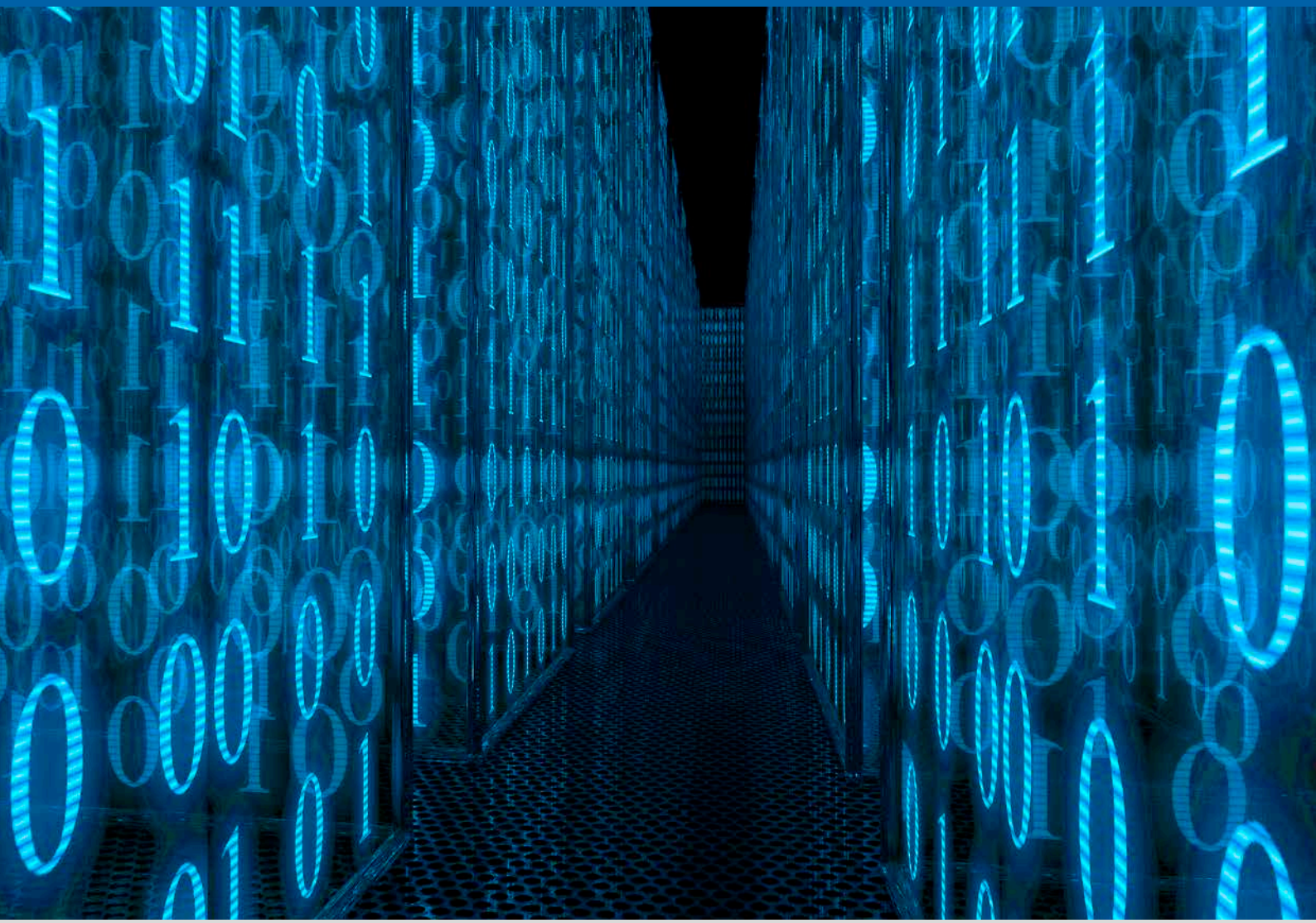
POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

bürgerorientiert ▪ professionell ▪ rechtsstaatlich



Cybercrime
Lagebild für NRW 2015

www.lka.polizei.nrw.de

Kriminalitätsentwicklung im Überblick

Cybercrime

> Allgemeiner Rückgang der Fälle durch Änderung der Erfassungsrichtlinien in der Polizeilichen Kriminalstatistik

> Rückgang der Fälle von Erpressung mit Tatmittel Internet

	2014	2015	Veränderung in %	
Cybercrime im engeren Sinne	**20 715**	**16 645**	**- 19,6**	
Computerbetrug	6 026	5 289	- 12,2	
Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei der Datenverarbeitung	2 625	2 092	- 20,3	
Datenveränderung/ Computersabotage	2 884	1 351	- 53,2	
Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen gem. §§ 202a, 202b, 202c StGB	4 381	3 115	- 28,9	
Betrug mittels rechtswidrig erlangter Debitkarten mit PIN	4 467	4 440	- 0,6	
Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten	296	302	+ 2,0	
Straftaten mit Tatmittel Internet	**67 384**	**58 829**	**- 12,7**	
Betrug mit Tatmittel Internet	48 343	43 630	- 9,7	
Erpressung mit Tatmittel Internet	514	433	- 15,8	
Anzahl der aufgeklärten Fälle mit Tatmittel Internet	37 558	36 775	- 2,9	

Inhalt

Abbildungsverzeichnis

Tabellenverzeichnis

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, sind 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 2015 erneut deutlich zurückgegangen, die Aufklärungsquoten sind hingegen weiter gestiegen. Die statistischen Daten sind zu einem wesentlichen Teil auf die andauernden Nachwirkungen der veränderten Erfassungsmodalitäten zurückzuführen. Bis einschließlich 2013 erfasste die Mehrzahl der Länder Cybercrime-Delikte mit einem Schadenseintritt in Deutschland auch, wenn unbekannt war, ob sich die kriminelle Handlung des Täters im In- oder Ausland ereignete.

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

Im Jahr 2014 wurde damit begonnen, Delikte der Cybercrime bundeseinheitlich nur noch in der PKS zu erfassen, wenn konkrete Anhaltspunkte für eine Handlung des Täters innerhalb Deutschlands vorliegen. Auf Grund der 2014 geänderten Erfassungsrichtlinien bilden die Zahlen der PKS der Jahre 2014 und 2015 zum Phänomen Cybercrime keine Bezugsgröße und keinen Vergleichsmaßstab zu den zurückliegenden Jahren. Die im Überblick für die Jahre 2014 und 2015 ausgewiesenen sinkenden Zahlen und Tendenzen erlauben deshalb nicht den Rückschluss, die Bedrohung durch Cybercrime sei rückläufig.

Einige Erscheinungsformen aktueller Phänomene können mit der deliktisch orientierten PKS allein nicht hinreichend dargestellt werden. Ransomware[2] beispielsweise wird je nach konkreter Ausprägung als Computersabotage, Datenveränderung oder Erpressung mit Tatmittel Internet erfasst.

1.2 Verfahrensdaten

Die Zahl der in der PKS erfassten Cybercrime-Fälle ist, nach kontinuierlichen Anstiegen bis 2013, im Jahr 2015 mit 16 645 Fällen zum zweiten Mal in Folge deutlich gesunken (20 715). Dies entspricht einem Rückgang von 19,6 Prozent. Die Aufklärungsquote stieg gegenüber dem Jahr 2014 um 5,6 Prozent auf nun 26,4 Prozent. Die Anzahl der ermittelten Tatverdächtigen ist mit 3 519 leicht angestiegen (3 462). Zu den dominierenden Erscheinungsformen zählen auch im Jahr 2015 die vielschichtigen Vorbereitungshandlungen und Begehungsweisen zum Diebstahl und Missbrauch digitaler Identitäten sowie Angriffe auf Online-Banking (Phishing).

2 Ransomware: Schadsoftware, die infizierte Computer sperrt, ggf. die Daten verschlüsselt und für eine (angebliche) Freischaltung ein Lösegeld fordert. Siehe auch Nr. 2.3

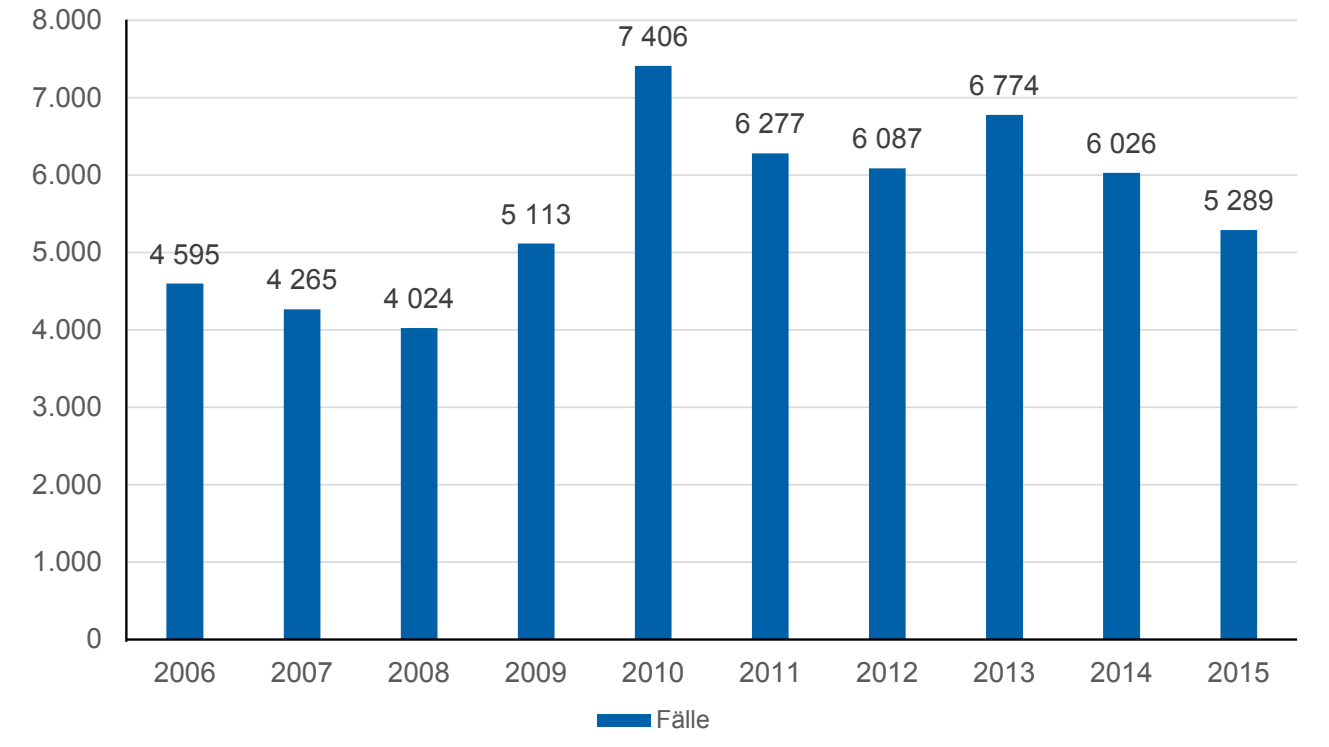
1.3 Einzelne Deliktsfelder

Computerbetrug

Die Fälle des Computerbetrugs sind zum zweiten Mal in Folge rückläufig. Für das Jahr 2015 wurden 5 289 Fälle erfasst, was einem Rückgang von 12,2 Prozent und dem niedrigsten Stand seit 2009 entspricht (2014: 6 026).

Wie bereits in den Vorjahren dominiert der Missbrauch digitaler Identitäten im E-Commerce[3] und beim Online-Banking. Durch den Einsatz von Schadsoftware in Verbindung mit einer überzeugenden Legende werden die Opfer zur Generierung bzw. Eingabe einer oder mehrerer TAN[4] verleitet. Die Täter suggerieren den Opfern, dass es zu Fehlüberweisungen gekommen sei und eine Rücküberweisung durchgeführt werden müsse oder Sicherheitsmaßnahmen der Kreditinstitute in Form von Demoüberweisungen erforderlich seien. Die grundsätzlich technisch sicheren mTAN[5]- und chipTAN[6]-Verfahren werden so mittels Social Engineering[7] überwunden. Teilweise gelang es den Tätern, die Rufnummern für das mTAN-Verfahren auszutauschen oder mit Hilfe betrügerisch erlangter SIM[8]-Karten Transaktionsnummern umzuleiten.

Abbildung 01
Computerbetrug



3 E-Commerce: Elektronischer Handel; das Kaufen und Verkaufen von Waren und Dienstleistungen mittels Internet.

4 TAN: transaction authentication number; Transaktionsnummer für das Online-Banking.

5 mTAN: mobile transaction authentication number; Transaktionsnummer, die per SMS auf Mobilfunkgeräte übertragen wird.

6 chipTAN: Beim chipTAN-Verfahren wird die Transaktionsnummer mittels Bankkarte und TAN-Generator (zusätzliche Hardware) zum jeweiligen Transaktionsauftrag erzeugt.

7 Bildung einer Legende, um eine Person zu beeinflussen und diese zu einer Handlung zu veranlassen.

8 SIM: subscriber identity modul; Chipkarte, die in Mobilfunkgeräten zur Identifikation des Teilnehmers im Mobilfunknetz dient.

Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei der Datenverarbeitung

Im Jahr 2015 wurden 2 092 Fälle registriert, was einem Rückgang um 20,3 Prozent entspricht (2014: 2 625). Zumeist liegt diesem Deliktsbereich die Zusendung von E-Mails unter glaubwürdig wirkender Vorspiegelung fremder, teils realer Identitäten oder Firmen zu Grunde. Das Opfer soll so zur Preisgabe von Informationen zu Accounts, Kreditkartendaten oder Zahlungen bewegt werden. Darüber hinaus entfallen auf diesen Bereich sowohl die Zusendung von E-Mails, in deren Anhang Schadsoftware als vermeintliche Bestellbestätigung, Zahlungsaufforderung oder Rechnung getarnt ist, als auch gefälschte oder kopierte Webseiten.

Datenveränderung/Computersabotage

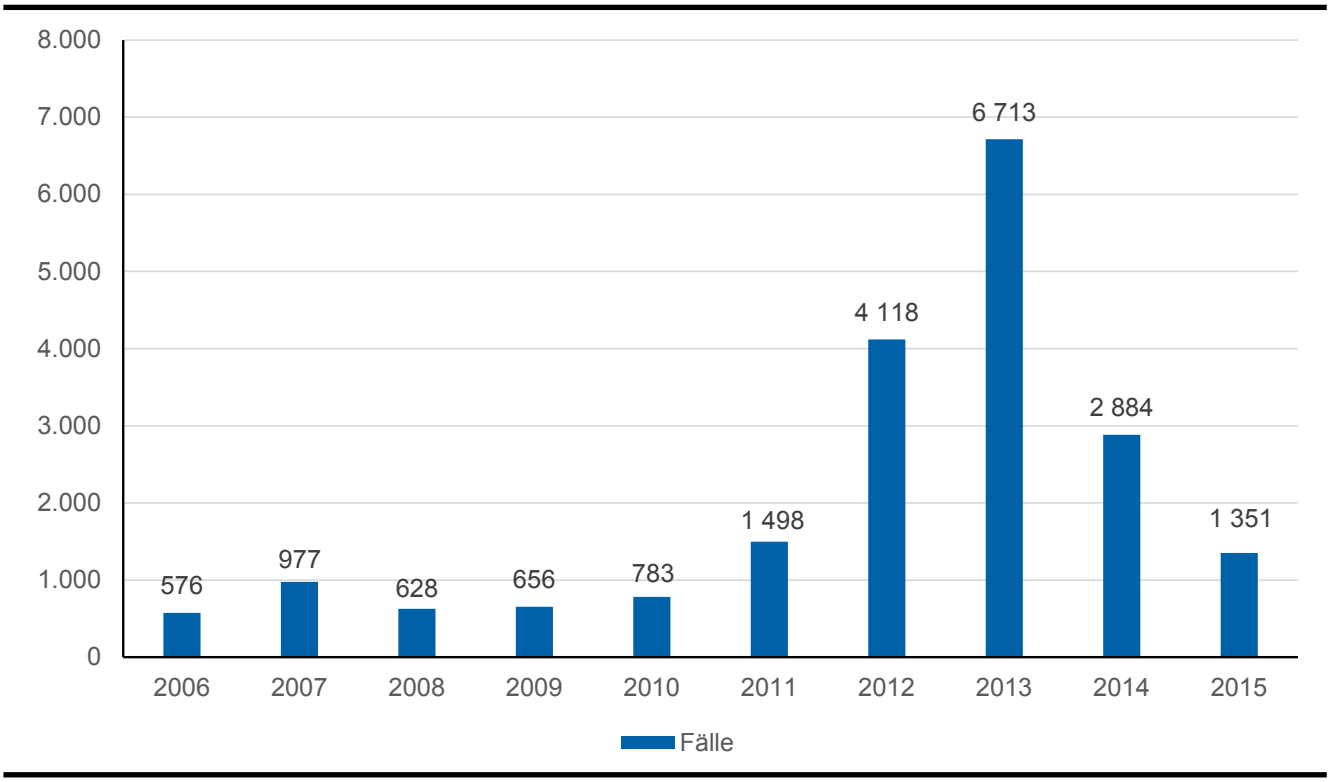
In diesem Deliktsbereich sind im Jahr 2015 die Fälle um 53,2 Prozent auf 1 351 zurückgegangen (2014: 2 884). Dies stellt, wie bereits im Vorjahr, den höchsten Rückgang aller Delikte der Cybercrime im engeren Sinne dar.

Der fortwährende Rückgang der Ransomware ist ausschlaggebend für die Fallzahlenreduktion.

Ausspähen, Abfangen von Daten einschließlich Vorbereitungshandlungen

Im Jahr 2015 weist die PKS zu diesem Deliktsbereich 3 115 Fälle aus, was eine Abnahme um 1 266 Fälle bzw. 28,9 Prozent bedeutet (2014: 4 381). Die dominierenden Erscheinungsformen sind auch hier vielfältige Account-Ausspähungen (z. B. digitale Identitäten, Benutzerkennungen, Kreditkarten- oder Kontodaten). Die erlangten Daten werden anschließend häufig in der „Underground Economy“[9] gehandelt.

Abbildung 02
Datenveränderung/Computersabotage



[9] Schwarzmarkt (insbesondere Internetforen), der dem illegalen Handel von inkriminierten Daten, Dienstleistungen oder Gegenständen dient.

Betrug mittels rechtwidrig erlangter Debitkarten[10] mit PIN[11]

Die Fallzahlen des betrügerischen Einsatzes von Debitkarten mit PIN stagnieren mit 4 440 Fällen (2014: 4 467). Der sorglose Umgang mit der PIN, die häufig als vermeintlich gut getarnte Telefonnummer oder auf einem Notizzettel mitgeführt wird, begünstigt die Tatausführung. In 521 Fällen ging die Tathandlung nicht über das Versuchsstadium hinaus (2014: 486). In der Regel geht diesem Deliktsfeld eine sogenannte Erlangungstat voraus (z. B. Einbruch- oder Taschendiebstahl).

Betrug mittels Zugangsberechtigungen zu Kommunikationsdiensten

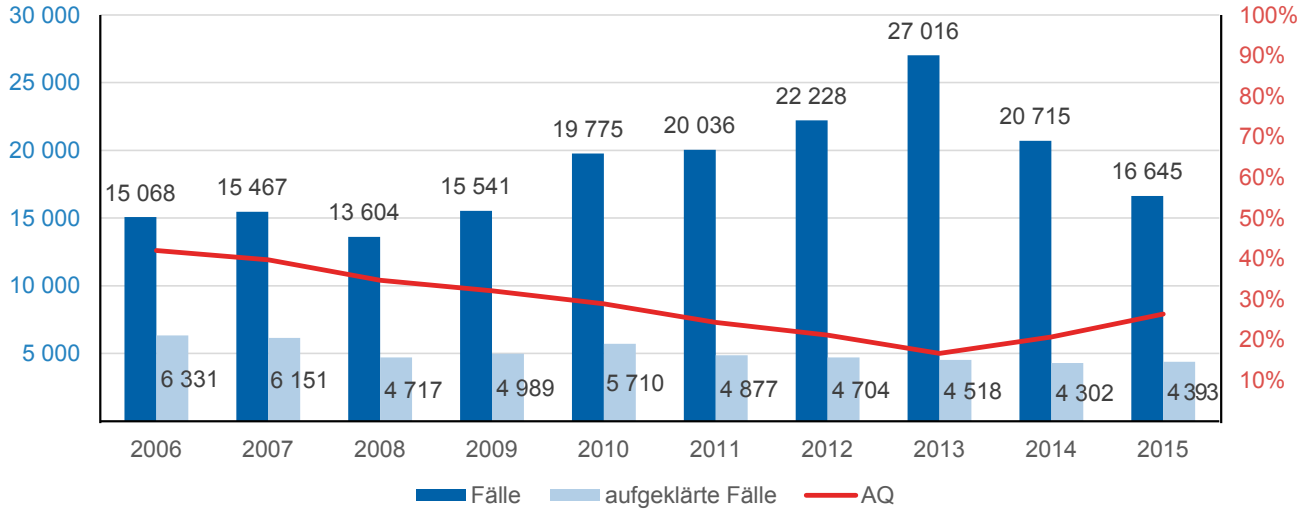
Die Zahlen dieses Deliktsbereichs steigen erstmals seit dem Jahr 2011 wieder an. Der Zuwachs um 2,0 Prozent auf nunmehr 302 Fälle (2014: 296) ist jedoch marginal.

Der Schwerpunkt liegt auf der Manipulation von Telekommunikationsanlagen. Die Täter greifen unter Ausnutzung von Sicherheitslücken oder schwacher Zugangssicherungen (Standard-Passwörter) auf Router[12] von Firmen oder Privatleuten zu und generieren teure Telefonverbindungen in das Ausland oder zu Mehrwertdiensten.

1.4 Aufklärungsquote

Im Jahr 2015 ist die Aufklärungsquote der Cybercrime im engeren Sinne auf 26,4 Prozent gestiegen. Die Steigerung um 5,6 Prozent (2014: 20,8 Prozent) ist auf den Rückgang der erfassten Fälle durch die fortwährenden Auswirkungen der geänderten Erfassungsrichtlinien der PKS zurückzuführen (vgl. Nr. 1.1).

Abbildung 03
Vergleich Fallzahlen und Aufklärungsquote



10 Zahlungskarten, deren Einsatz unmittelbar zur Kontobelastung führt - Girocard oder EC/Maestro-Karte.

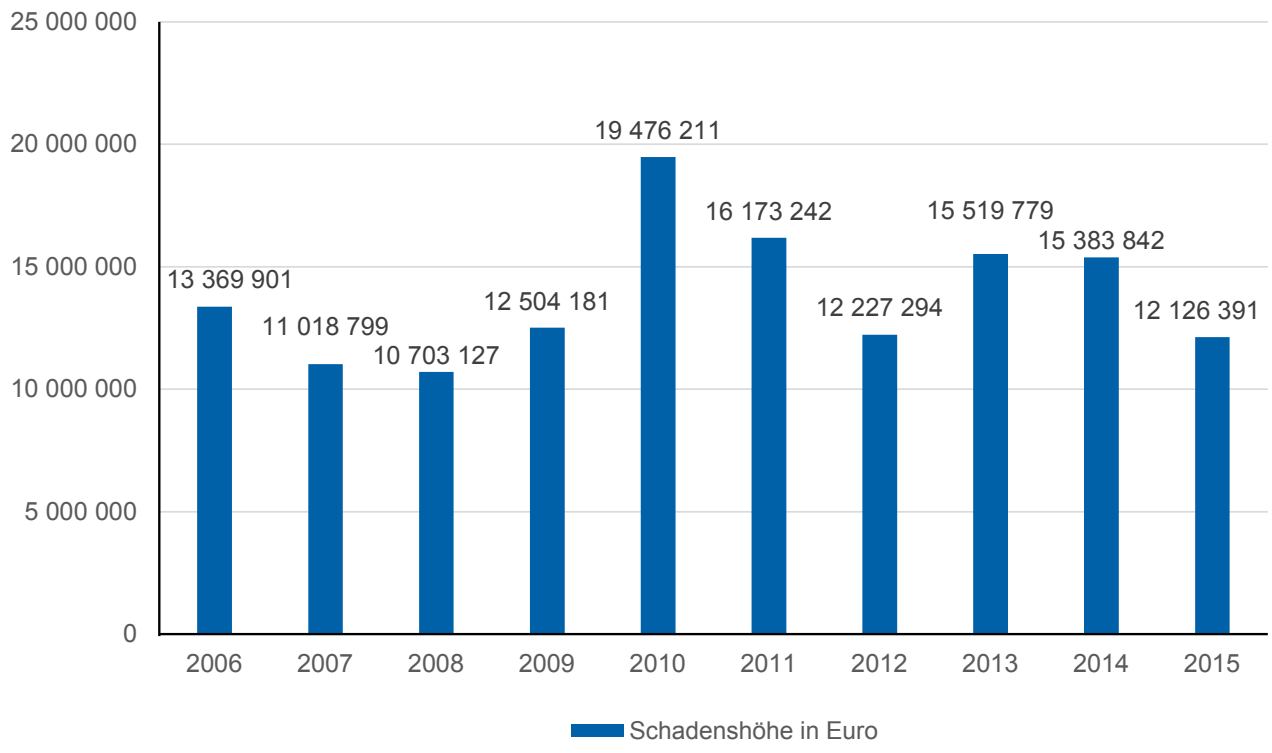
11 PIN: personal identification number; persönliche Geheimzahl.

12 Netzwerkgerät zur Anbindung von Netzwerken und Endgeräten an das Internet.

1.5 Schadensentwicklung

Die Gesamtschadenssumme der erfassten Cybercrime-Delikte im engeren Sinne sinkt für das Jahr 2015 um 21,2 Prozent auf 12 126 391 Euro. Diese Reduzierung ist vor allem auf die mit 7 000 000 Euro deutlich geringere Schadenssumme des Deliktsbereichs Computerbetrug (2014: 9 800 000 Euro) zurückzuführen.

Abbildung 04
Schadensentwicklung



1.6 Tatmittel Internet

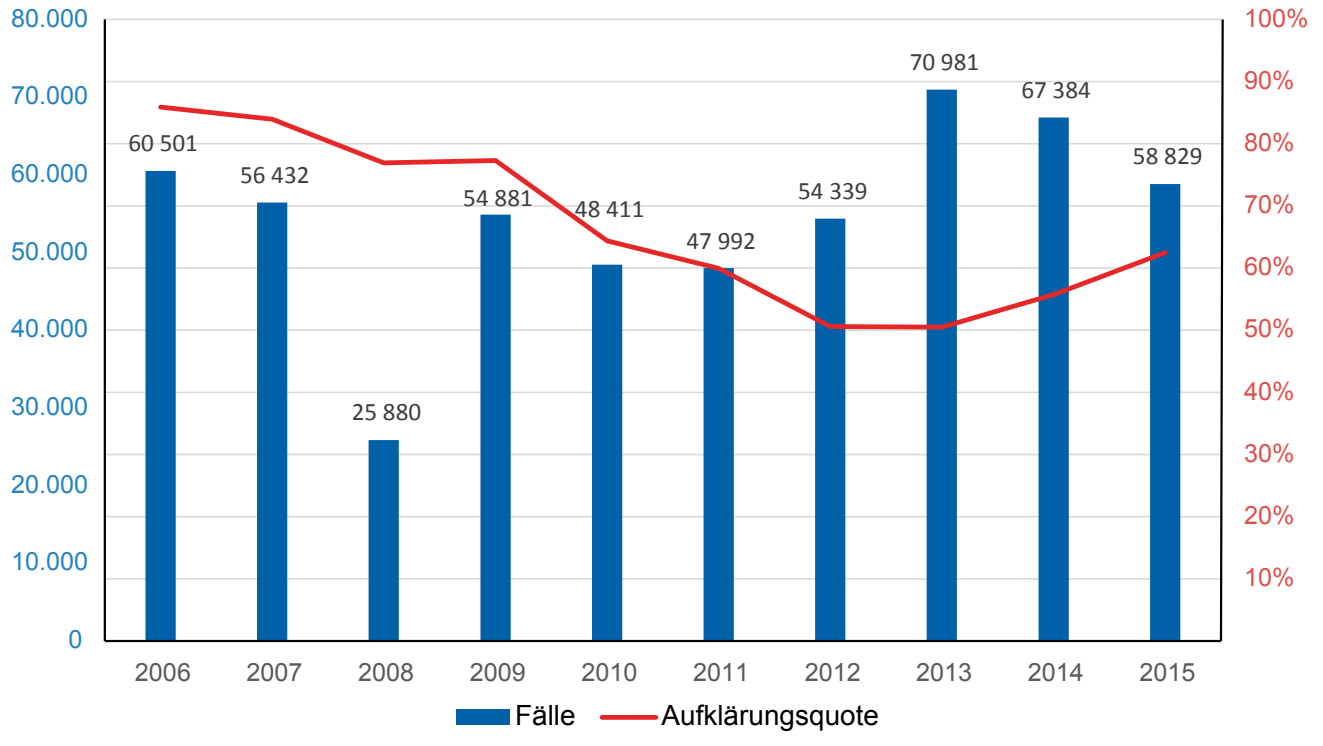
Mit der Sonderkennung „Tatmittel Internet“ werden in der PKS Straftaten erfasst, zu deren Tatbestandsverwirklichung das Medium Internet als Tatmittel verwendet wird. Neben den sogenannten Veräußerungs- und Verbreitungsdelikten, bei denen das bloße Einstellen von Informationen in das Internet bereits Tatbestände erfüllt, kommen auch Delikte in Betracht, bei denen das Internet zur Tatausführung genutzt wird.

Spielt das Internet bei der Tat eine untergeordnete Rolle, beispielsweise wenn Kontakte zwischen Täter und Opfer über das Internet der eigentlichen Tat lediglich vorgelagert sind, ist die Sonderkennung „Tatmittel Internet“ nicht zu verwenden.

Im Jahr 2015 wurden 58 829 und damit 12,7 Prozent weniger Fälle mit der Sonderkennung „Tatmittel Internet“ erfasst als 2014 (67 384). Die Anzahl der aufgeklärten Fälle ging um 783 auf 36 775 zurück. Durch die Abnahme der Fälle insgesamt stieg die Aufklärungsquote auf 62,5 Prozent (2014: 55,7 Prozent). Der Anteil der Straftaten mit dieser Sonderkennung an der Gesamtkriminalität sank auf 3,9 Prozent (2014: 4,5 Prozent).

74,2 Prozent der Straftaten dieser Sonderkennung entfielen auf Betrugsdelikte. Die anhaltende Abnahme der Ransomware führt dazu, dass die Erpressungen mit dem „Tatmittel Internet“ auf 433 Fälle zurückgingen (2014: 514).

Abbildung 05
Tatmittel Internet

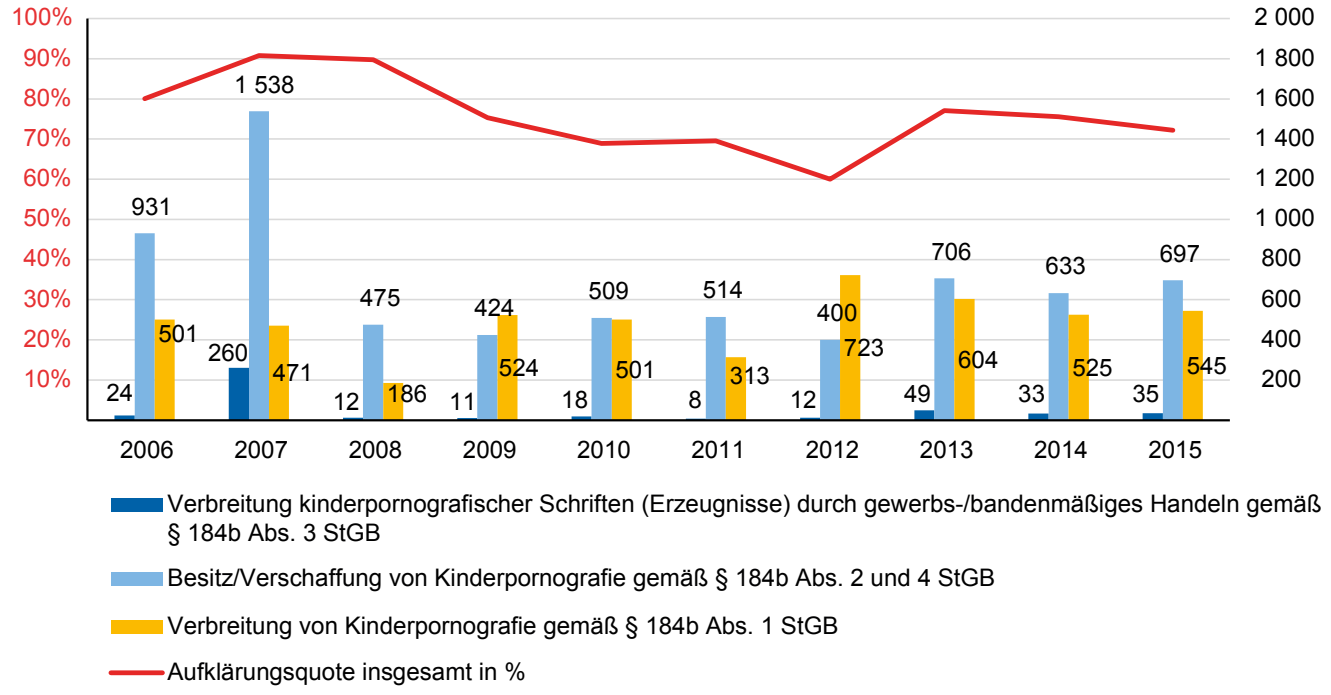


Kinderpornografie

Die Fallzahlen im Deliktsbereich „Verbreitung, Besitz und Verschaffung von Kinderpornografie“ sind zum Teil großen jährlichen Schwankungen der bekannt gewordenen Straftaten unterworfen, was insbesondere auf den Zeitpunkt des Abschlusses von Umfangsverfahren mit einer Vielzahl von Einzeltaten zurückzuführen ist. Die Anzahl der Fälle von Besitz, Verschaffung oder Verbreitung von Kinderpornografie erhöhte sich geringfügig auf 1 505 Fälle (+89, 2014: 1 416), darunter 41 Fälle der gewerbs- bzw. bandenmäßigen Verbreitung von Kinderpornografie (40).

Der PKS 2015 kann entnommen werden, dass das Tatmittel Internet bei den Straftaten gegen die sexuelle Selbstbestimmung von 1 822 Fällen im Jahr 2014 auf 1 901 Fälle im Jahr 2015 gestiegen ist. Dies entspricht einer Steigerung von 4,2 Prozent. Das Tatmittel Internet spielte mit einem Anteil von 84,9 Prozent auch im Jahr 2015 bei Delikten der Kinderpornografie eine herausragende Rolle. Insgesamt wurden im Deliktsbereich Kinderpornografie mit Tatmittel Internet im Jahr 2015 1 277 Fälle (1 191) erfasst. Dies entspricht einer Zunahme um 86 Fälle. Die Aufklärungsquote betrug 72,2 Prozent (75,6 Prozent).

Abbildung 06
Kinderpornografie mit Tatmittel Internet



2 Ausgewählte Phänomene

2.1 Identitätsdiebstahl/ID-Theft

Der Diebstahl von digitalen Identitäten nimmt, wie auch in den Jahren 2013 und 2014, den Großteil aller erfassten Fälle der Cybercrime im Vorgangsbearbeitungssystem der Polizei NRW ein.

Um an die Identitäten potentieller Opfer zu gelangen, sind der Kreativität der Täter kaum Grenzen gesetzt. Ständig den aktuellen Sicherheitsvorkehrungen angepasst, entwickeln sie ausgeklügelte Angriffs- und Täuschungsmethoden. Dabei nutzen sie immer effektiveres, auf die entsprechenden Ziele (Targets) abgestimmtes Social-Engineering. Die klassischen Methoden wie Phishing, Hacking, manipulierte Internetseiten oder schadhafte E-Mail-Anhänge sind bei den Tätern weiterhin beliebt und erfolgsversprechend. Das Interesse gilt insbesondere Bankdaten und E-Mail-Konten aber auch Zugangsdaten zu Kommunikationsdiensten, Verkaufsplattformen, sozialen Netzwerken oder Online-Spielen. Jeder Geschäftsprozess im Internet erfordert das Verifizieren mit persönlichen Daten, dies bietet den Tätern vielzählige Chancen eines Angriffs. Bei der Erlangung gestohlener Identitäten spielt weiterhin die Underground-Economy eine große Rolle. Die Möglichkeit, anonym und technisch abgeschottet große Mengen an digitalen Identitäten käuflich zu erwerben, bietet auch Tätern ohne spezialisiertes Fachwissen eine lukrative Chance, sich mit gestohlenen Identitäten zu bereichern. Die Erlangungstat, also das Stehlen der digitalen Identität, wird dabei nicht zwangsläufig durch denselben Täter begangen wie der spätere missbräuchliche Einsatz der digitalen Identität.

Fall:
Der E-Mail Zugang des Geschädigten wurde auf unbekannte Art und Weise übernommen. Die anschließende Anforderung neuer Passwörter für weitere Accounts durch den Täter führte zu einer kompletten Übernahme der vorhandenen digitalen Identitäten.

Freunde des Geschädigten wurden über ein soziales Netzwerk mit der Aufforderung angeschrieben, der Geschädigte solle sich beim Täter melden, um einer anschließend formulierten Geldforderung nachzukommen. Würde dies nicht geschehen, wurde mit dem Missbrauch der digitalen Identiät und der Löschung der persönlichen Daten gedroht. Eine zwischenzeitliche Rückerlangung des ursprünglich übernommenen E-Mail Zuganges durch den Geschädigten führte dazu, dass der Täter über eine hinterlegte Ausweiskopie erneuten Zugriff auf den E-Mail-Zugang erwirken konnte. Der Geschädigte stellte im Anschluss fest, dass seine Accounts missbräuchlich benutzt wurden. Hierbei wurden unter anderem persönliche Profile in sozialen Netzwerken verändert, Warenbestellungen getätigt und sich in Online-Spiele eingeloggt.

2.2 Angriffe gegen das Online-Banking

Der Angriff auf das Online-Banking stellt einen Spezialfall des digitalen Identitätsdiebstahls dar. Die Tat zielt auf den unbefugten Zugang zu einem Online-Banking Angebot einer Bank und dessen Missbrauch ab.

Wie im Jahr 2014 sind bei den Angriffen gegen das Online-Banking die Modi Operandi vielfältig. Trotz Sicherheitsvorkehrungen seitens der Banken gelingt es den Tätern immer wieder, Schwachstellen zu finden und die Unachtsamkeit der Geschädigten auszunutzen. Für einen Angriff vorrangig notwendig ist das Ausspähen von Kundendaten. Dafür wird Schadsoftware eingesetzt, die in das System der Geschädigten eingeschleust werden kann (Drive-by-Download[13], E-Mail-Anhänge, manipulierte Websei-

[13] Durch Sicherheitslücken von Browsern lädt sich das Programm beim Besuch der Seite selbst auf den Rechner des Anwenders.

ten). Wird ein Bankkunde mit kompromittiertem System aktiv und öffnet das Online-Banking seiner Bank, treten die Angreifer in Aktion. So werden beispielsweise Testüberweisungen, Sicherheitsüberprüfungen oder die neue Eingabe der persönlichen Daten vorgegaukelt. Diese Aktion muss dann mit der Eingabe einer oder mehrerer TAN validiert werden. Diese freigegebenen TAN werden täterseitig für Überweisungen vom angegriffenen Konto genutzt.

Das zur Erhöhung der Sicherheit eingerichtete mTAN-Verfahren, bei dem bei einer Aktion (Überweisung etc.) die benötigte TAN via SMS an den Kunden versendet wird, kann durch das Austellen weiterer SIM-Karten und eine Rufnummerportierung überwunden werden. Die TAN wird so an die Täter versendet und anschließend für Vermögensverfügungen genutzt.

Fall:
Die Geschädigte erhielt eine E-Mail, deren Absender und Aufmachung sie glauben ließ, es handele sich um eine E-Mail ihrer Bank. Darin wurde sie zum Abgleich ihrer persönlichen Daten und zum Anklicken eines Links aufgefordert. Die im Anschluss geöffnete Webseite erweckte den Eindruck einer bankentypischen Eingabemaske. Die Geschädigte kam der Aufforderung nach und pflegte ihre persönlichen Daten sowie die Zugangsnummer und PIN ihres Kontos ein. Am darauffolgenden Tag erhielt sie einen Anruf von einer Person, die sich als Mitarbeiterin ihrer Bank ausgab. Die Person bezog sich auf die am Vortag übermittelten Daten und glich diese mit der Geschädigten ab. Um den Vorgang abzuschließen, wurden zwei Nummern der TAN-Liste gefordert. Die Geschädigte übermittelte die geforderten TAN, mit denen am selben Tag 5 700 Euro auf ein ausländisches Konto überwiesen wurden.

2.3 Ransomware

Unter dem Begriff Ransomware wird eine Vielzahl von Schadprogrammen erfasst, die Computersysteme sperren oder Daten verschlüsseln und den Nutzer zur Zahlung eines Lösegeldes (engl. ransom) über elektronische Zahlungssysteme auffordern.

Der letztjährig festgestellte starke Rückgang dieses Phänomens hält unvermindert an und hat eine zum Teil deutliche Abnahme der in der PKS erfassten Fallzahlen für die Delikte Datenveränderung, Computersabotage sowie Erpressung mit Tatmittel Internet zur Folge. Der „BKA-Trojaner“ und seine Varianten (u. a. GVU-Trojaner) werden nur noch selten registriert, wobei die noch vorhandenen Angriffe sich vermehrt auf mobile Geräte (Smartphone, Tablet-PC) konzentrieren. Die Sensibilisierung der Bevölkerung sowie verbesserte Antiviren-Produkte sind hierbei wesentliche Einflussfaktoren. Obwohl ein Rückgang der Fallzahlen in 2015 erkennbar ist, kann von einer Zunahme der gezielten Angriffe gesprochen werden. Dies verdeutlicht die Veränderungsdynamik und Anpassungsfähigkeit der Cybercrime. Die Geschädigten, häufig Firmen, sollen nach Zusendung einer E-Mail unter Nutzung einer Legende (z. B. Zusendung von Bewerbungsunterlagen) dazu bewegt werden, den Dateianhang zu öffnen oder den enthaltenen Link anzuklicken. Der dadurch aktivierte Schadcode führt zur Verschlüsselung aller Dateien. Die Täter fordern für die Übermittlung eines Codes zur Entschlüsselung eine in der Regel dreistellige Summe, die in Form einer digitalen Währung (z. B. Bitcoin) entrichtet werden soll.

Fall:
Innerhalb eines Unternehmens öffneten Mitarbeiter die ZIP-Datei eines E-Mail-Anhangs. Das dadurch aktivierte Schadprogramm verschlüsselte alle Dateien, auf welche die Mitarbeiter zugriffsberechtigt waren. In den betroffenen Verzeichnissen lag eine Textdatei der Täter, die das Opfer darüber informierte, der Schlüssel zur Entschlüsselung werde nur gegen die Zahlung von 500 US-Dollar in der digitalen Währung Bitcoin übermittelt.

2.4 Phone-Scam

Das Phänomen Phone-Scam existiert seit einigen Jahren. Die Täter rufen die Opfer an und geben sich, häufig in englischer Sprache, als Support-Mitarbeiter von Softwarekonzernen oder Providern aus. Unter dem Vorwand, den angeblich von Viren befallenen Computer zu säubern, verschaffen sich die Täter mittels Fernwartungssoftware[14] Zugriff und können so unbemerkt Schadsoftware installieren. In der Folge kommt es zur Übernahme des Online-Bankings-Accounts, Ausspähen von Daten oder Verschlüsselung von Dateien.

Fall:
Die Geschädigte erhielt einen Warnhinweis auf ihren PC, dass dieser mit Viren infiziert sei. Über eine angegebene Telefonnummer erhalte man Informationen zur Lösung des Problems. Bei Anruf meldete sich ein angeblicher Support-Mitarbeiter eines Softwarekonzerns, der anbot, die Viren per Remote-Zugriff zu entfernen. Die Geschädigte ließ sich auf die Installation einer Fernwartungssoftware ein und ermöglichte dem Täter damit den Zugriff auf ihren PC. Durch geschickte Gesprächsführung und das Aufbauen eines Bedrohungszenarios gab die Geschädigte schließlich ihre Kreditkartendaten preis. Es kam zu einem Schaden von 210 Euro. Dieser bislang unbekannte Modus Operandi suggerierte den Geschädigten, dass der Zugriff auf den Computer und die Nachricht tatsächlich von einer authorisierten Stelle stammte.

Einige Geschädigte wurden zusätzlich als Finanzagenten angeworben und sollten Gelder, welche betrügerisch mittels Angriffen auf das Online-Banking erlangt wurden, weiterleiten.

2.5 Manipulation von Telekommunikationsanlagen

Die Manipulation von Telekommunikationsanlagen wird in der Regel unter dem Betrug mittels Zugangsberechtigung zu Kommunikationsdiensten erfasst (siehe Nr. 1.3).

Dieses Delikt weist 2015 die einzige Steigerung (2,0 Prozent) unter den Straftaten der Cybercrime im engeren Sinne auf. Die in der PKS erfasste Schadenssumme ging gleichzeitig um 57,2 Prozent auf nun 256 000 Euro (597 000 Euro) zurück.

Die Angriffe auf Telekommunikationsanlagen erfolgen vorzugsweise am Wochenende oder außerhalb der Arbeitszeiten über bekannte Schwachstellen in der Software und werden durch schwache oder nicht vorhandene Zugangssicherungen begünstigt. Hat der Täter die Kontrolle über die Anlage, werden kostenintensive Auslandstelefonverbindungen generiert und sogenannte Premium- bzw. Mehrwertdienste in Anspruch genommen. Die dabei erzielten Umsätze fließen den Tätern mittel- oder unmittelbar zu. Neben den Telekommunikationsanlagen von Firmen gehören auch die Router von Privathaushalten zu den Angriffszielen. Der Telekommunikationsanlagenmanipulation kann mit einfachen und zugleich effektiven Präventionsmaßnahmen begegnet werden. Die Anlage sollte stets auf dem aktuellen technischen Stand gehalten und mit der neuesten Software/Firmware betrieben werden. Werksseitige Standardpasswörter sollten durch einen individuellen starken Zugangscode ersetzt werden. Viele Telekommunikationsanlagen und Provider bieten die Möglichkeit einer Drittanbietersperre, welche die Nutzung teurer Premium- und Mehrwertdienste unterbindet. Eine Auslandsrufnummernsperre ist ein weiteres effektives Mittel, den Schaden im Falle eines Angriffs gering zu halten.

Die stark rückläufigen Schadenssummen für diesen Deliktsbereich lassen vermuten, dass die in den vergangenen Jahren mit Kooperationspartnern publizierten Präventionsmaßnahmen greifen.

[14] Programme, die eine räumlich getrennte Reparatur oder Wartung eines Systems ermöglichen.

3 Gesetz zur Einführung einer Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten

Am 18.12.2015 trat das Gesetz zur Einführung einer Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten in Kraft. Es verpflichtet die Telekommunikationsunternehmen spätestens 18 Monate nach dem 18.12.2015 zur Speicherung der darin genannten Daten.

Mit der vollumfänglichen Datenverfügbarkeit ist ab Mitte September 2017 zu rechnen. Mit dem Gesetz ist nun auch die Datenhehlerei unter Strafe gestellt (§ 202d StGB). Der Gesetzgeber beabsichtigt damit vor allem Schutzlücken zu schließen, wenn ausgespähte, abgefangene oder in anderer Weise rechtswidrig erlangte Daten gehandelt werden. Bisher war der Handel mit illegal erlangten Daten in der Regel straflos.

4 Prävention

Die Prävention von Cybercrime obliegt in Nordrhein-Westfalen den Kreispolizeibehörden. Das Landeskriminalamt unterstützt die Kreispolizeibehörden insbesondere durch

> Erhebung des kriminalpräventiven Handlungsbedarfs

> Fortschreiben von Standards und Entwickeln von Medien

> Initiieren und Koordinieren von überregionalen Präventionsmaßnahmen.

Bei der polizeilichen Präventionsarbeit stehen verhaltensorientierte Ansätze im Vordergrund. Diese werden durch Workshops, Vorträge oder Projekte verfolgt.

Das Cybercrime-Kompetenzzentrum des LKA führte im Jahr 2015 Vortragstätigkeiten bei verschiedenen Veranstaltungen von Behörden und in der Wirtschaft durch. Der Besuch von Großveranstaltungen wie der CeBIT 2015 und dem Deutschen Präventionstag 2015 wurden genutzt, um mit Vorträgen und Informationsständen die breite Öffentlichkeit zu erreichen.

Am 21. Oktober 2015 fand im Congress Center Düsseldorf der Kongress Cybercrime unter dem Motto „Cybercrime - Eine Herausforderung für die Innere Sicherheit“ statt. Renommierte Experten aus Wirtschaft, Politik, Wissenschaft, Justiz und Polizei tauschten sich über aktuelle Themen der Cybercrime aus. Die Schnelllebigkeit und Komplexität des Deliktsbereichs erfordern, dass die Polizei weitere Akteure in die Bewältigung dieser Aufgabe einbindet. Durch die Kooperationen mit dem Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) und VOICE Bundesverband der IT-Anwender e.V. konnten Präventionsinhalte im vergangenen Jahr effizient einem großen Spektrum von Personen und Firmen zugänglich gemacht werden.

5 Fazit

Die Fallzahlen der Cybercrime sind zum zweiten Mal in Folge stark zurückgegangen. Dies lässt, wie auch im vergangenen Jahr, nicht auf eine veränderte Bedrohungssituation durch Cybercrime schließen. Nach wie vor finden täglich Angriffe statt.

In der medialen Berichterstattung fallen Begriffe wie Cyberwar, Cybercrime as a service oder Angriffe auf kritische Infrastrukturen. Die immer weitreichendere Vernetzung der Gesellschaft bietet den Tätern stets neue Angriffsmöglichkeiten. Eine klare Abgrenzung zwischen gewöhnlicher und digitaler Kriminalität fällt zunehmend schwerer. Professionelle Tätergruppen agieren international und schöpfen das Anonymisierungspotential in Gänze aus. Erschwerend kommt hinzu, dass Cybercrime mittlerweile auch ohne besonderes informationstechnisches Wissen verübt werden kann. Dieser Umstand erweitert den Täterkreis und führt dazu, dass die Strafverfolgungsbehörden größere Anstrengungen unternehmen müssen, Taten aufzuklären.

Der Rückgang der Fallzahlen in der PKS ist zum Teil auf die ab 2014 geänderten Erfassungsmodalitäten zurückzuführen. Danach sind Straftaten nur zu erfassen, wenn konkrete Anhaltspunkte für ein Täterhandeln innerhalb Deutschlands vorliegen (vgl. Nr. 1.1). Damit wird eine Vielzahl von bekannt gewordenen Straftaten – insbesondere die nicht aufgeklärten Straftaten - nicht in der PKS erfasst. Die Anzahl der E-Mails mit Schadprogrammen ist konstant hoch, während die Straftaten in diesem Bereich in den vergangenen beiden Jahren rückläufig sind.

Um zum Erfolg zu gelangen, ändern die Täter Methodik und Zielrichtung der Angriffe. Die auf Masse ausgelegte Ransomware führt immer seltener zum Erfolg. Die Täter kompensieren dies mit zunehmend gezielten Angriffen und der technischen Fortentwicklung der Schadprogramme. Es deutet sich zudem an, dass zunehmend Firmen und Behörden Ziel der Angriffe werden.

Die Komplexität und Dynamik der Cybercrime wird die Polizei auch in den kommenden Jahren vor Herausforderungen stellen, die nur durch das Zusammenspiel von Prävention und Repression und die schon bestehenden Kooperationen mit Verbänden, Wirtschaftsunternehmen sowie Forschung und Lehre zu bewältigen sein werden.

Mit der Verabschiedung des Gesetzes zur Einführung einer Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten reagiert der Gesetzgeber im Sinne der Strafverfolgungsbehörden. Ob das Gesetz eine Ermittlungserleichterung zur Folge haben wird, kann erst in den kommenden Jahren beurteilt werden.

In der Sonderausgabe der Streife „Cybercrime – Die Polizei NRW im Kampf gegen Computerkriminelle“[15] finden Sie weitere Informationen.

[15] http://www.polizei.nrw.de/artikel__12054.html

6 Anlagen

6.1 Datenbasis

Grundlage dieses Lagebildes sind Daten aus der 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 wurden die im polizeilichen Vorgangsbearbeitungssystem erfassten Datensätze ergänzend ausgewertet.

6.2 Tabellen – Polizeiliche Kriminalstatistik

Tabelle 01
Fallzahlen in einzelnen Deliktsfeldern der Cybercrime im engeren Sinne

Straftaten	2014	2015	in Zahlen	in %
Computerbetrug	6 026	5 289	- 737	- 12,2
Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung	2 625	2 092	- 533	- 20,3
Datenveränderung/Computersabotage	2 884	1 351	- 1 533	- 53,2
Ausspähen, Abfangen von Daten einschl.Vorbereitungs-handlungen	4 381	3 115	- 1 266	- 28,9
Betrug mittels rechtswidrig erlangter Debitkarte mit PIN	4 467	4 440	- 27	- 0,6
Betrug mit Zugangsberechtigungen zu Kommunikations-diensten	296	302	+ 6	+ 2,0
Softwarepiraterie private Anwendung	19	35	+ 16	+ 28,9
Softwarepiraterie - gewerbsmäßiges Handeln	17	21	+ 4	+ 23,5
Computerkriminalität insgesamt	20 715	16 645	- 4 070	- 19,6

Tabelle 02
Aufklärungsquoten

	Aufgeklärte Fälle		Aufklärungsquote in %		Zu-/ Abnahme
Straftaten	2014	2015	2014	2015	%-Punkte
Computerbetrug	1 491	1 688	24,7	31,9	+ 7,2
Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung	642	624	24,5	29,8	+ 5,4
Datenveränderung/Computersabotage	295	203	10,2	15,0	+ 4,8
Ausspähen, Abfangen von Daten einschl. Vorbereitungs-handlungen	470	455	10,7	14,6	+ 3,9
Betrug mittels rechtswidrig erlangter Debitkarte mit PIN	1 257	1 324	28,1	29,8	+ 1,7
Betrug mit Zugangsberechtigungen zu Kommunikations-diensten	115	47	38,9	15,5	- 23,3
Softwarepiraterie - private Anwendung	17	33	89,5	94,3	+ 4,8
Softwarepiraterie - gewerbsmäßiges Handeln	15	19	88,2	90,5	+ 2,2
Computerkriminalität insgesamt	4 302	4 393	20,8	26,4	+ 5,62

Tabelle 03
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 %
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
2015	16 645	- 19,6	4 393	26,4

Tabelle 04a
Entwicklung der Altersverteilung der Tatverdächtigen

	Tatverdächtige								
	Unter 14		14 bis <18		18 bis <21		Ab 21		
Jahr	Anzahl	in %	Anzahl	in %	Anzahl	in %	Anzahl	in %	insgesamt
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
2015	27	0,8	218	6,2	332	9,4	2 942	83,6	3 519

Tabelle 04b
Entwicklung der Altersverteilung der Tatverdächtigen

	Tatverdächtige												
	unter 21		21 bis <30		30 bis <40		40 bis <50		50 bis <60		Ab 60		
Jahr	Anzahl	in %	Anzahl	in %	Anzahl	in %	Anzahl	in %	Anzahl	in %	Anzahl	in %	insgesamt
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
2015	577	16,4	1 116	31,7	855	24,3	525	14,9	334	9,5	112	3,2	3 519

Tabelle 05
Tatmittel Internet

	erfasste Fälle	darunter Tatmittel Internet	
Straftaten	2015	Fälle	Anteil in %
Insgesamt	1 517 448	58 829	3,9
gegen die sexuelle Selbstbestimmung	9 845	1 901	19,3
> Verbreitung pornografischer Erzeugnisse	2 110	1 654	78,4
- Besitz/Verschaffen von Kinderpornografie	825	697	84,5
- Verbreitung von Kinderpornografie	639	545	85,3
Betrug	247 351	43 630	17,6
> Waren- und Warenkreditbetrug	82 991	30 032	36,2
> Computerbetrug	5 289	3 782	71,5
> Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten	302	156	51,7
Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung	2 092	1 506	72,0
Datenveränderung, Computersabotage	1 351	1 126	83,3
Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen	3 115	2 370	76,1
Erpressung	1 710	433	26,3

Herausgeber

Landeskriminalamt Nordrhein-Westfalen
Völklinger Straße 49
40221 Düsseldorf

Abteilung 4
Cybercrime-Kompetenzzentrum
Dezernat 41

Redaktion KOR Helmut Picko
Telefon +49 211 939-4100
Fax +49 211 939-194100
CNPol 07-224-4100

Dez41.LKA@polizei.nrw.de
www.lka.polizei.nrw.de