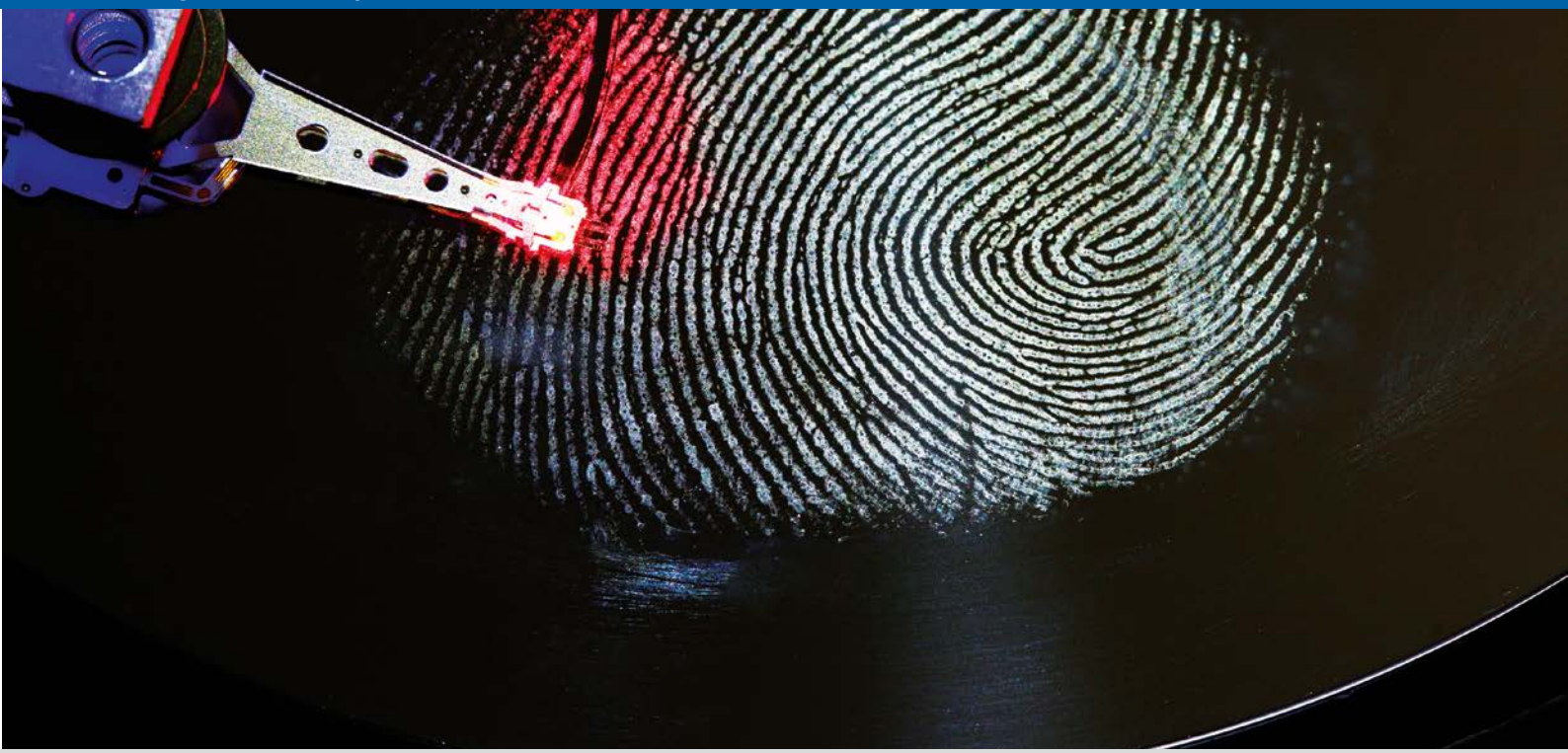
POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

bürgerorientiert · professionell · rechtsstaatlich



Cybercrime
Lagebild 2014

Kriminalitätsentwicklung im Überblick

Cybercrime in NRW – Entwicklung und Bewertung

- **Allgemeiner Rückgang der Fälle durch Änderung der Erfassungsrichtlinien in der Polizeilichen Kriminalstatistik**
- **Weiterer Anstieg der Fälle von Betrug mit Tatmittel Internet**
- **Rückgang der Fälle von Erpressung mit Tatmittel Internet**

	2013	2014	in %	Tendenz
Cybercrime im engeren Sinne	**27 016**	**20 715**	**- 23,3**	↘
Computerbetrug	6 774	6 026	- 11,0	↘
Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei der Datenverarbeitung	3 121	2 625	- 15,9	↘
Datenveränderung/Computersabotage	6 713	2 884	- 57,0	↘
Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen gem. §§ 202a, 202b, 202c StGB	5 486	4 381	- 20,1	↘
Betrug mittels rechtswidrig erlangter Debitkarten mit PIN	4 553	4 467	- 1,9	↘
Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten	319	296	- 7,2	↘
Straftaten mit Tatmittel Internet	**70 981**	**67 384**	**- 5,1**	↘
Betrug mit Tatmittel Internet	45 751	48 343	+ 5,7	↗
Erpressung mit Tatmittel Internet	1 981	514	- 74,1	↘
Anzahl der aufgeklärten Fälle mit Tatmittel Internet	35 810	37 558	+ 4,9	↗

Inhalt

1 Lagedarstellung

1.1 Vorbemerkungen

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 steht im Einklang mit internationalen Begriffsbestimmungen wie der Convention on Cybercrime des Europarats[1].

Cybercrime im engeren Sinne umfasst Straftaten, bei denen die elektronische Datenverarbeitung eine tatbestandliche Voraussetzung für die Begehung der Straftat ist. Dazu zählen:

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

Das Lagebild Cybercrime stellt im Schwerpunkt die Entwicklung der Cybercrime im engeren Sinne im Land Nordrhein-Westfalen dar. Die Daten basieren auf Ermittlungsverfahren der Polizeibehörden in NRW, die nach einheitlichem Standard erhoben werden. Die im Überblick dargestellten und unter Nr. 1 näher erläuterten Zahlen beruhen auf Daten der Polizeilichen Kriminalstatistik (PKS). Einzelne Delikte, die mit Hilfe des Tatmittels Internet begangen werden, werden unter Nr. 1.6 gesondert dargestellt. Klammerwerte bei Zahlenangaben beziehen sich, soweit nicht anders angegeben, auf das Vorjahr. In einzelnen Phänomenen ist von einem großen Dunkelfeld auszugehen, da der Polizei viele Straftaten nicht bekannt bzw. nicht zur Anzeige gebracht werden.

In der PKS ist die Anzahl der auf Cybercrime entfallenden Straftaten für das Jahr 2014 gegenüber den Vorjahren deutlich geringer, zugleich sind die Aufklärungsquoten gestiegen. Diese statistischen Aussagen sind zu einem wesentlichen Teil auf veränderte Erfassungsmodalitäten in der PKS zurückzuführen. Bis einschließlich 2013 erfasste die Mehrzahl der Länder Cybercrimedelikte mit einem Schadenseintritt in Deutschland (beispielsweise ein mit Schadsoftware befallener Rechner oder ein Betrugsopfer in Deutschland), auch wenn unbekannt war, ob sich die kriminelle Handlung im In- oder Ausland ereignet hatte.

Für das Jahr 2014 wurde damit begonnen, Delikte der Cybercrime bundeseinheitlich nur noch in der PKS zu erfassen, wenn konkrete Anhaltspunkte für eine Tathandlung innerhalb Deutschlands vorliegen. Die Zahlen der PKS des Jahres 2014 zum Phänomen Cybercrime bilden insofern keine Bezugsgröße und keinen Vergleichsmaßstab zu den zurückliegenden Jahren. Die im Überblick für das Jahr 2014 ausgewiesenen Zahlen und Tendenzen erlauben somit keinen Rückschluss auf eine rückläufige Bedrohung durch Straftaten der Cybercrime.

Die mit dem aktuellen Erfassungsmodus in 2014 nicht berücksichtigten Straftaten sollen zukünftig gesondert ausgewiesen, erfasst und in die Lagedarstellung wieder aufgenommen werden.

Einige Erscheinungsformen aktueller Phänomene können mit der deliktisch orientierten PKS allein nicht hinreichend dargestellt werden. Ein Beispiel ist die Zusendung von Schadsoftware per E-Mail. Je nach konkreter Ausprägung kann diese Tat als Fälschen beweiserheblicher Daten, Ausspähen/Abfangen von

[1] Übereinkommen des Europarats über Computerkriminalität vom 23. November 2001 in Budapest

Daten, Datenveränderung/Computersabotage oder im Fall von Ransomware[2] als Erpressung mit Tatmittel Internet erfasst werden. Die Darstellung der Phänomene unter Nr. 2 basiert daher vor allem auf den deliktischen Beschreibungen aus dem Datenbestand des polizeilichen Vorgangsbearbeitungssystems (vgl. Nr. 3.1).

1.2 Verfahrensdaten

Im Jahr 2014 sank die Anzahl der in der PKS erfassten Straftaten der Cybercrime im engeren Sinne auf 20 715 (- 23,3 %) Fälle. Die Aufklärungsquote stieg gegenüber dem Jahr 2013 auf 20,8 % (+ 4,1 %), wobei die Anzahl ermittelter Tatverdächtiger nahezu unverändert blieb (3 462). Ein wesentlicher Grund für den Rückgang der Fallzahlen liegt in den veränderten Erfassungsmodalitäten (vgl. Nr. 1.1).

Unverändert gehören die vielschichtigen Vorbereitungshandlungen und Begehungsweisen zum Diebstahl und Missbrauch digitaler Identitäten (sogenannter Accountdiebstahl/-missbrauch) sowie Angriffe auf das Online-Banking zu den wesentlichen Erscheinungsformen.

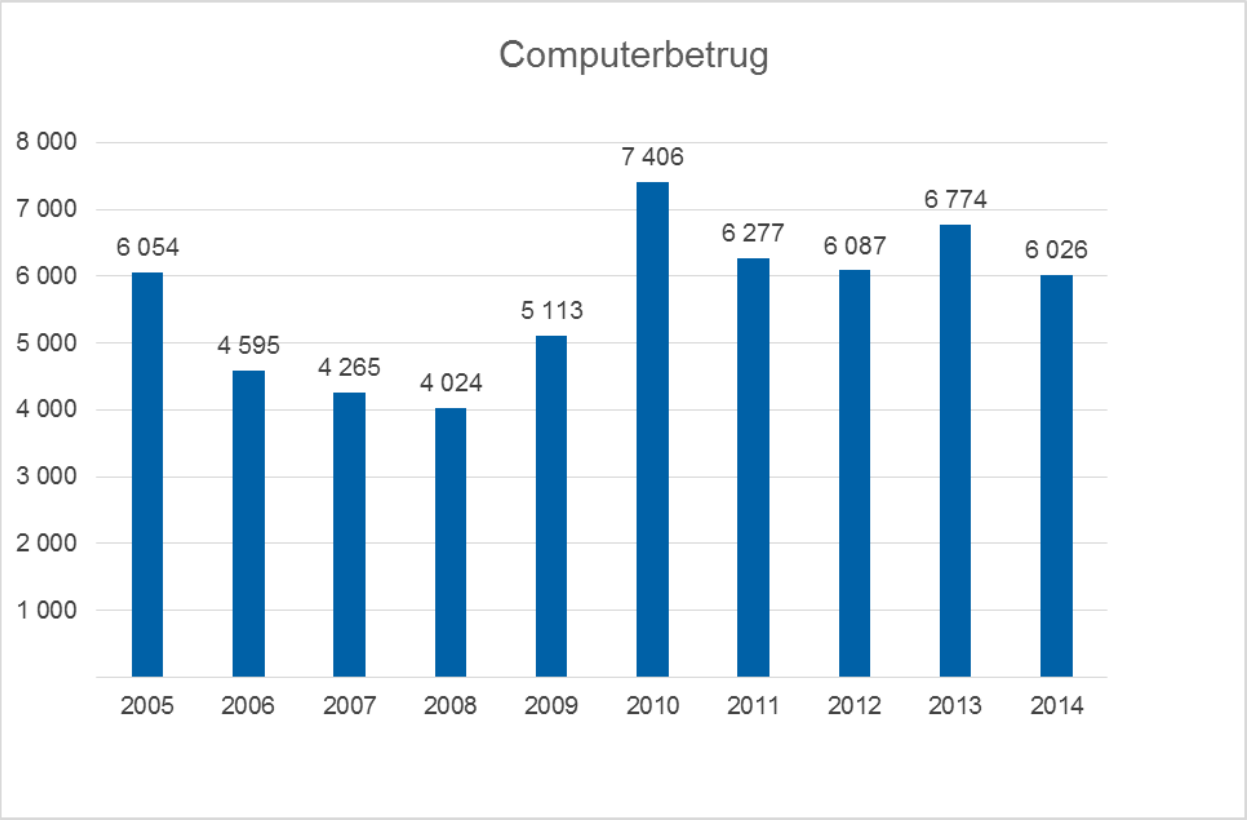
[2] Derivate von Schadsoftware, die Computersysteme sperren, Daten verschlüsseln und Nutzer anschließend zu einer Zahlung über elektronische Zahlungsmittel (u. a. UKash, Paysafe-Card) zur angeblichen Freischaltung auffordern.

1.3 Einzelne Deliktsfelder

Computerbetrug

Die Fallzahlen der letzten Jahre im Bereich des Computerbetrugs sind schwankend. Über den Betrachtungszeitraum 2009 bis 2013 zeigte sich ein insgesamt ansteigender Trend (2009: 5 113, 2010: 7 406, 2011: 6 277, 2012: 6 087, 2013: 6 774). Im Jahr 2014 ist ein Rückgang um 748 Fälle (- 11,0 %) auf 6 026 Fälle festzustellen.

Unverändert dominierte der Missbrauch digitaler Identitäten. Grundsätzlich sichere mTAN[3]- und chipTAN[4]-Verfahren wurden mit überzeugenden Legenden wie vorgeblich erforderlicher Synchronisation von chipTAN-Geräten oder Anpassungen/Verifikationen zur Erhöhung der Systemsicherheit überwunden. Den Tätern gelang es, die Rufnummern auszutauschen, die für das mTAN-verfahren hinterlegt waren oder mittels weiterer SIM-Karten Transaktionsnummern umzuleiten, die als SMS im mTAN-Verfahren versendet wurden.



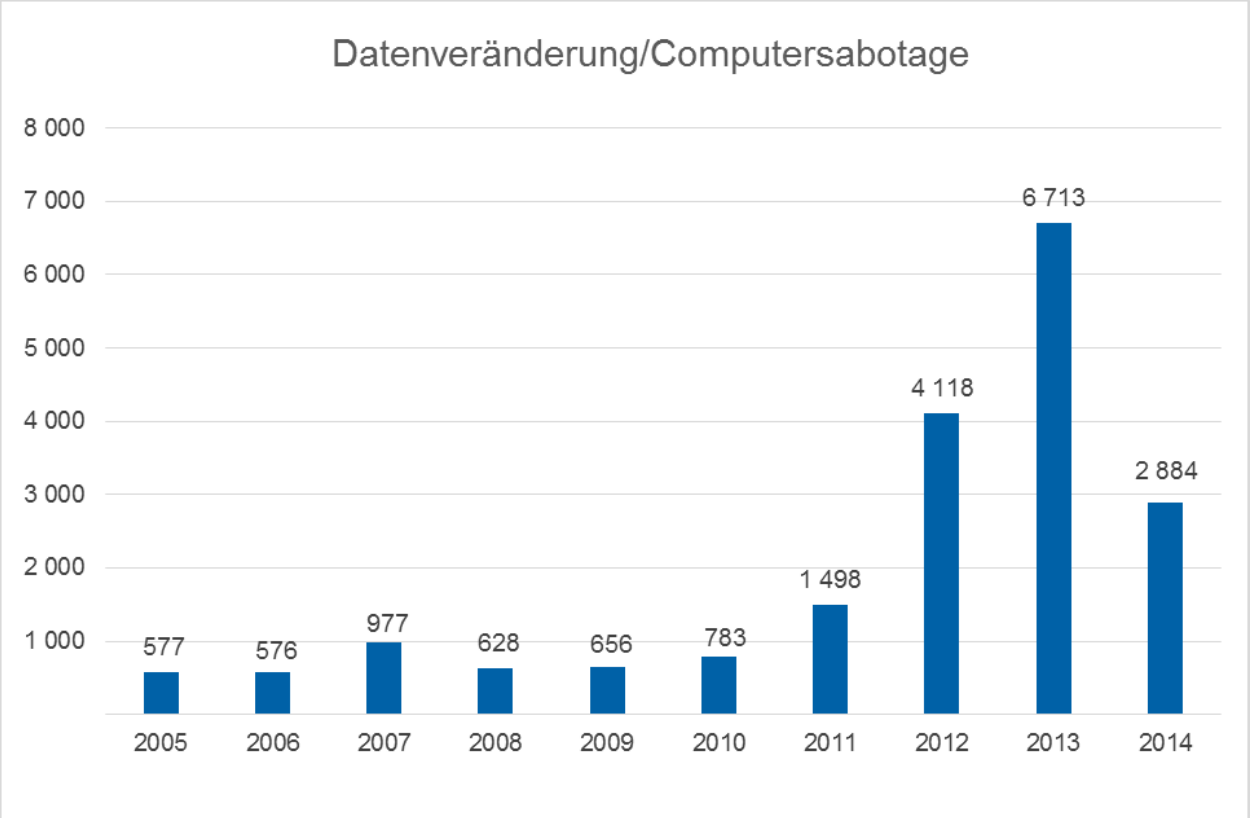
Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei der Datenverarbeitung

Im Betrachtungszeitraum 2014 sank die Zahl der erfassten Fälle auf 2 625 (- 15,9 %). Diesem Deliktsbereich liegt im Wesentlichen die Zusendung von E-Mails unter Vorspiegelung fremder (realer) Identitäten oder Firmen zu Grunde. Mit überzeugenden Legenden soll hierbei das Opfer z. B. zur Preisgabe von Account-Informationen, Kreditkartendaten oder auch zu Zahlungen bewegt werden. Darüber hinaus unterfällt diesem Deliktsbereich auch die Zusendung von als Rechnungen getarnter Schadsoftware in E-Mail-Anhängen.

[3] mTAN: mobile transaction authentication number oder smsTAN: Transaktionsnummer, die per SMS auf Mobilfunkgeräte übertragen wird
[4] chipTAN: Beim chipTAN-Verfahren wird die Transaktionsnummer mittels Bankkarte und TAN-Generator (zusätzliche Hardware) zum jeweiligen Transaktionsauftrag erzeugt

Datenveränderung/Computersabotage

Gegenüber dem Jahr 2013 wurden in der PKS 2 884 Fälle erfasst (6 713). Dies entspricht einem Rückgang um 57,0 %. Die Ursache liegt in einer auffälligen Abnahme der Fälle von Ransomware. Account-Übernahmen und die E-Mail-Zusendung von Trojanern zählten 2014 dennoch zu den dominierenden Erscheinungsformen. Die Dateianhänge beinhalten Schadsoftware, welche bei Ausführung durch Anklicken zumeist vielschichtig Nutzerdaten ausspähen. Die Auswirkungen reichen soweit, dass mitunter auch der E-Mail-Account der Opfer übernommen und zur Weiterverbreitung der vermeintlichen Rechnungsmails missbraucht wird.



Ausspähen, Abfangen von Daten einschließlich Vorbereitungshandlungen

Im Jahr 2014 wurden 4 381 Fälle erfasst. Im Vergleich zum Jahr 2013 (5 486 Fälle) bedeutet dies einen Rückgang um 20,1 %. Auch in diesem Deliktsbereich stehen digitale Identitäten, Kreditkarten-, E-Commerce- oder Kontodaten im Fokus der Cyberkriminellen. Die inkriminierten Daten finden im Handel in der „Underground Economy“[5] weiterhin ihren Absatz.

Betrug mittels rechtswidrig erlangter Debitkarten[6] *mit PIN*

Beim betrügerischen Einsatz von Debitkarten mit PIN (Girokarten bzw. Maestro-Karten, früher EC-Karten) sind die Fallzahlen des Jahres 2014 mit 4 467 erfassten Fällen im Vergleich zu den Vorjahren weiterhin rückläufig (2013: 4 553; 2012: 4 880). Die Tatausführung wird durch einen unachtsamen und sorglosen Umgang mit der PIN begünstigt, da diese vom Berechtigten häufig auf einem Notizzettel oder als vermeintlich gut getarnte Telefonnummer mitgeführt wird. Den Taten gehen meist sogenannte Erlangungstaten voraus (wie z. B. Taschendiebstahl).

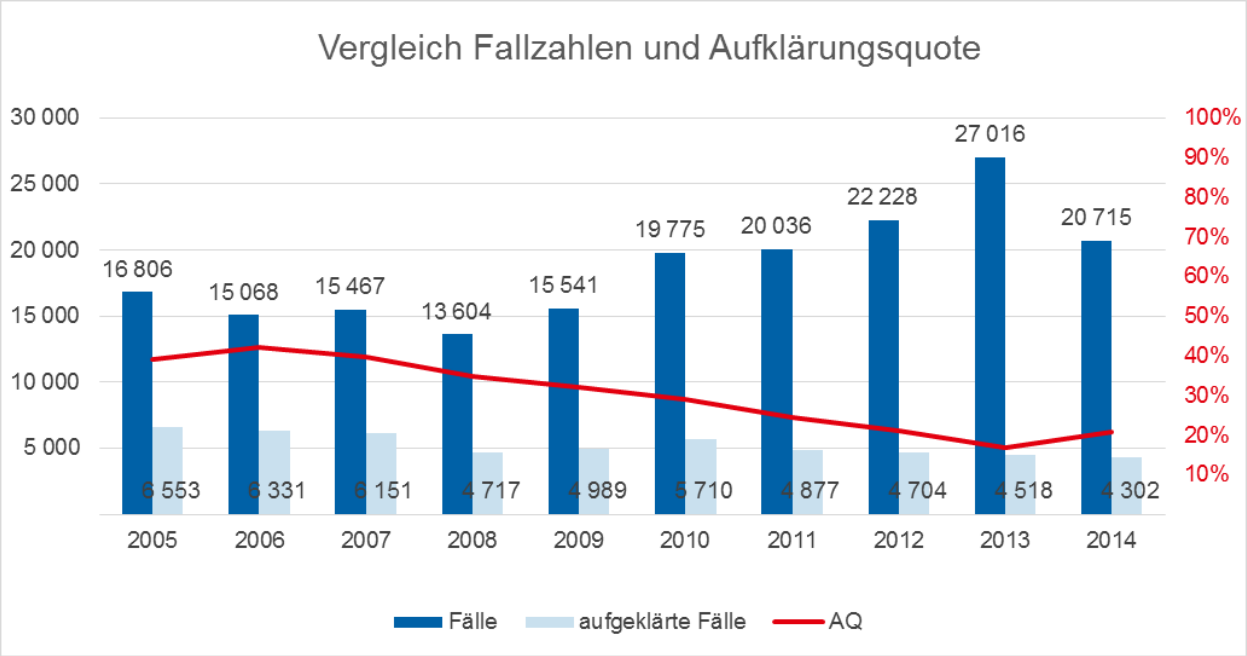
[5] Insbesondere Internetforen, in denen u. a. inkriminierte Daten und Dienstleistungen gehandelt werden
[6] Zahlungskarten, deren Einsatz unmittelbar zur Kontobelastung führt – Girocard oder EC/Maestro-Karte

Betrug mittels Zugangsberechtigungen zu Kommunikationsdiensten

Die Anzahl der Fälle im Jahr 2014 liegt mit 296 (319) geringfügig unter der des Jahres 2013. Ein Schwerpunkt ist die Manipulation von Telekommunikationsanlagen. Unter Ausnutzung von Sicherheitslücken oder schwachen Zugangssicherungen werden sowohl bei Firmen als auch bei Privathaushalten z. B. durch den unberechtigten Zugriff auf Router[7] teure Auslandstelefonverbindungen angewählt und Premium- bzw. Mehrwertdienste in Anspruch genommen.

1.4 Aufklärungsquote

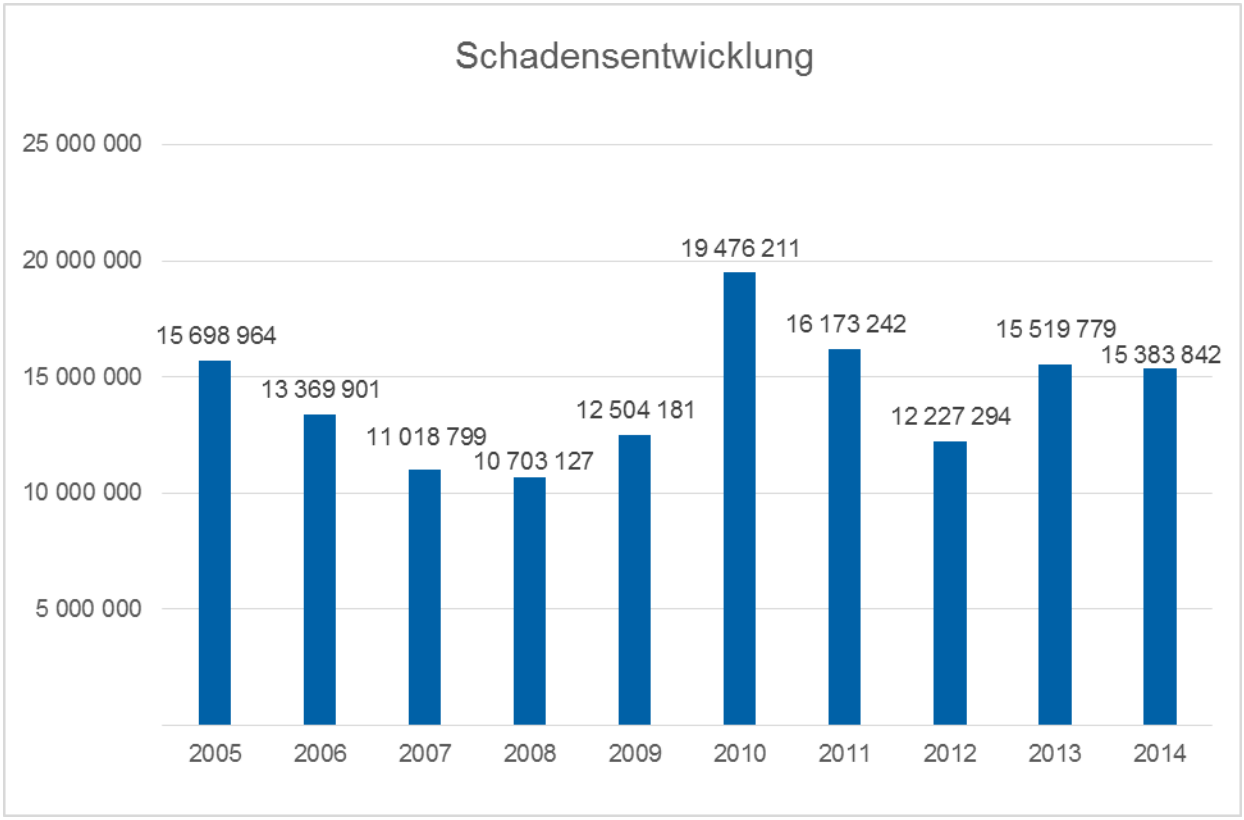
Die Aufklärungsquote der Cybercrime im engeren Sinne ist gegenüber dem Jahr 2013 von 16,7 % auf 20,8 % gestiegen. Neben dem Rückgang der erfassten Fälle durch die Änderung der Erfassungsrichtlinien der PKS (vgl. Nr. 1.1) dürfte sich der Rückgang der nur begrenzt ermittelbaren Fälle von Ransomware positiv auf die Aufklärungsquote ausgewirkt haben.



[7] Netzwerkgerät zur Anbindung von Netzwerken und Endgeräten an das Internet

1.5 Schadensentwicklung

Die Gesamtschadenssumme der erfassten Cybercrime-Delikte im engeren Sinne beläuft sich für das Jahr 2014 auf 15 383 842 Euro. Damit liegt sie trotz sinkender Fallzahlen auf einem nur geringfügig niedrigeren Niveau als im Jahr 2013 (15 519 779 Euro). Ein Grund ist der besonders auffällige Rückgang von Fallzahlen in Deliktsbereichen, bei denen grundsätzlich keine Schadenserfassung in der PKS erfolgt (z. B. bei Datenveränderung/Computersabotage).



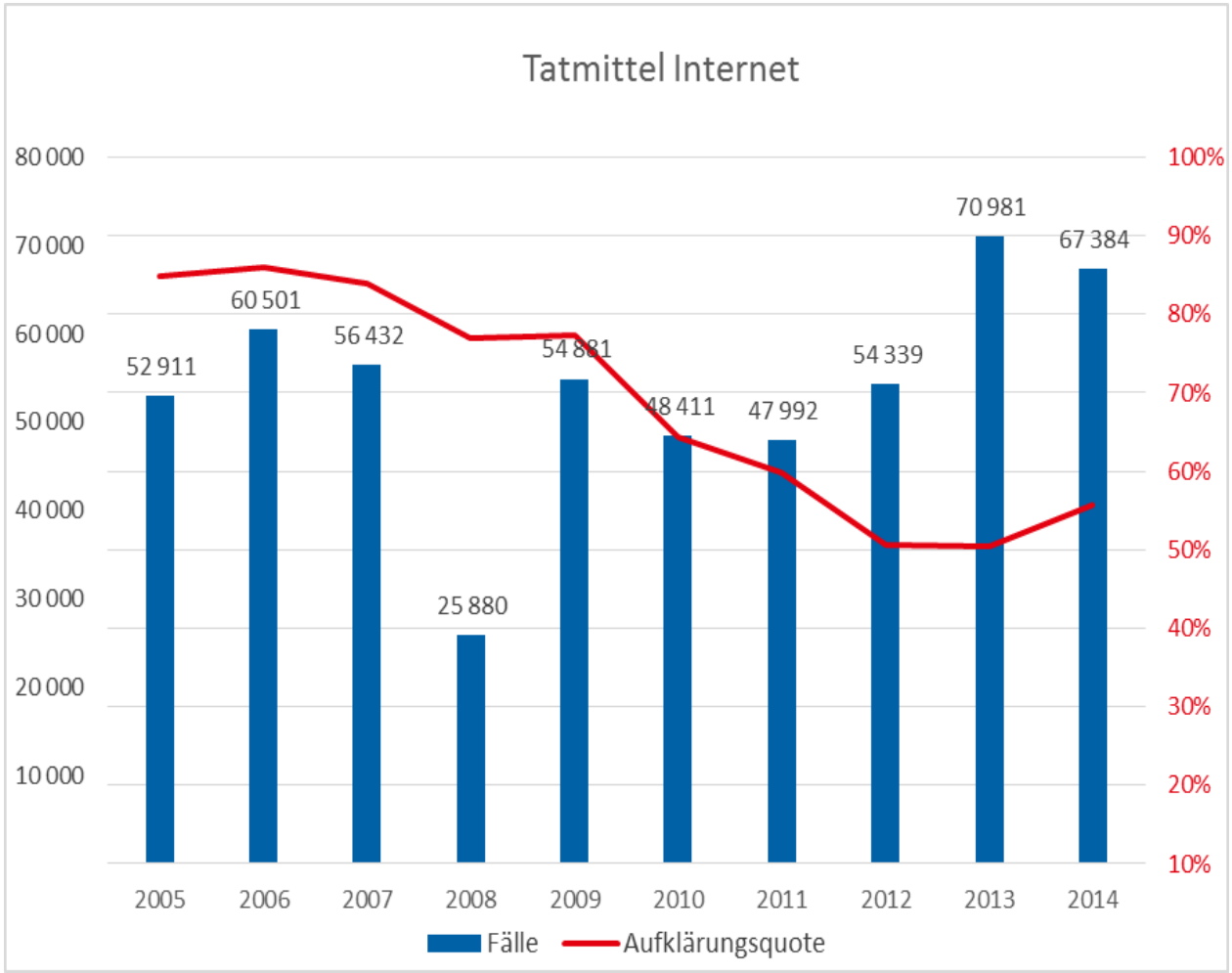
1.6 Tatmittel Internet

Mit dem Zusatz „Tatmittel Internet“ werden in der PKS Straftaten erfasst, bei denen das Internet als Tatmittel bei der Tatbestandsverwirklichung eingesetzt wird. Ebenfalls werden sogenannte Äußerungs- und Verbreitungsdelikte erfasst, deren Tatbestände bereits durch das Einstellen von Informationen in das Internet erfüllt sind. Spielt das Internet im Hinblick auf die Tatverwirklichung eine untergeordnete Rolle, wird die Sonderkennung „Tatmittel Internet“ nicht verwendet. Dies ist beispielsweise der Fall, wenn lediglich Kontakte zwischen Täter und Opfer mittels Internet im Vorfeld der eigentlichen Tat stattfinden.

Für das Jahr 2014 wurden 67 384 Fälle mit der Sonderkennung „Tatmittel Internet“ erfasst. Nach den Anstiegen der Jahre 2011 bis 2013 bedeutet dies eine Abnahme um 5,1 %. Die Anzahl der aufgeklärten Fälle stieg auf 37 558, was einer Aufklärungsquote von 55,7 % (50,5 %) entspricht.

Der Anteil der Straftaten mit dieser Sonderkennung an der Gesamtkriminalität sank leicht auf 4,5 % (4,8 %). 71,7 % der Straftaten mit dem „Tatmittel Internet“ entfielen auf Betrugsdelikte.

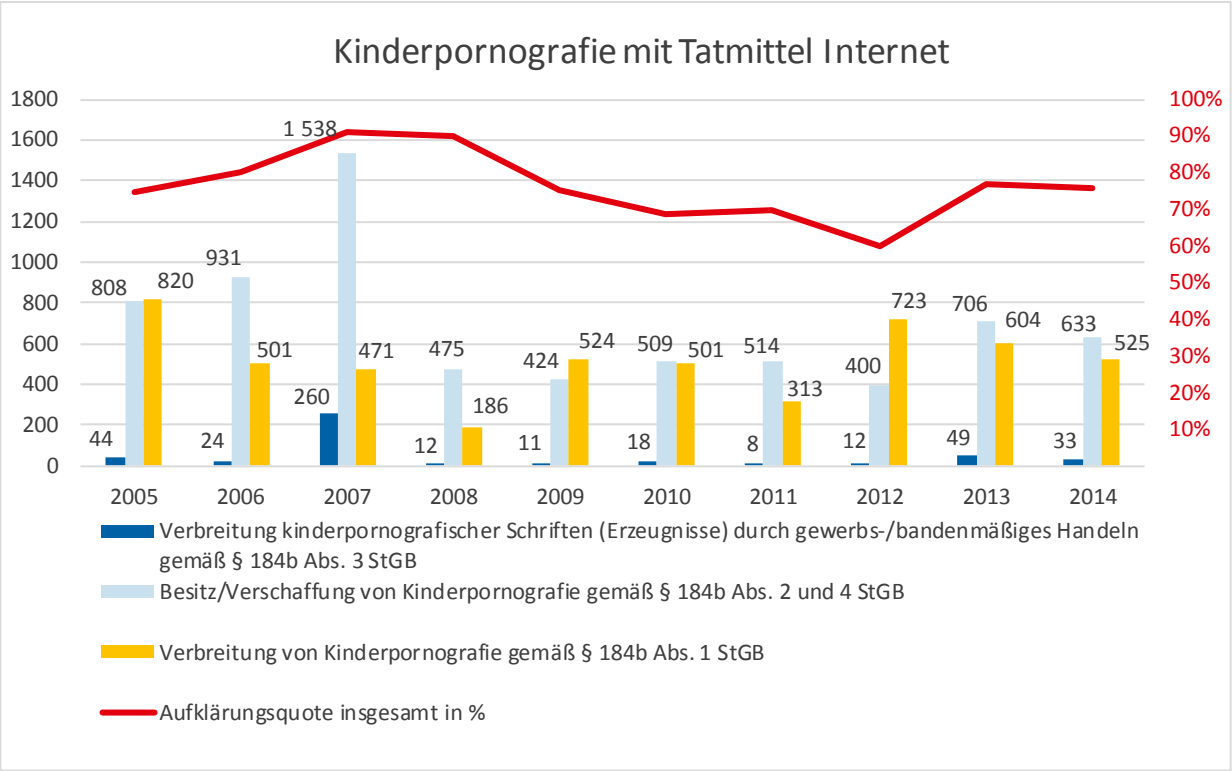
Der Anteil der Erpressungen mit dem „Tatmittel Internet“ nahm um 74,1 % auf nun 514 Fälle ab. Dies ist vorwiegend auf den Rückgang der Ransomware zurückzuführen.



Kinderpornografie

Die jährlichen Fallzahlen im Deliktsbereich „Verbreitung und Besitz/Verschaffung von Kinderpornografie“ sind mitunter deutlichen Schwankungen unterworfen, weil die Erfassung erst mit dem Abschluss der Verfahren, zum Teil von Umfangsverfahren mit einer Vielzahl von Einzeltaten, erfolgt. Die Anzahl der so erfassten Fälle verringerte sich im Jahr 2014 gegenüber dem Jahr 2013 von 1 578 auf 1 456 Fälle, darunter 40 Fälle der gewerbs- bzw. bandenmäßigen Verbreitung von Kinderpornografie (53).

Das Tatmittel Internet spielte mit einem Anteil von 84,1 % auch im Jahr 2014 bei Delikten der Kinderpornografie eine herausragende Rolle. Insgesamt wurden im Deliktsbereich Kinderpornografie mit Tatmittel Internet im Jahr 2014 1 191 Fälle (1 359) erfasst. Dies entspricht einem Rückgang um 168 Fälle. Die Aufklärungsquote betrug 75,6 % (77,0 %).



2 Ausgewählte Phänomene

2.1 Identitätsdiebstahl/ID-Theft

Der Identitätsdiebstahl hatte mit einer Anzahl von ca. 12 500 Fällen im Jahr 2014 wie in den zurückliegenden Jahren einen wesentlichen Teil an den im Vorgangsbearbeitungssystem der Polizei NRW erfassten Fällen der Cybercrime. Mittels Phishing, Hacking, manipulierter Internetseiten, Social Engineering[8] oder einfacher Open-Source-Recherchen[9] gelangten die Täter an Kontodaten, Kreditkartendaten, Benutzeraccounts von Internetbezahldiensten und –handelsplattformen sowie weitere sensible Daten.

Die einfache Möglichkeit, große Mengen derartiger Datensätze auf anonymen, technisch abgeschotteten Internetverkaufsplattformen, der Underground-Economy[10], zu kaufen, ermöglicht es Tätern ohne spezielles IT-Wissen, solche Daten illegal zu verwenden. Mittels dieser fremden Identitäten werden i. d. R. Waren bestellt, Verträge abgeschlossen oder weitere Personen betrogen. Gezielte Angriffe gegen einzelne Personen, um bspw. Codes oder Geschäftsgeheimnisse zu erlangen, auch als Spear-Phishing bezeichnet, verursachten im Jahr 2014 hohe Schäden im sechsstelligen Bereich.

Fallbeispiel

Ein Unternehmen erhielt über die E-Mail-Adresse eines ausländischen Geschäftspartners die Mitteilung, dass sich die Kontoverbindung geändert habe. In der Folge überwies das Unternehmen Rechnungen von über 400 000 Euro auf ein falsches Konto im Ausland. Ein unbekannter Täter hatte den E-Mail-Account des Geschäftspartners übernommen. Der Betrug fiel erst auf, nachdem die offenen Rechnungen durch den Geschäftspartner angemahnt wurden.

2.2 Angriffe gegen das Online-Banking

Trotz Sicherheitsvorkehrungen im Onlinebanking, wie TAN-Generatoren oder mTAN-Verfahren, konnten Cyberkriminelle auch im Jahr 2014 Zahlungsvorgänge manipulieren. Gegenüber dem Vorjahr wurden 3 893 Fälle (3 178) erfasst. Dies entspricht einem Anstieg um 22,5 %.

Bankkunden wurden mittels Schadsoftware ausgespäht. Anschließend nutzten die Täter Unachtsamkeiten beim Umgang[11] mit TAN-Generatoren aus, ließen Duplikate von SIM-Karten ausstellen oder änderten die im Onlinebanking hinterlegten Rufnummern für den Empfang der per SMS versandten TAN. Weiterhin wurden Bankkunden durch Schadsoftware beim Online-Banking aufgefordert, nach vorgeblichen Änderungen im Onlinebanking-Verfahren, Test- oder Demoüberweisungen durchzuführen, bei denen das Geld jedoch auf Konten der Täter geleitet wurde. Auch durch Anrufe angeblicher Bank- oder Supportmitarbeiter gelangten die Täter an die erforderlichen Daten, um die Manipulationen zu ermöglichen.

Es entstanden hohe Schäden durch Rücküberweisungsbetrug. Hier suggeriert die Schadsoftware dem Anwender, dass versehentlich ein hoher Geldbetrag auf dessen Konto überwiesen worden sei, der umgehend zurück überwiesen werden müsse.

Fallbeispiel

Von dem Bankkonto eines Unternehmens wurden durch unbekannte Täter Überweisungen in Gesamthöhe von nahezu 500 000 Euro auf ausländische Konten durchgeführt. Den Tätern war es gelungen, im Onlinebanking-Account des Unternehmens die für die Nutzung des mTAN-Verfahrens vorgesehene Rufnummer zu ändern.

[8] Bildung einer Legende, um eine Person zu beeinflussen und diese zu einer Handlung zu veranlassen (z. B. angebliche Sicherheitsmaßnahme, Test-/Fehlüberweisung oder SEPA-Umstellung)
[9] Nutzung öffentlich zugänglicher Informationen, insbesondere im Internet
[10] Insbesondere Internetforen, in denen u. a. inkriminierte Daten und Dienstleistungen gehandelt werden
[11] Auf dem TAN-Generator werden stets die tatsächlichen Daten (Zielkonto, Betrag) angezeigt, während die Bildschirmanzeige manipuliert sein kann.

2.3 Ransomware

Nach einem Höchststand der Ransomware in den Jahren 2012 und 2013 mit jeweils über 8 000 Fällen sank die Zahl der im Vorgangsbearbeitungssystem der Polizei NRW erfassten Fälle im Jahr 2014 auf unter 500. Hieran lässt sich deutlich die Veränderungsdynamik der Cybercrime erkennen. Die zunehmende Sensibilisierung der Bevölkerung einerseits und verbesserte Antivirenprodukte andererseits sind wesentliche Einflussfaktoren.

2.4 Telekommunikationsanlagenmanipulation

Im Vergleich zum zurückliegenden Jahr hat sich im Jahr 2014 die Anzahl der im polizeilichen Vorgangsbearbeitungssystem erfassten Fälle von Manipulationen an Telekommunikationsanlagen mit 657 Fällen (220) fast verdreifacht. Die Schadenssumme stieg im Vergleich zum Vorjahr um 55,0 % auf etwa 1 400 000 Euro. In vielen Fällen verschafften sich die Täter über bekannte Schwachstellen in der Kommunikationssoftware und mangelnde Zugangssicherungen Zugriff auf die Anlagen. Die Systeme wurden missbraucht, um kostenintensive Auslandsgespräche zu führen und Premium- bzw. Mehrwertdienste in Anspruch zu nehmen. Private Telefonanlagen wurden auch im Jahr 2014 in 338 Fällen durch Kriminelle über Schwachstellen in der Firmware angegriffen. Es entstand hierbei ein Schaden in Höhe von etwa 470 000 Euro (durchschnittlich ca. 1 400 Euro je Fall).

3 Fazit

Die rückläufigen Fallzahlen in der PKS lassen nicht auf eine veränderte Bedrohungssituation durch Cybercrime schließen. Der Vergleich mit den Daten des polizeilichen Vorgangsbearbeitungssystems zeigt einerseits, dass ein Rückgang der Fallzahlen in einzelnen Phänomenbereichen tatsächlich stattgefunden hat. Andererseits bildet das polizeiliche Vorgangsbearbeitunssystem einen Anstieg in einzelnen Phänomenbereichen ab, die in der PKS scheinbar rückläufig sind. Die Auswirkungen der geänderten Erfassungsrichtlinien der PKS erzeugen zudem Unschärfen. Cyberkriminelle entwickeln stetig neue Techniken, um Sicherheitsmaßnahmen zu umgehen und sich finanziell zu bereichern. Eine erfolgreiche Verhütung vor und Bekämpfung von Cybercrime wird auch zukünftig von verschiedenen Faktoren abhängig sein. Bei der Verhütung von Cybercrime sind kurze Reaktionszeiten bei der Erkennung neuer Phänomene und Sensibilisierung der Bevölkerung erforderlich. Für eine effektive Verfolgung von Cybercrimedelikten müssen Polizei, Justiz und Wirtschaftsunternehmen national und international ihre Zusammenarbeit intensivieren. Auch der Gesetzgeber ist gefordert, klare rechtliche Rahmenbedingungen für die Nutzung neuer Technologien zu setzen. Die Strafverfolgungsbehörden benötigen geeignete Instrumente, um ihre Aufgaben zum Schutz der Bevölkerung und Verfolgung von Straftätern auch im Internet effektiv wahrnehmen zu können. Kein anderer Deliktsbereich unterliegt einer annähernd vergleichbaren Komplexität und Veränderungsdynamik. Die Präventionsverantwortlichen und die Strafverfolgungsbehörden müssen mit gleicher Dynamik gestärkt werden. Erforderlich sind kontinuierliche Inverstitionen, die Stärkung innovativer Prozesse sowie angemessene Ermittlungsmethoden.

4 Anlagen

4.1 Datenbasis

Grundlage dieses Lagebildes sind Daten aus der Polizeilichen Kriminalstatistik (PKS), Sachverhalte aus dem polizeilichen Vorgangsbearbeitungssystem und dem Kriminalpolizeilichen Sondermeldedienst Cybercrime. In der PKS werden unter dem Summenschlüssel 897000 nur die Delikte der Cybercrime im engeren Sinne zusammengefasst (siehe Nr. 1.1 Vorbemerkungen).

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

- § 202a StGB Ausspähen von Daten
- § 202b StGB Abfangen von Daten
- § 202c StGB Vorbereitungshandlungen zum Ausspähen und Abfangen von Daten
- § 263a 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, mittelbare Falschbeurkundung/Urkundenunterdrückung, § 348 StGB im Zusammenhang mit Datenverarbeitung
- § 303a StGB Datenveränderung
- § 303b StGB Computersabotage

Während sich aus der PKS nicht alle Informationen zu den einzelnen Straftaten entnehmen lassen, bietet der Kriminalpolizeiliche Sondermeldedienst Cybercrime 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.

4.2 Tabellen – Polizeiliche Kriminalstatistik

Tabelle 1: Fallzahlen in einzelnen Deliktsfeldern der Cybercrime im engeren Sinne

	Delikte		Zu-/ Abnahme	
Straftaten	**2013**	**2014**	**in Zahlen**	**in %**
Computerbetrug	6 774	6 026	- 748	- 11,0
Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung	3 121	2 625	- 496	- 15,9
Datenveränderung/ Computersabotage	6 713	2 884	- 3 829	- 57,0
Ausspähen, Abfangen von Daten einschl.Vorbereitungshandlungen	5 486	4 381	- 1 105	- 20,1
Betrug mittels rechtswidrig erlangter Debitkarte mit PIN	4 553	4 467	- 86	- 1,9
Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten	319	296	- 23	- 7,2
Softwarepiraterie private Anwendung	34	19	- 15	- 44,1
Softwarepiraterie - gewerbsmäßiges Handeln	16	17	+ 1	+ 6,3
Computerkriminalität insgesamt	27 016	20 715	- 6 301	- 23,3

Tabelle 2: Aufklärungsquoten

	aufgeklärte Fälle		Aufklärungsquote in %		Zu-/ Abnahme
Straftaten	**2013**	**2014**	**2013**	**2014**	**% - Punkte**
Computerbetrug	1 452	1 491	21,4	24,7	+ 3,3
Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung	643	642	20,6	24,5	+ 3,9
Datenveränderung/ Computersabotage	342	295	5,1	10,2	+ 5,1
Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen	489	470	8,9	10,7	+ 1,8
Betrug mittels rechtswidrig erlangter Debitkarte mit PIN	1 482	1 257	32,6	28,1	- 4,4
Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten	65	115	20,4	38,9	+ 18,5
Softwarepiraterie - private Anwendung	29	17	85,3	89,5	+ 4,2
Softwarepiraterie - gewerbsmäßiges Handeln	16	15	100,0	88,2	- 11,8
Computerkriminalität insgesamt	4 518	4 302	16,7	20,8	+ 4,1

Tabelle 3: Entwicklung der Fallzahlen und Aufklärungsquoten der Cybercrime im engeren Sinne

	bekannt gewordene Fälle		Aufklärung	
Jahr	**erfasste Fälle - insgesamt**	**Zu-/ Abnahme in %**	**aufgeklärte Fälle**	**Aufklärungsquote in %**
2005	16 806	- 1,3	6 553	39,0
2006	15 068	- 10,3	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
2013	27 016	+ 21,5	4 518	16,7
2014	20 715	- 23,3	4 302	20,8

Tabelle 4: Entwicklung der Altersverteilung der Tatverdächtigen

	Tatverdächtige								
	unter 14		14 bis < 18		18 bis < 21		über 21		
Jahr	Anzahl	in %	Anzahl	in %	Anzahl	in %	Anzahl	in %	insgesamt
2005	75	2,1	350	9,7	425	11,8	2 741	76,3	3 591
2006	46	1,3	396	11,5	420	12,2	2 589	75,0	3 451
2007	68	1,7	453	11,4	485	12,2	2 985	74,8	3 991
2008	61	1,6	383	10,2	457	12,1	2 849	76,0	3 750
2009	65	1,4	412	9,1	544	12,0	3 499	77,4	4 520
2010	87	1,8	472	9,7	636	13,1	3 671	75,4	4 866
2011	50	1,2	379	9,0	447	10,6	3 326	79,2	4 202
2012	64	1,7	298	7,9	410	10,9	2 981	79,4	3 753
2013	49	1,4	262	7,5	380	10,9	2 801	80,2	3 492
2014	40	1,2	201	5,8	341	9,8	2 880	83,2	3 462

	Tatverdächtige												
	unter 21		21 bis < 30		30 bis < 40		40 bis < 50		50 bis < 60		über 60		
Jahr	Anzahl	in %	Anzahl	in %	Anzahl	in %	Anzahl	in %	Anzahl	in %	Anzahl	in %	insgesamt
2005	850	23,7	1 070	29,8	909	25,3	515	14,3	189	5,3	58	1,6	3 591
2006	862	25,0	927	26,9	793	23,0	563	16,3	234	6,8	72	2,1	3 451
2007	1 006	25,2	1 020	25,6	820	20,5	714	17,9	337	8,4	94	2,4	3 991
2008	901	24,0	1 042	27,8	859	22,9	618	16,5	246	6,6	84	2,2	3 750
2009	1 021	22,6	1 264	28,0	979	21,7	798	17,7	336	7,4	122	2,7	4 520
2010	1 195	24,6	1 433	29,4	1 054	21,7	736	15,1	338	6,9	110	2,3	4 866
2011	876	20,8	1 348	32,1	925	22,0	666	15,8	291	6,9	96	2,3	4 202
2012	772	20,6	1 116	29,7	813	21,7	647	17,2	301	8,0	104	2,8	3 753
2013	691	19,8	1 018	29,2	779	22,3	607	17,4	276	7,9	121	3,5	3 492
2014	582	16,8	1 105	31,9	806	23,3	574	16,6	294	8,5	101	2,9	3 462

Tabelle 5: Tatmittel Internet

	erfasste Fälle	darunter Tatmittel Internet	
Straftaten	**2014**	**Fälle**	**Anteil in %**
Insgesamt	1 501 125	67 384	4,5
gegen die sexuelle Selbstbestimmung	10 138	1 822	18,0
• Verbreitung pornografischer Erzeugnisse	*2 047*	*1 559*	*76,2*
- Besitz/ Verschaffen von Kinderpornografie	*790*	*633*	*80,1*
- Verbreitung von Kinderpornografie	*626*	*525*	*83,9*
Betrug	253 333	48 343	19,1
• Waren- und Warenkreditbetrug	*75 197*	*28 192*	*37,5*
• Computerbetrug	*6 026*	*4 882*	*81,0*
• Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten	*296*	*140*	*47,3*
Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung	2 625	2 215	84,4
Datenveränderung, Computersabotage	2 884	2 734	94,8
Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen	4 381	3 872	88,4
Erpressung	1 842	514	27,9

Herausgeber

Landeskriminalamt Nordrhein-Westfalen
Völklinger Straße 49
40221 Düsseldorf

Abteilung 4
Cybercrime-Kompetenzzentrum
Dezernat 41
Redaktion: KOR Helmut Picko
Telefon: +49 211 939-4100 oder Polizeinetz 07-224-4100
Telefax: +49 211 939-194100 oder Polizeinetz 07-224-194100

Dez41.LKA@polizei.nrw.de

Impressum

Landeskriminalamt Nordrhein-Westfalen
Abteilung 4, Cybercrime-Komeptenzzentrum
Völklinger Straße 49
40221 Düsseldorf

Telefon: +49 211 939-0
Telefax: +49 211 939-4119

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

Titelbild: Polizei NRW