus des kriminellen Akteurs.

Ein weiteres Phänomen der digitalen Welt sind das rasche Entstehen und Wachsen von Cybercommunities. Sie verstehen sich als eine neue Macht - als Protestbewegung in einer neuen digitalen Welt, gegen „verkrustete alte“ Strukturen aufbegehrend, oft mit zunächst ethisch-moralischem Anspruch, dann mit eigener Ideologie, eigenen Regeln, eigener Werteordnung und zunehmend mit einer abgehobenen Arroganz angeblich legitimer Macht. Ihre Aktivitäten – DDoS-Angriffe, Hackerangriffe und Datendiebstähle – gehen über einen „Schabernack“ oder legitime demonstrative Aktionen weit hinaus. Sie nutzen – wenn auch mit anderer Motivation – die gleichen Mittel wie profitorientierte Kriminelle, verwirklichen die gleichen Straftatbestände und verursachen in gleicher Weise wirtschaftliche Schäden. In ihrem Zielspektrum liegen mit wechselnder Ausrichtung Großunternehmen, Sicherheitsbehörden und andere staatliche Stellen , die für ihre Aktivitäten „abgestraft“ oder in ihrer Tätigkeit gestört werden sollen. Festzustellen sind Tendenzen einer Radikalisierung im Einsatz der Mittel und der beabsichtigten oder in Kauf genommenen Schäden, in Einzelfällen auch profitorientierte allgemeinkriminelle Aktivitäten von Angehörigen der Communities.

Bei zunehmender Radikalisierung der Gruppierungen besteht die Möglichkeit, dass noch wirksamere Angriffe durchgeführt werden, die schwerwiegende Folgen für das Wirtschaftsleben oder die Handlungsfähigkeit von Behörden haben könnten. Letztlich könnte auch kritische Infrastruktur in den Fokus der Täter geraten. Diese Tendenz gilt es zu beobachten. Präventive Ansätze sind aufgrund der Abschottung der Gruppierung sowie aufgrund der unscharfen Zugehörigkeit zu solchen Gruppen in den Erfolgsaussichten begrenzt. Erfolgreiche Ermittlungen und Verurteilungen der Täter jedoch entfalten auch präventive Wirkung.

Diesen Entwicklungen werden sich moderne und leistungsfähige Polizeiorganisationen im Zusammenwirken mit staatlichen und nichtstaatlichen Partnern stellen müssen. Die Polizei NRW hat hierzu mit strukturellen und personellen Verbesserungen zukunftsweisende Schritte unternommen und Ermittlungserfolge erzielt.

5 Begriffsbestimmungen und Anlagen

5.1 Definitionen

IuK-Kriminalität/Cybercrime [27]

IuK-Kriminalität ist Kriminalität unter Nutzung von Informations- und Kommunikationstechnik. Delikte der IuK-Kriminalität werden nach IuK-Kriminalität im engeren Sinne und IuK-Kriminalität im weiteren Sinne unterschieden. IuK-Kriminalität ist dem international gebräuchlichen Begriff „Cybercrime“ gleichzusetzen.

IuK-Kriminalität im engeren Sinne

Die IuK-Kriminalität 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. Vorbreitungshandlungen gem. §§ 202 a, 202 b und 202 c StGB[28]
- Softwarepiraterie (privates Handeln)
- Softwarepiraterie (gewerbsmäßiges Handeln)
- Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten

IuK-Kriminalität im weiteren Sinne

IuK-Kriminalität im weiteren Sinne bezeichnet alle Straftaten, bei denen die Informations- und Kommunikationstechnik zur Planung, Vorbereitung oder Ausführung eingesetzt wird. Diese erstrecken sich mittlerweile auf nahezu alle Deliktsbereiche.

Bot-Netz

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 so genannten „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.

[27] Die Definitionen beruhen auf dem 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 (Bekämpfung der IuK-Kriminalität)“

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

5.2 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 LKA NRW beauftragt, ein spezifisches jährliches Lagebild 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.

5.3 Datenbasis

Grundlage dieses Lagebildes sind Daten aus der Polizeilichen Kriminalstatistik, Sachverhalte aus dem polizeilichen Vorgangsbearbeitungssystem und dem Kriminalpolizeilichen Meldedienst-IuK.

In der Polizeilichen Kriminalstatistik werden unter dem Summenschlüssel 897000 nur die Delikte der IuK-Kriminalität im engeren Sinne zusammengefasst (siehe Nr. 5.1). Die Daten der Polizeilichen Kriminalstatistik ergeben kein wirklichkeitsgetreues Abbild der IuK-Kriminalität in ihrer kriminologischen Gesamtheit, da die Straftaten der IuK-Kriminalität im weiteren Sinne, wie z.B. Betrugsdelikte im Zusammenhang mit Online-Auktionshäusern, Beleidigungsdelikte oder Urheberrechtsverletzungen nur unter ihrem Grundtatbestand erfasst werden.

Im Kriminalpolizeilichen Meldedienst-IuK melden die Polizeibehörden folgende Straftaten der IuK-Kriminalität 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, 348 StGB — Falschbeurkundung/Urkundenunterdrückung im Zusammenhang mit Datenverarbeitung
- § 303 a StGB — Datenveränderung
- § 303 b StGB — Computersabotage

Während sich aus der Polizeilichen Kriminalstatistik nur wenige Angaben zu der einzelnen Straftat entnehmen lassen, bietet der Kriminalpolizeiliche Meldedienst-IuK die Möglichkeit einer differenzierten Auswertung von Informationen zur Phänomenologie einzelner Delikte.

Um neue Tatbegehungsformen der IuK-Kriminalität zeitnah erkennen zu können, bietet der Kriminalpolizeiliche Meldedienst-IuK 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.

Auch die Daten aus dem Kriminalpolizeilichen Meldedienst-IuK ergeben keine umfassende Datenbasis polizeilich bekannt gewordener IuK-Kriminalität im engeren Sinne, da ein Vergleich zeigt, dass nicht alle in der Polizeilichen Kriminalstatistik erfassten Straftaten im Meldedienst erscheinen.

Aus diesem Grunde wurde im Jahr 2010 auf eine Auswertung im polizeilichen Vorgangsbearbeitungssystem umgestellt. Das Vorgangsbearbeitungsprogramm enthält die Grunddaten aller bei der Polizei NRW bearbeiteten Strafermittlungsvorgänge. Der Kriminalpolizeiliche Meldedienst-IuK wird aus dem polizeilichen Vorgangsbearbeitungssystem generiert und von den Sachbearbeitern hinsichtlich der Phänomenbeschreibungen vervollständigt.

Insofern stammen die aufgeführten Zahlen aus dem polizeilichen Vorgangsbearbeitungssystem und die Phänomenbeschreibungen aus dem Kriminalpolizeilichen Meldedienst-IuK.

5.4 Tabellen

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

	Delikte		Zu- bzw. Abnahme	
	2010	2011		%
Computerbetrug	7.406	6.277	- 1.129	- 15,2
Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung	1.442	1.994	+ 552	+ 38,3
Datenveränderung/ Computersabotage	783	1.498	+ 715	+ 91,3
Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen	3.954	3.257	- 697	- 17,6
Betrug mittels rechtswidrig erlangter Debitkarte mit PIN	5.511	6.108	+ 597	+ 10,8
Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten	637	881	+ 224	+ 38,3
Softwarepiraterie private Anwendung	34	12	- 22	- 64,7
Softwarepiraterie gewerbsmäßiges Handeln	8	9	+ 1	+ 12,5
Computerkriminalität insgesamt	19.775	20.036	+ 261	+ 1,3

Tabelle 2: Aufklärungsquoten

	aufgeklärte Fälle		Aufklärungsquote %		Zu- bzw. Abnahme
	2010	2011	2010	2011	% - Punkte
Computerbetrug	2100	1369	28,4	21,8	- 6,6
Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung	634	740	44,0	37,1	- 6,9
Datenveränderung / Computersabotage	197	224	25,2	15,0	- 10,2
Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen	604	456	15,3	14,0	- 1,3
Betrug mittels rechtswidrig erlangter Debitkarte mit PIN	1 .880	1.884	34,1	30,2	- 3,9
Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten	259	227	40,7	25,8	- 14,9
Softwarepiraterie private Anwendung	28	11	82,4	91,7	+ 9,3
Softwarepiraterie gewerbsmäßiges Handeln	8	6	100,0	66,7	- 33,3
Computerkriminalität insgesamt	5.710	4.877	28,9	24,3	- 4,5

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

Tabelle 4: Entwicklung der 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 %	
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

Tabelle 5: Tatmittel Internet

Tatmittel Internet			
	erfasste Fälle	darunter	
	insgesamt	Tatmittel Internet	
	2011	absolut	Anteil %
Straftaten insgesamt	**1.511.469**	**47.992**	**3,2**
Straftaten gegen die sexuelle Selbstbestimmung	10.957	1.156	10,6
- Verbreitung pornografischer Erzeugnisse	1.800	1.096	60,9
darunter:			
- Besitz/Verschaffen von Kinderpornografie	737	514	69,7
- Verbreitung von Kinderpornografie	562	313	55,7
Betrug	236.830	37.923	16,0
darunter:			
- Waren- und Warenkreditbetrug	72.423	23.661	32,7
- Computerbetrug	6.277	5.938	94,6
- Betrug mit Zugangsdaten zu Kommunikationsdiensten	881	269	30,5
Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung	1.994	1.515	76,0
Datenveränderung, Computersabotage	1.498	1.393	93,0
Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen	3.257	2.718	83,5
Erpressung	1.963	336	17,1

5.5 Ansprechpartner/ergänzende Hinweise

Landeskriminalamt Nordrhein-Westfalen
Abteilung 4
Dezernat 41
Zentrale Ansprechstelle IuK-Kriminalität
0211-939-4040
Cybercrime.Lka@polizei.nrw.de

Weitere Informationen für Polizeibedienstete im Intrapol NRW:
http://intrapol.polizei.nrw.de/Kriminalitaet/Delikte/IuKKrim/Seiten/default.aspx

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