POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

bürgerorientiert ▪ professionell ▪ rechtsstaatlich

Cybercrime
Lagebild für NRW 2016

www.lka.polizei.nrw.de

Kriminalitätsentwicklung im Überblick
Cybercrime

> Allgemeiner Anstieg der Fallzahlen durch Änderung in den Erfassungsrichtlinien der Polizeilichen Kriminalstatistik

> Anstieg der Fälle von Datenveränderung/ Computersabotage
> Rückgang der Fälle von Missbrauch von Telekommunikationsdiensten

	2015	2016	Veränderung in %	
Computerkriminalität	**16 645**	**22 708**	**+ 36,4**	
Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei der Datenverarbeitung	2 092	1 879	- 10,2	
Datenveränderung/Computersabotage	1 351	1 764	+ 30,6	
Ausspähen, Abfangen von Daten einschl. Vorbereitunshandlungen gem. §§ 202a, 202b, 202c StGB	3 115	3 215	+ 3,2	
Computerbetrug	*	**15 799**		
Straftaten mit Tatmittel Internet	**58 829**	**57 241**	**- 2,7**	
Betrug mit Tatmittel Internet	43 630	40 905	- 6,2	
Erpressung mit Tatmittel Internet	433	557	+ 28,6	
Anzahl der aufgeklärten Fälle mit Tatmittel Internet	36 775	33 499	- 8,9	

* Durch die Änderungen der Erfassungsrichtlinie der PKS 2016 wurden neue PKS-Schlüsselzahlen eingeführt und erstmalig für den Bereich Computerkriminalität erfasst. Diese Zahlen sind mit denen aus 2015 nicht vergleichbar. Näheres siehe unter 1.1 und 1.6 Computerbetrug.

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 oder die mittels dieser Informationstechnik begangen werden. Diese Definition steht im Einklang mit internationalen Begriffsbestimmungen wie der Convention on Cybercrime des Europarats[1].

Dabei umfasst Cybercrime im engeren Sinne die Straftaten, bei deren Begehung Elemente der elektronischen Datenverarbeitung in den Tatbestandsmerkmalen enthalten sind. Dazu zählen:

> Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung §§ 269, 270 StGB

> Datenveränderung, Computersabotage §§ 303a, 303b StGB

> Ausspähen, Abfangen von Daten einschließlich Vorbereitungshandlungen gemäß §§ 202a, 202b, 202c StGB

> Verletzung des Urheberrechtsgesetzes durch Softwarepiraterie (privates Handeln und gewerbsmäßiges Handeln)

> Computerbetrug gemäß § 263a StGB:

- weitere Arten des Warenkreditbetruges
- Computerbetrug mittels rechtswidrig erlangter Zahlungskarten mit PIN
- Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten
- Computerbetrug mittels rechtswidrig erlangter sonstiger unbarer Zahlungsmittel
- Leistungskreditbetrug
- Missbräuchliche Nutzung von Telekommunikationsdiensten
- Überweisungsbetrug
- weitere Arten des Computerbetrugs

Das Lagebild Cybercrime stellt schwerpunktmäßig die Entwicklung der Cybercrime im engeren Sinne im Land Nordrhein-Westfalen (NRW) dar. Die Daten basieren auf Ermittlungsverfahren der Polizeibehörden in NRW, die nach einheitlichem Standard erhoben werden. Die im Überblick dargestellten und in Tabelle 1 näher erläuterten Zahlen beruhen auf Daten der Polizeilichen Kriminalstatistik (PKS). Einzelne Delikte, die mit Hilfe des Tatmittels Internet begangen werden, sind unter Nr. 1.7 gesondert dargestellt. Klammerwerte bei Zahlenangaben beziehen sich auf das Vorjahr, soweit nicht anders angegeben. In einzelnen Phänomenen ist von einem großen Dunkelfeld auszugehen, da der Polizei viele Straftaten nicht bekannt bzw. nicht zur Anzeige gebracht werden.

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

Nachdem die Anzahl der erfassten Cybercrime-Fälle zwei Jahre in Folge gefallen ist, ist sie im Berichtszeitraum stark angestiegen. Sie erreicht nach 2013 den zweithöchsten Stand seit Erfassung der Cybercrime.

Zum Anstieg beigetragen haben die erneuten Anpassungen der PKS-Erfassungsrichtlinien, die nun eine differenzierte Erfassung verschiedener Delikte des Computerbetrugs ermöglichen und eine Verschiebung von Fallzahlen aus dem Bereich der Betrugsdelikte mit Tatmittel Internet zur Folge hat. Die Fallzahlen sind daher mit den Vorjahren nicht unmittelbar vergleichbar. Die Zunahme der Fallzahlen ist aber auch auf eine höhere Anzeigenbereitschaft zurückzuführen, die durch die vereinfachten Anzeigenwege verursacht wurde (zum Beispiel Online-Anzeige und Zentrale Ansprechstelle Cybercrime im LKA).

Die Datenbasis für die Darstellung der einzelnen Phänomene stammt aus dem polizeilichen Vorgangsbearbeitungssystem (vgl. Nr. 6.1), da einige Erscheinungsformen aktueller Phänomene mithilfe der deliktisch orientierten Polizeilichen Kriminalstatistik nicht hinreichend beschrieben werden können. Als Beispiel kann das Verbreiten von Ransomware[2] durch Straftäter dienen, das je nach konkreter Ausprägung als Computersabotage, Datenveränderung oder Erpressung mit Tatmittel Internet erfasst werden kann.

Die Zahlen des Jahres 2016 sind nicht unmittelbar mit 2015 vergleichbar. Zur besseren Unterscheidung zwischen Betrug (§ 263 StGB) und Computerbetrug (§ 263a StGB) wurden für die statistische Erfassung getrennte Straftatenschlüsselzahlen eingerichtet, so dass diese Fälle nunmehr differenziert der Computerkriminalität zugeordnet werden können.

1.2 Verfahrensdaten

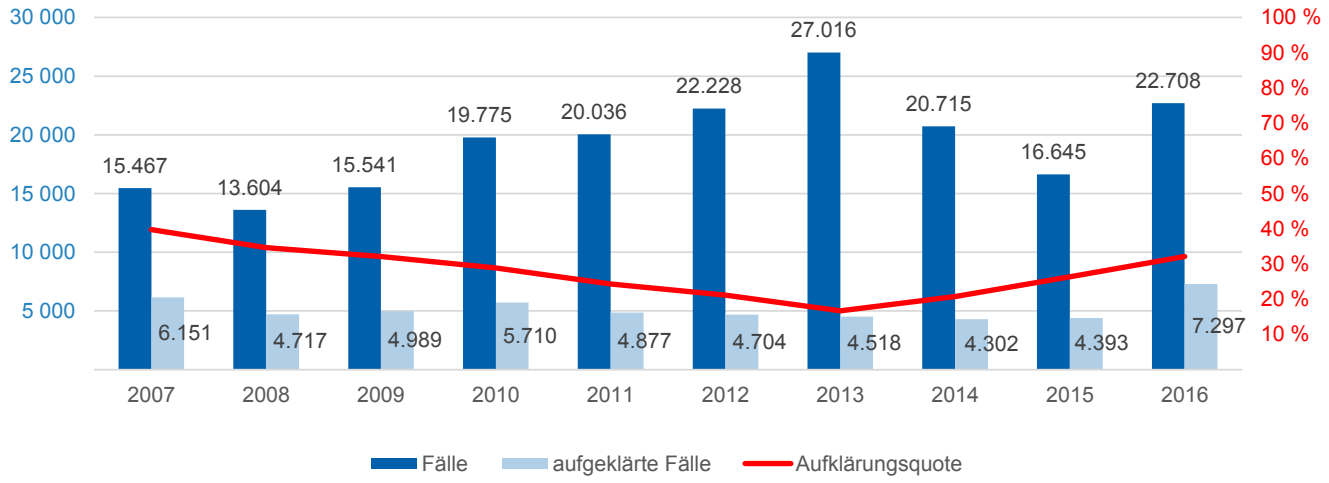
Nachdem die Zahl der erfassten Cybercrime-Fälle zwei Jahre in Folge gefallen ist, stieg sie im Jahr 2016 mit 22 708 Fällen stark an (16 645). Dies entspricht einer Steigerung um 6 063 Fälle (+ 36,4 Prozent). Sie erreicht damit nach 2013 den zweithöchsten Stand seit der Erfassung der Cybercrime. Die Aufklärungsquote stieg gegenüber dem Jahr 2015 um 5,7 Prozentpunkte auf 32,1 Prozent (26,4 Prozent). Die Zahl der ermittelten Tatverdächtigen stieg auf 5 790 (3 519). Zu den dominierenden Erscheinungsformen zählten im Jahr 2016 die vielschichtigen Begehungsweisen der Datenveränderung und Computersabotage sowie die verschiedenen Erscheinungsformen des Computerbetrugs.

[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 Aufklärungsquote

2016 wurden 7 297 Fälle der Cybercrime aufgeklärt. Die Aufklärungsquote lag bei 32,1 Prozent und überstieg damit die Vorjahresquote um 5,7 Prozentpunkte (26,4 Prozent). Durch die geänderten Erfassungsrichtlinien fallen nun mehr Betrugsdelikte in den Bereich der Cybercrime. Diese lassen sich häufig besser aufklären als andere Straftaten. So wurden 53,4 Prozent des Warenkreditbetrugs und 84,6 Prozent des betrügerischen Erlangens von Kraftfahrzeugen aufgeklärt. 81,8 Prozent aller aufgeklärten Fälle der Cybercrime entfallen auf den Bereich des Computerbetrugs.

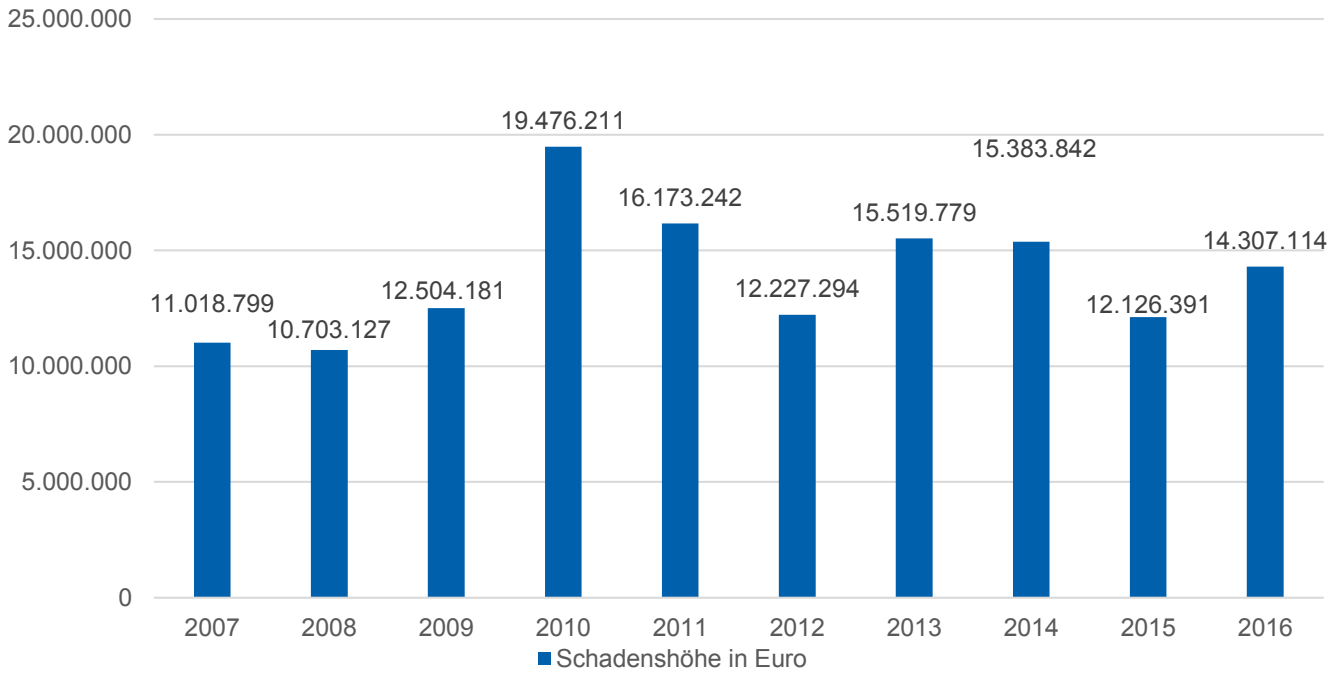
Abbildung 01
Vergleich Fallzahlen und Aufklärungsquote



1.4 Schadensentwicklung

Für die Cybercrime werden in der PKS nur für die Delikte des Computerbetrugs und der Softwarepiraterie Schäden registriert. Bei der Schadenssumme ist im Jahr 2016 ein Anstieg um 18 Prozent auf 14 307 114 Euro zu verzeichnen (12 126 391 Euro). Davon entfallen 13 952 597 Euro auf den Bereich Computerbetrug und 354 517 Euro auf die Softwarepiraterie.

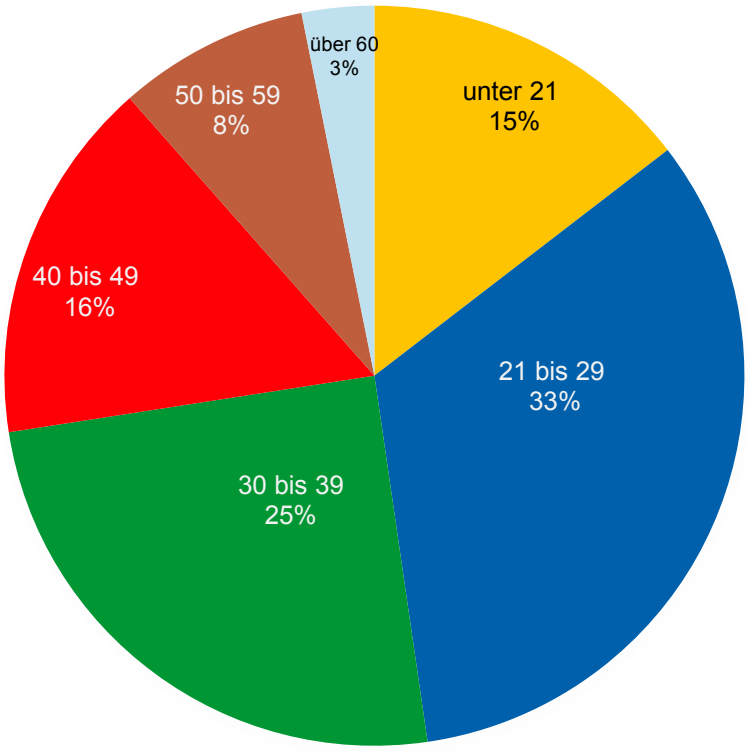
Abbildung 02
Schadensentwicklung



1.5 Täterstruktur

Die Zahl der ermittelten Tatverdächtigen im Bereich Cybercrime ist mit 5 790 auf dem höchsten Stand seit ihrer Erfassung. Dieser Anstieg deckt sich mit der Steigerung der Fallzahlen der Cybercrime. Von den erfassten Tatverdächtigen waren 30,4 Prozent Frauen. Der Anteil der Tatverdächtigen der 14- bis 21-Jährigen beträgt 14,6 Prozent. Die am stärksten vertretene Altersgruppe sind die 21- bis 29-Jährigen mit 33 Prozent. 52 Prozent der Straftaten werden von Tatverdächtigen begangen, die über 29 Jahre alt sind.

Abbildung 03
Altersstruktur der Tatverdächtigen



1.6 Einzelne Deliktsfelder

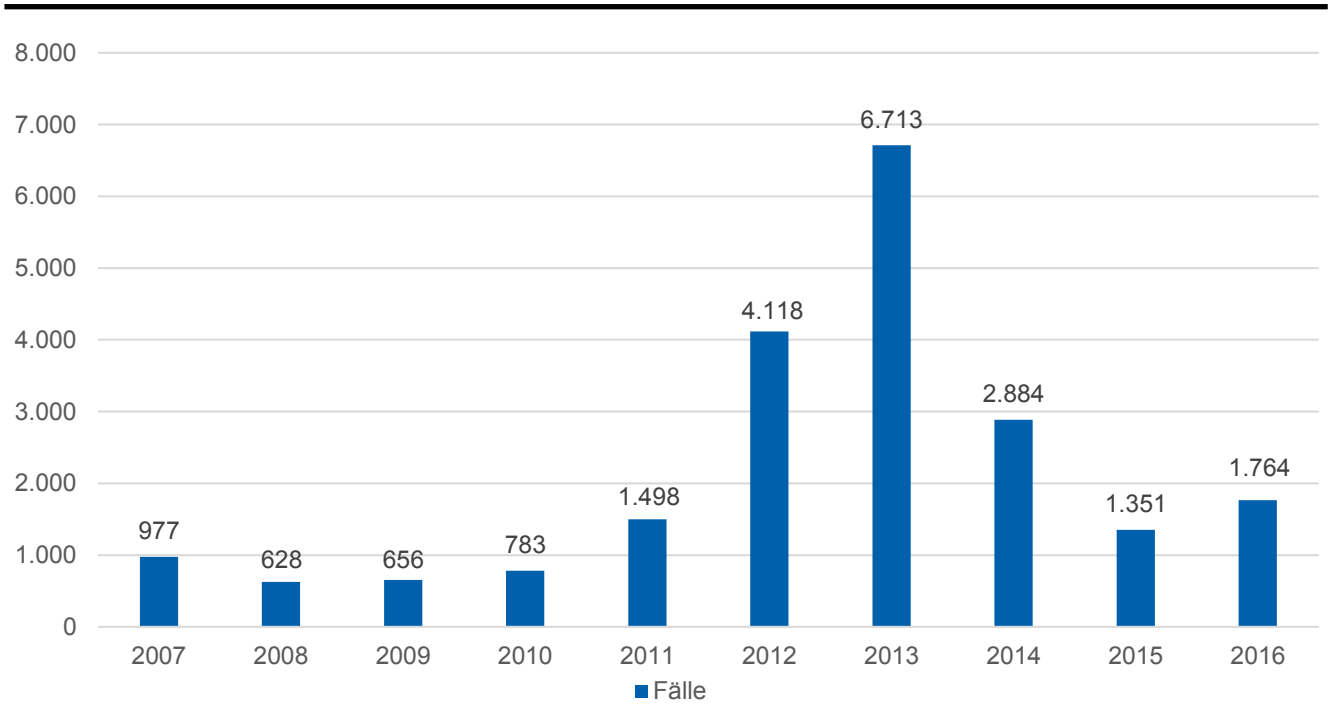
Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei der Datenverarbeitung (543000)

Im Jahr 2016 wurden 1 879 Fälle registriert, was einem erneuten Rückgang um 10,2 Prozent entspricht (2 092). Diesem Deliktsbereich liegt zumeist die Zusendung von E-Mails unter Vorspiegelung fremder, teils realer Identitäten zu Grunde. Die Opfer sollen zur Preisgabe von Zugangsdaten zu Onlinekonten, Kreditkartendaten oder zu Zahlungen bewegt werden.

Datenveränderung, Computersabotage (674200)

Die Zahlen dieses Deliktsbereichs sind im Jahr 2016 um 30,6 Prozent auf 1 764 Fälle angestiegen (1 351 Fälle). Dies stellt nach zwei Jahren des Rückgangs eine deutliche Steigerung dar. Der Anstieg dürfte hier auf das vermehrte Auftreten von Schadsoftware zurückzuführen sein. Bei Ransomware, die unter verschiedenen Namen vorkommt (wie Locky, Petya, Cerber, Goldeneye), wird die schädliche Software meist als E-Mail-Anhang versandt. Der Dateianhang ist zum Beispiel als Rechnung oder Bewerbung in Form einer Word- oder Excel-Datei getarnt. Wird der Dateianhang geöffnet und damit die Schadsoftware ausgeführt, verschlüsselt sie Dateien. Zur Entschlüsselung fordern die Täter meist ein „Lösegeld“ in Form digitaler Währungen, zum Beispiel Bitcoin.

Abbildung 04
Datenveränderung/Computersabotage



Ausspähen, Abfangen von Daten einschließlich Vorbereitungshandlungen (678000)

Im Jahr 2016 weist die PKS zu diesem Deliktsbereich 3 215 Fälle aus, was eine Steigerung um 100 Fälle bedeutet (3 115). Die dominierenden Erscheinungsformen sind hier verschiedene Account[3]-Ausspähungen (zum Beispiel digitale Identitäten, Benutzerkennungen, Kreditkarten- oder Kontodaten).

Computerbetrug (897100)

Die Neuregelungen zur Erfassung des Computerbetrugs betreffen folgende Straftaten: Betrügerisches Erlangen von Kraftfahrzeugen (511120), weitere Arten des Warenkreditbetruges (511212), Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten (516520), Leistungskreditbetrug (517220), Abrechnungsbetrug im Gesundheitswesen (518112) und Überweisungsbetrug (518302), jeweils soweit es sich um eine Straftat gemäß § 263a StGB handelt. Die bisherigen Delikte des Computerbetrugs mittels rechtswidrig erlangter Zahlungskarten mit PIN (516300), der Missbräuchlichen Nutzung von Telekommunikationsdiensten (517900) und des Sonstigen Computerbetrugs (517500) werden unverändert erfasst.

Zusätzlich wurde der Summenschlüssel 897100 zur Gesamtbetrachtung des Computerbetrugs gemäß § 263a StGB eingeführt. Unter diesem Summenschlüssel wurden 15 799 Straftaten erfasst.

Weitere Arten des Warenkreditbetruges (511212)

4 062 Fälle wurden erstmals unter der PKS-Schlüsselzahl 511212 erfasst, von denen 2 168 Fälle aufgeklärt werden konnten. Bei dieser Betrugsart wird zum Beispiel eine Ware über das Internet mit falschen Angaben zur Person oder zur Bankverbindung bestellt. Die Geschädigten erhalten keine Bezahlung, nachdem sie die Waren verschickt haben.

Computerbetrug mittels rechtwidrig erlangter Zahlungskarten mit PIN (516300)

Die Fallzahlen dieses Deliktbereiches sind mit 3 827 Fällen zurückgegangen (4 440). Seit 2016 werden Debitkarten und Kreditkarten unter dem einheitlichen Begriff Zahlungskarten erfasst. Der sorglose und unachtsame Umgang mit der PIN, die häufig als vermeintlich gut getarnte Telefonnummer oder auf einem Notizzettel mitgeführt wird, begünstigt die Tatausführung. In 538 Fällen gingen die Tathandlungen nicht über das Versuchsstadium hinaus (521).

Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten (516520)

Insgesamt wurden 1 894 Straftaten im Jahr 2016 registriert. Daten real existierender Zahlungskarten, die zum Teil aus Skimming- oder Phishing-Straftaten stammen, werden zum Beispiel im Darknet zum Kauf angeboten. Werden diese Daten später für Einkäufe im Internet eingesetzt, bemerken die Geschädigten den Schaden häufig erst bei der Kontrolle ihrer Kontoauszüge.

Computerbetrug mittels rechtswidrig erlangter sonstiger unbarer Zahlungsmittel (516920)

Dieser Deliktsbereich wies 432 Straftaten auf. Unbare Zahlungsmittel sind zum Beispiel PayPal-Konten, Guthabenkarten, Schecks oder Bonuskarten. In den meisten Fällen wurden Waren im Online-Handel bestellt und über ein zuvor gehacktes oder ausgespähtes PayPal-Konto bezahlt.

Leistungskreditbetrug (517220)

Für das Jahr 2016 wurden 1 046 Fälle registriert. Beim Leistungskreditbetrug erbringt der Verkäufer eine Leistung im Voraus. Der Täter bestellt diese Leistung über das Internet, zum Beispiel beauftragt er das Erstellen einer Webseite. Mit dem Täter wird eine spätere Zahlung vereinbart. Der Täter hatte von Anfang an nicht die Absicht zu zahlen. Oft werden von dem Täter falsche oder real existierende Personalien anderer Personen benutzt.

[3] Ein Benutzerkonto (englisch user account), kurz Nutzerkonto oder Account ist eine Zugangsberechtigung zu einem zugangsbeschränkten IT-System. Üblicherweise muss ein Benutzer sich beim Einloggen mit Benutzernamen und Kennwort authentifizieren. Über das Benutzerkonto identifiziert das System den einzelnen Benutzer. (Quelle: https://de.wikipedia.org/wiki/Benutzerkonto, Stand: 10.04.2017)

Sonstiger Computerbetrug (517500)

Die Zahlen in diesem Deliktsbereich gingen zum dritten Mal in Folge zurück. Für das Jahr 2016 wurden 3 780 Fälle erfasst, was einem Rückgang von 28,5 Prozent entspricht (5 289). Hierunter werden alle sonstigen Computerbetrugsdelikte registriert, soweit sie nicht unter den neu eingeführten Straftatenschlüsselzahlen erfasst werden können. Der Rückgang der Fallzahlen korreliert mit den neu eingerichteten Straftatenschlüsselzahlen.

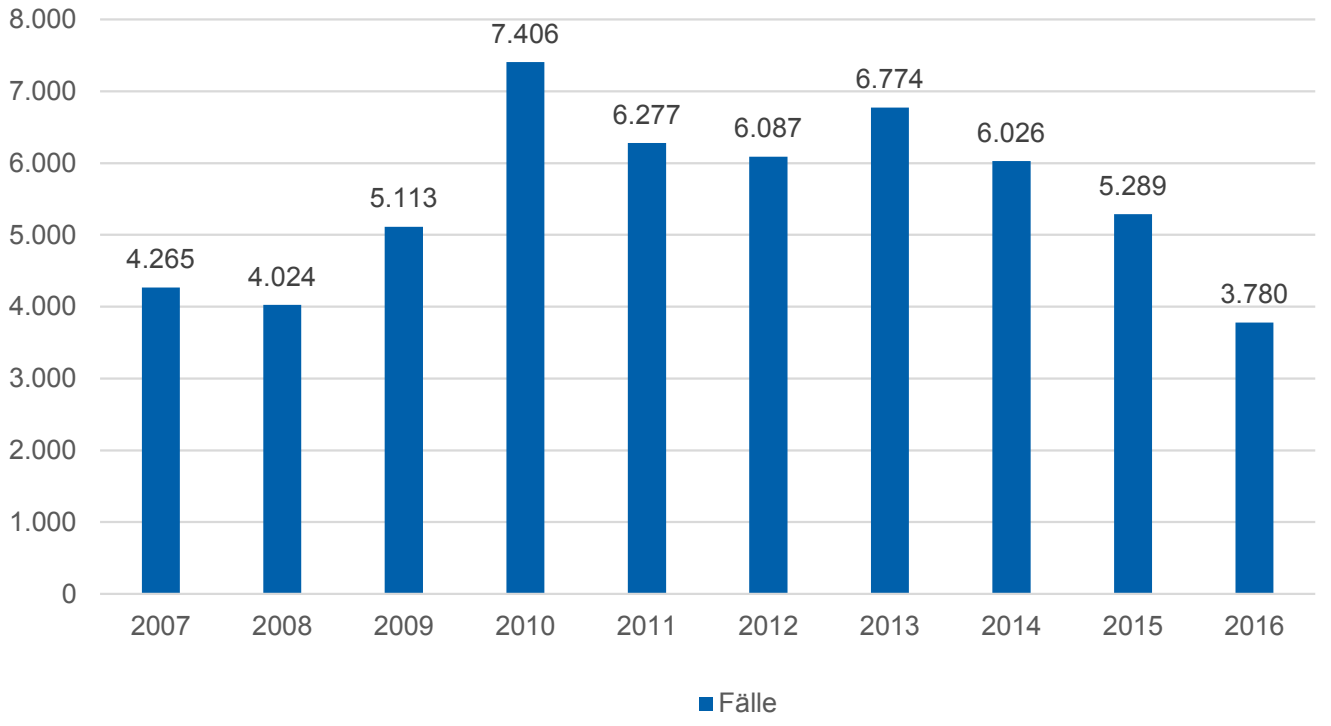
Missbräuchliche Nutzung von Telekommunikationsdiensten (517900)

Die Fälle aus diesem Straftatenbereich nahmen im letzten Jahr um 49,0 Prozent auf 154 ab (302). Der Schwerpunkt liegt nach wie vor auf der Manipulation von Telekommunikationsanlagen. Die Täter greifen unter Ausnutzung von Sicherheitslücken oder schwacher Zugangssicherungen (Standard-Passwörter) auf Router von Firmen oder Privatleuten zu und generieren teure Verbindungen in das Ausland oder zu Mehrwertdiensten. Trotz der gesunkenen Fallzahlen stieg der Gesamtschaden im Jahr 2016 auf 278 246 Euro (255 625 Euro).

Überweisungsbetrug (518302)

Im Jahr 2016 wurden 575 Fälle des Überweisungsbetruges registriert. Mit einer Quote von 20,9 Prozent war dieses Phänomen des Computerbetrugs am schwierigsten aufzuklären. Durch Einreichen einer ge- oder verfälschten Überweisung bzw. Zahlungsaufforderung wird dem kontoführenden Institut vorgetäuscht, der Kontoinhaber habe die Überweisung auf das Konto des Täters beauftragt. Erfolgt dieser Prozess automatisiert, ohne dass ein Mensch die Überweisung prüft und getäuscht wird, erfüllt dies den Tatbestand des § 263a StGB.

Abbildung 05
Sonstiger Computerbetrug



1.7 Tatmittel Internet

Straftaten, bei denen das Internet als Tatmittel verwendet wird, werden in der Polizeilichen Kriminalstatistik mit der Sonderkennung „Tatmittel Internet“ erfasst. Es kommen sowohl Straftaten in Betracht, deren Tatbestände durch das bloße Einstellen von Informationen in das Internet bereits erfüllt sind (so genannte Äußerungs- bzw. Verbreitungsdelikte), als auch solche Delikte, bei denen das Internet zur Tatbestandsverwirklichung genutzt wird.

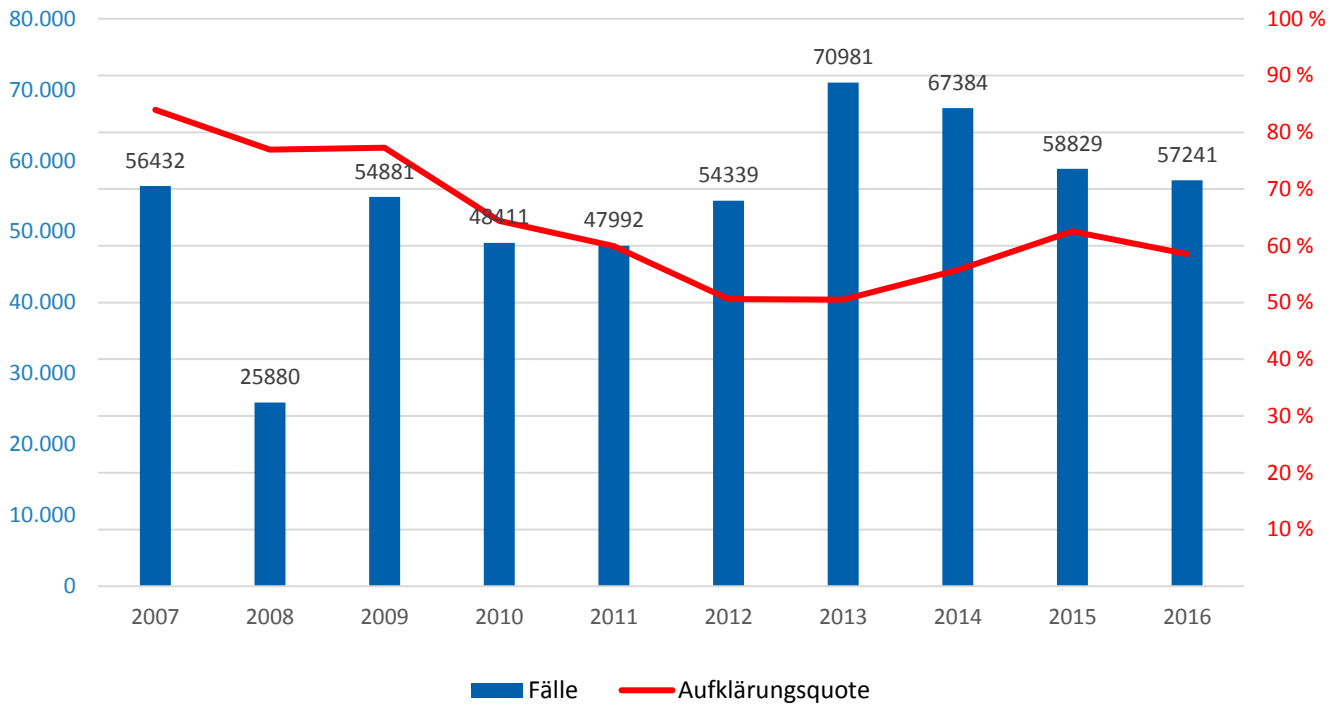
Spielt das Internet im Hinblick auf die Tatverwirklichung eine untergeordnete Rolle, wird die Sonderkennung „Tatmittel Internet“ nicht verwendet. Dies ist beispielsweise der Fall, wenn Kontakte zwischen Täter und Opfer mittels Internet im Vorfeld der eigentlichen Tat stattfinden.

Im Jahr 2016 wurden 57 241 Fälle (58 829) mit dieser Sonderkennung erfasst. Dies entspricht einem erneuten Rückgang um 2,7 Prozent. Der Anteil der Straftaten der Sondererkennung „Tatmittel Internet“ an der Gesamtkriminalität ist mit 3,9 Prozent gleich geblieben, da auch die Gesamtzahl aller Straftaten im Berichtszeitraum gesunken ist. Die Anzahl der aufgeklärten Fälle ging um 3 276 Fälle auf 33 499 zurück. Trotz des Rückgangs der Fallzahlen in dieser Sondererhebung fiel die Aufklärungsquote auf 58,5 Prozent (62,5 Prozent). Mit 71,5 Prozent der Fälle haben Betrugsdelikte den größten Anteil an dieser Sondererhebung. Der Anstieg der Erpressungen mit dem „Tatmittel Internet“ auf 557 Fälle (433) resultiert größtenteils auf die wieder angestiegene Zahl von Ransomware-Verbreitung.

Kinderpornografie

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 Einzel-

Abbildung 06
Tatmittel Internet



taten zurückzuführen ist. Darüber hinaus wurden im Zuge der letzten Strafrechtsreform zum § 184 b StGB (Verbreitung, Erwerb und Besitz kinderpornografischer Schriften) die der PKS zugrundeliegenden Schlüsselzahlen angepasst, sodass die Zahlen des Jahres 2016 nicht unmittelbar mit den Zahlen des Jahres 2015 vergleichbar sind.

Die Anzahl bekannt gewordener Fälle von Verbreitung, Erwerb, Besitz und Herstellung kinderpornografischer Schriften sank um 480 Fälle auf 1 025 Fälle (1 505). Dies entspricht einem Rückgang von 31,9 Prozent. Das Tatmittel Internet spielte dabei mit einem Anteil von 76,6 Prozent wieder eine bedeutende Rolle (84,9 Prozent).

Insgesamt wurden im Deliktsbereich Kinderpornografie mit Tatmittel Internet im Jahr 2016 785 Fälle (1 277) erfasst. Dies entspricht einem Rückgang um 492 Fälle (38,5 Prozent). Die Aufklärungsquote betrug 87,1 Prozent (72,2 Prozent).

2 Ausgewählte Phänomene

2.1 Identitätsdiebstahl (ID-Theft) und Angriff gegen das Online-Banking

Der „Diebstahl“ und der Missbrauch persönlicher Daten sind nach wie vor ein Massenphänomen. Der Alltag der Menschen verlagert sich immer mehr ins Internet. Dort werden Einkäufe und Bankgeschäfte getätigt, Reisen gebucht oder „Behördengänge“ erledigt. Viele dieser Handlungen im Internet erfordern die Angabe persönlicher Daten. Auch die freiwillige Herausgabe der eigenen Daten in den sozialen Medien stellt ein zunehmendes Problem dar. Diese Daten lassen sich problemlos im Internet finden.

Gängige Methoden wie Phishing, Hacking, manipulierte Internetseiten oder schadhafte E-Mail Anhänge stehen bei den Tätern nach wie vor hoch im Kurs. Das Interesse gilt insbesondere Bankdaten und E-Mail Konten aber auch Zugangsdaten zu Kommunikationsdiensten, Verkaufsplattformen, Sozialen Netzwerken oder Online-Spielen. Hat ein Krimineller genug Daten von seinen Opfern gesammelt, verkauft er diese entweder weiter, eröffnet damit beispielsweise einen Online-Shop oder bestellt Waren auf deren Namen.

Das „Stehlen“ der digitalen Identität (Erlangungstat) wird dabei nicht zwangsläufig durch denselben Täter begangen wie der missbräuchliche Einsatz der digitalen Identität (Verwertungstat). Die Möglichkeit, anonym und technisch abgeschottet große Mengen an digitalen Identitäten käuflich zu erwerben, bietet auch Tätern ohne spezialisiertes Fachwissen eine lukrative Möglichkeit, sich mit „gestohlenen“ Identitäten zu bereichern. Dabei spielt weiterhin die Underground-Economy eine große Rolle.

Fallbeispiel:
Die Täter gelangen an die Zugangsdaten eines Online-Shops, der über die Marketplace-Plattform von Amazon Waren anbietet. Die Täter stellen in kürzester Zeit hochwertige Produkte in diesem Shop ein und unterbieten mit Dumpingpreisen alle Wettbewerber. Sie setzten dabei auf den ausgeprägten Wunsch der Kunden, Schnäppchen zu machen. Der Bestellprozess wird kurz vor Beendigung abgebrochen und den Käufern dieser Produkte eine E-Mail zugestellt. Abweichend vom üblichen Zahlungsweg des Online-Shops erhalten die Kunden darin Bankdaten (meist von ausländischen Banken), an die sie den Kaufpreis überweisen sollen. Tatsächlich erhalten die geprellten Kunden trotz Zahlung nie ihre Ware.

Neben dem „Diebstahl“ von persönlichen Daten gelangen die Täter durch Phishing auch an Zugangsdaten für das Online-Banking. Hierfür werden allerdings noch die notwendigen Transaktionsnummern (TAN) zur Ausführung von Überweisungen benötigt. Die Einführung neuer Sicherheitsvorkehrungen wie mTAN[4], photoTAN[5] und TAN Generatoren zur Autorisierung von Finanztransaktionen erschweren ihnen den Zugriff auf die nur kurzzeitig verwendbaren Transaktionsnummern. Hier bieten sich aufgrund der steigenden Verbreitung von Smartphones und Tablets neue Angriffsvektoren. Die Täter greifen mobile Endgeräte gezielt mit spezieller Schadsoftware an. Gelingt es den Tätern, Zugriff auf die Konten der Geschädigten zu erhalten sowie deren mobile Endgeräte zu kompromittieren, können mTAN auf Mobilgeräte der Täter umgeleitet und Überweisungen durchgeführt werden.

2.2 Manipulation von Telekommunikationsanlagen

Die Manipulation von Telekommunikationsanlangen wird seit 2016 in der Statistik unter der geänderten PKS-Bezeichnung „Missbräuchliche Nutzung von Telekommunikationsanlagen“ erfasst. Im Vergleich zu den 302 Fällen aus dem Jahr 2015 hat sich die Anzahl der missbräuchlichen Nutzung von Telekommunikationsanlagen im Jahr 2016 auf 154 Fälle annähernd halbiert.

Dagegen ist die Schadenssumme mit 278 246 Euro fast auf Vorjahresniveau geblieben. Die typischen Angriffsmuster wurden auch im Jahr 2016 festgestellt. Hierzu zählen beispielsweise die Angriffe am Wochenende bzw. außerhalb der normalen Arbeitszeiten. Ferner werden die Angriffe durch bekannte Schwachstellen (Nebenstellen- und Fernwartungszugänge) und durch mangelnde Zugangssicherungen begünstigt (zum Beispiel Standard-PIN). Haben der oder die Täter die Kontrolle über die Telekommunikationsanlage erlangt, werden innerhalb kürzester Zeit kostenintensive Auslandstelefonverbindungen hergestellt und sogenannte Premium- bzw. Mehrwertdienste in Anspruch genommen. Neben den Telekommunikationsanlagen von Firmen gehören auch die Router von Privathaushalten zu den Angriffszielen.

Fallbeispiel:
Die geschädigte Firma wird durch ihren Netzbetreiber über Auffälligkeiten bei abgehenden Telefonaten in Kenntnis gesetzt. Sie teilten mit, dass seit drei Tagen erhebliche Gesprächskosten durch Anwahl von Auslandsrufnummern entstehen würden. Eine Überprüfung der Telefonanlage ergab einen offenen Port.

Die Täter riefen mehrfach über verschiedene ausländische Rufnummern den Anschluss der Firma an. Der Anrufbeantworter registrierte alle Anrufe und zeichnete diese auf. Die Täter riefen dann in der Nacht und am Wochenende wieder bei der Firma an. Mit dem Standardpasswort (0000) erhielten sie Zugang zur Steuerung des Anrufbeantworters. Über die Ausnutzung der Rückruffunktion des Anrufbeantworters führten sie Gespräche vom Anschluss der Firma auf die teuren Auslandsrufnummern. Dadurch generierten die Täter Gesprächskosten in Höhe von 12 000 Euro. Die Täter löschten anschließend alle Nummern auf dem Anrufbeantworter und vergaben neue Passwörter. Von der IT-Firma wurde der offene Port geschlossen.

Präventiv lässt sich der missbräuchlichen Nutzung von Telekommunikationsanlagen effektiv begegnen. Die Anlagen sollten immer auf dem neuesten technischen Stand sein und der Nutzer sollte regelmäßig ein Software- und Firmware Update durchführen. Werksseitig vergebene Standardpasswörter sollten durch ein individuelles sicheres Passwort ersetzt werden.

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

5 photoTAN: Nach Eingabe der Überweisungsdaten wandelt die Banksoftware die Transaktionsdaten in ein ca. 3 x 3 cm großes Bild aus kleinen Punkten um. Mittels Smartphone, auf dem sich eine photoTAN-App befindet, oder Lesegerät scannt der Bankkunde diese Grafik direkt vom Computerbildschirm ab. Die photoTAN-App auf dem Smartphone oder das Lesegerät wandeln die Bilddaten in eine 7-stellige Transaktionsnummer um. Mit Eingabe der so generierten Transaktionsnummer auf der Webseite der Bank wird die Überweisung frei gegeben.

Die Telefonanbieter sind gemäß § 45d TKG (Abs. 2 und 3) verpflichtet, Drittanbietersperren einzurichten. Hierdurch wird die Nutzung teurer Premium- und Mehrwertdienste unterbunden. Eine Auslandsrufnummernsperre ist ein weiteres effektives Mittel, den Schaden im Falle eines Angriffs gering zu halten.

2.3 Ransomware

Als Ransomware werden Schadprogramme bezeichnet, die Daten oder ganze Systeme verschlüsseln und den Zugriff darauf verhindern. Zur Freigabe wird die Zahlung eines Lösegeldes (engl.: ransom) gefordert. Die häufigste Angriffsmethode, über die Systeme verschlüsselt werden, sind schadhafte Anhänge in E-Mails.

Der letztjährig festgestellte starke Rückgang dieses Phänomens konnte dieses Jahr nicht beobachtet werden. Im Gegenteil, die Anzahl der in der PKS erfassten Fälle stieg für die Delikte Datenveränderung, Computersabotage auf 1 764 Fälle an (1 351). Die Zeit der massenhaft ungezielten Verbreitung von Spam-E-Mails scheint vorbei zu sein. Die Hersteller von Antivirenprogrammen haben ihre Produkte verbessert und die Bevölkerung ist zunehmend sensibler geworden, was den Versand von Spam E-Mail betrifft. Die Täter haben auf diese Veränderungen reagiert und verschicken gezielt E-Mails, die den Anschein von Seriosität haben. Die Täter betreiben auch im Vorfeld mehr Aufwand, um ihre Opfer auszuforschen.

Fallbeispiel: Verschlüsselungstrojaner
Ende des Jahres wurde der Verschlüsselungstrojaner Goldeneye gezielt an Personalstellen und -verantwortliche in Unternehmen und Behörden versandt. Die E-Mails erweckten den Anschein von Stellenbewerbungen auf konkrete Stellenausschreibungen. Es wurden nur Unternehmen angeschrieben, die auch tatsächlich neue Mitarbeiter suchten. Die E-Mails waren in fehlerfreiem Deutsch verfasst. Die Anrede passte zu der jeweiligen Zieladresse. Im Anhang befanden sich eine Excel-Datei und ein zur Bewerbung passendes PDF-Dokument. Beim Öffnen der Excel-Datei forderte das System zum Ausführen von Makros auf. Wurde dies bestätigt, begann die Schadsoftware mit der Verschlüsselung von Dateien und forderte im Nachgang ein Lösegeld zur Entschlüsselung.

Fallbeispiel: Ransomware-Angriff auf Krankenhäuser
Im Februar stellte ein Krankenhaus fest, dass Unbekannte in das interne Netz des Krankenhauses eingedrungen waren. Ein Schadprogramm verschlüsselte Dateien, sodass diese für den Krankenhausbetrieb unbrauchbar wurden. Ursache für die Störung war ein Ransomware-Trojaner, welcher durch einen infizierten E-Mail-Anhang in das IT-System des Krankenhauses gelangte.

Das Krankenhaus reagierte schnell: Um sensible Patientendaten zu schützen, wurden alle betroffenen Systeme sofort heruntergefahren. Auch der weitgehend digitalisierte Operationsbereich war betroffen, woraufhin sich die Klinikleitung entschied, alle Operationen zu verschieben.

Durch das schnelle Handeln der Klinikverantwortlichen wurde nur ein kleiner Teil der Daten verschlüsselt. Es entstand kein Schaden an Leib und Leben der Patienten. Allerdings waren die Auswirkungen des Angriffs auch Monate danach noch zu spüren. Die Kosten für die Analyse und Wiederherstellung des IT-Systems beliefen sich nach Angaben der Klinikleitung auf ca. eine Million Euro.

2.4 Botnetze und das Internet der Dinge (Internet of Things=IoT)

Das Internet hält immer mehr Einzug in alltägliche Dinge des Haushalts. Dazu zählen nicht nur herkömmliche Computer, sondern auch Haushaltsgeräte wie Smart-TV, Kühlschränke, Waschmaschinen, Überwachungskameras und sogar Babyphones. Diese werden mit einem kleinen Computer ausgestattet, um sich beispielsweise über das Internet fernsteuern zu lassen oder um Statusmeldungen abzusetzen.

All dies funktioniert nur, wenn diese Gegenstände mit dem Router der Besitzer verbunden sind. Sind die Besitzer nicht zuhause, senden die Geräte ihre Nachrichten auch über das Internet an das Smartphone. Weil diese Geräte mit dem Internet verbunden sind, spricht man vom Internet der Dinge.

Die Technikverliebtheit, der Wunsch, alles zu kontrollieren oder jederzeit über alles informiert zu sein und die nützlichen Seiten der Technik motivieren die Menschen dazu, diese „vernetzten“ Geräte zu kaufen. Laut einer Studie der Bitkom[6] aus dem Jahr 2015 wird die Anzahl der vernetzten Geräte bis 2020 auf 100 Millionen anwachsen. Dabei ist die eingebaute Verbindungstechnik zum Internet bei diesen Produkten nicht immer auf dem neuesten Stand. Über solche Sicherheitslücken kapern und manipulieren Hacker die Geräte. Die Besitzer merken nicht, dass ihre Fernseher und Kühlschränke zum Beispiel Spam-E-Mails verschicken und Teil eines Botnetzes geworden sind.

Fallbeispiele:

Nachdem Anfang Oktober der Quellcode des „mächtigen“ DDoS[7]-Tools Mirai veröffentlicht wurde, kam es zu mehren großen Angriffen auf Internetserver (siehe 2.5). Ende Oktober schafften es Hacker durch den Aufbau eines riesigen Botnetzes, bestehend aus mehr als einer Million ungesicherter Geräten, eine massive DDoS Attacke gegen US-Internetdienste durchzuführen. Teile des Ostens der USA und viele Menschen in Europa hatten über Stunden keinen Zugriff auf Amazon, Twitter, Spotify, Paypal und Netflix.

Auch Kunden eines großen deutschen Telefonkommunikationsanbieters wurden Ende des Jahres Opfer von Hackerangriffen. Die Angreifer versuchten über den Fernwartungszugang der firmeneigenen Internetrouter, sich dieser Router zu bemächtigen und daraus ein riesiges Botnetz aufzubauen. Dadurch hatten bis zu 900 000 Kunden der Telekom AG über mehrere Tage keinen Zugang zum Internet.

6 Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. https://www.bitkom.org/noindex/Publikationen/2015/Studien/CE-Studie-2015/150901-CE-Studie-2015-online.pdf - Seite 51.

7 DDoS: Distributet Denail of Service, verteilter Überlastungsangriff auf einen Internetserver, der daraufhin seinen Dienst einstellt. Der Server ist nicht mehr zu erreichen.

2.5 DDoS-Angriffe

DDoS-Angriffe sind ein Phänomenbereich, der auch 2016 verstärkt zu beobachten war. Dabei verschickten Tätergruppen gezielt per E-Mail Erpresserschreiben an Onlineshop-Betreiber oder Internetdienstleister. Darin kündigten Sie einen DDoS-Angriff an, wenn nicht bis zu einem bestimmten Zeitpunkt ein Lösegeld gezahlt würde. Die Zahlungen sollten in Form einer virtuellen Währung erfolgen, meist in Bitcoins.

Zur Untermauerung ihrer Fähigkeiten und der Ernsthaftigkeit der DDoS-Erpressung starteten einige Tätergruppierungen einen Testangriff, der Server des betroffenen Opfers kurzzeitig beeinträchtigte. Dadurch entstanden bei den betroffenen Unternehmen bereits finanzielle Schäden durch Umsatzeinbußen und durch die notwendige Installation von Abwehrmaßnahmen durch externe Dienstleister.

Für die Durchführung solcher DDoS-Erpressungen brauchen die Angreifer keine besonderen technischen Fähigkeiten. Das Knowhow und die Technik werden als Dienstleistungen im Internet in den Undergroundforen zum Kauf oder zur Miete angeboten (Crime-as-a-Service).

Fallbeispiel:
Die geschädigte Firma erhielt eine E-Mail mit erpresserischem Inhalt. In der anonymisierten E-Mail wird seitens einer unbekannten Gruppierung mit einem DDoS-Angriff auf die Webserver der Firma gedroht. Dieser Angriff sollte seitens der Firma durch Zahlung von 50 Bitcoins (BTC) bis zu einem bestimmten Datum verhindert werden können. (Am 31.12.2016 betrug der Kurswert von einem BTC 956,23 US-Dollar, ca. 885 Euro). Bei Weigerung sollte die Zahlung auf 75 Bitcoins erhöht und danach täglich um weitere 10 Bitcoin gesteigert werden. Die Täter gaben an, über sehr große Botnetze mit einem hohen Angriffspotenzial zu verfügen. Seitens der Firma wurde keine Zahlung geleistet. Ein Angriff fand nicht statt.

3 Datenhehlerei gemäß § 202d StGB

Seit dem 18.12.2015 ist der Straftatbestand der Datenhehlerei gemäß § 202d StGB eingeführt. Danach macht sich strafbar, wer Daten, die nicht allgemein zugänglich sind und die ein anderer durch eine rechtswidrige Tat erlangt hat, sich oder einem anderen verschafft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, um sich oder einen Dritten zu bereichern oder einen anderen zu schädigen.

Mit der Änderung wurde eine Anpassung des PKS-Straftatenkatalogs erforderlich. Zur Erfassung der Datenhehlerei wird 2017 die Straftatenschlüsselzahl 678040 eingerichtet. Diese gehört, neben den Schlüsselzahlen 678010 (Ausspähen von Daten), 678020 (Abfangen von Daten) und 678030 (Vorbereiten des Ausspähens und Abfangens von Daten), zu dem Oberschlüssel 678000 (Ausspähen und Abfangen von Daten einschließlich Vorbereitungshandlungen gemäß § 202a StGB). In 2016 wurde die Datenhehlerei unter den verschieden PKS-Schlüsselzahlen des Oberschlüssels 678000 erfasst.

4 Prävention

Die Prävention von Cybercrime obliegt den Kreispolizeibehörden. Das Landeskriminalamt NRW 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 NRW sensibilisierte im Jahr 2016 durch Vorträge bei verschiedenen Veranstaltungen von Behörden und in der Wirtschaft zu den Gefahren durch Cybercrime. Der Besuch von Großveranstaltungen wie der CeBIT 2016 und dem Deutschen Präventionstag 2016 wurden genutzt, um mit Vorträgen und Informationsständen die breite Öffentlichkeit zu erreichen. Am 01.06.2016 veranstalteten der Voice-Bundesverband der IT-Anwender e. V. und das LKA NRW den 2. Voice-IT-Sicherheitstag und schafften so einen Rahmen, in dem sich Experten aus Wirtschaft, Politik, Wissenschaft, Justiz und Polizei intensiv über aktuelle Themen der Cybercrime austauschen konnten.

Die Schnelllebigkeit und Komplexität des Deliktsbereichs erfordern, dass die Polizei weitere Akteure in die Bewältigung dieser Aufgabe einbinden muss. Durch die Kooperationen mit dem BITKOM und VOICE konnten Präventionsbotschaften auch im vergangenen Jahr effizient einem großen Spektrum von Personen und Firmen zugänglich gemacht werden. Im Rahmen der Sicherheitspartnerschaft Nordrhein-Westfalen wurde unter dem Motto „Unternehmenssicherheit ist Chefsache“ die Veranstaltungsreihe „Entscheider-Dialog“ mit mehreren Terminen für den Mittelstand umgesetzt.

5 Fazit

Nach wie vor finden täglich „Cyber Angriffe“ statt. In der medialen Berichterstattung fallen Begriffe wie Cyberwar, Crime as a service oder Angriffe auf kritische Infrastrukturen. Die immer weitreichendere Vernetzung der Gesellschaft bietet den Tätern stets neue Angriffsmöglichkeiten.

Die Anzahl der erfassten Cybercrime-Fälle ist, nach dem sie zwei Jahre in Folge gefallen ist, im Jahr 2016 wieder stark gestiegen. Ursächlich hierfür sind in weiten Teilen erneute Änderungen der PKS-Richtlinien mit sieben neuen PKS Schlüsselzahlen. So lassen sich Phänomene des Computerbetrugs nun wesentlich differenzierter erfassen als bisher. Ebenfalls zum Anstieg der Fallzahlen beigetragen hat ein geändertes Anzeigenverhalten der Bürgerinnen und Bürger. Die Lebenswelt bestimmter Bevölkerungsgruppen spielt sich zunehmend im Internet ab. Die Möglichkeit der Online-Anzeige wird daher viel eher wahrgenommen als die Anzeigenerstattung in einer Polizeiwache. So sind 12 275 Delikte als „Betrug im Internet“ im Jahr 2016 in Form der Online-Anzeige erstattet worden (1 931).

Eine klare Abgrenzung zwischen gewöhnlicher und digitaler Kriminalität fällt zunehmend schwerer. Die Bedrohungslagen werden immer komplexer und die Gefahren für die digitale Welt nehmen zu. Auf der einen Seite stehen intelligente, professionelle Tätergruppen mit innovativen kriminellen Vorgehensweisen, die international agieren und die Anonymität im Internet ausnutzen. Hier erschweren Zuständigkeitsregelungen, die an den Ländergrenzen enden, und die zunehmenden Möglichkeiten der Anonymisierung die Ermittlungsarbeit. Auf der anderen Seite stehen Cyberkriminelle, die über wenig bis gar keine speziellen informationstechnische Kenntnisse verfügen, aber denen der Einstieg in das kriminelle Milieu mit gekauften Baukästen (Tool-Kit) leicht gemacht wird. Software zum Start einer DDoS-Attacke oder zur Verbreitung von Ransomware kann inzwischen jeder mieten oder kaufen. Hier kommt der Underground-Community eine bedeutende Rolle zu.

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, verschwindet daher weiter und geht mit einem Anstieg gezielter Attacken einher. Durch Social Engineering gelangen hoch spezialisierte Tätergruppen vermehrt an Informationen zu Firmen, deren Personal, Organisationsabläufen und persönlichen Beziehungen des Personals untereinander. Durch Ausnutzung dieser Informationen erschleichen sich die Täter das Vertrauen ihrer Opfer. Dadurch wird den Tätern die Möglichkeit eingeräumt, Schadsoftware zu installieren oder sich unbefugten Zugriff auf ein Computersystem zu verschaffen. Privatpersonen sind hiervon nicht ausgenommen.

Das Internet der Dinge (IoT) wird zur Normalität werden. Nicht nur der internetaffine, sondern auch der weniger versierte Nutzer wird kaum noch ein Gerät ohne Vernetzungsmöglichkeiten erwerben können. Hier entwickelt sich eine Vielzahl von Angriffsvektoren in der Cybercrime, aber auch in der Allgemeinkriminalität (zum Beispiel Möglichkeiten zur Überwindung elektronischer Schließsysteme). Hersteller sollten im Bereich Smart-Home nicht auf den schnellen Profit setzen, sondern ihre Geräte gut vor solchen Angriffen schützen. Aber auch der Gesetzgeber sollte zur Einhaltung von Sicherheitsstandards Regularien schaffen, um die Bürger vor Schäden durch die Übernahme ihrer eigenen Geräte zu schützen.

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

6 Anlagen

6.1 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 die Straftaten der Cybercrime im engeren Sinne (siehe Nr. 1.1).

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 spezielles informationstechnisches Fachwissen auf Täterseite erforderlich ist,
- Täter besondere Techniken zur konspirativen Kommunikation (zum Beispiel Kryptografie[8] oder Steganografie[9]) nutzen,
- eine bundesweite oder internationale Bedeutung bestehen könnte,
- ein überdurchschnittlich hoher Schaden vorliegt oder
- ein neuer oder abweichender Modus Operandi festgestellt wird.

8 Verschlüsselung von Daten

9 Verborgene Speicherung oder Übermittlung von Informationen in einem Trägermedium (Container, zum Beispiel in Fotos).

6.2 Tabellen – Polizeiliche Kriminalstatistik

Tabelle 01
Fallzahlen in einzelnen Deliktsfeldern der Cybercrime im engeren Sinne
(Die freien Zellen in 2015 enthalten keine Zahlen, weil es diese PKS-Zahlen 2015 noch nicht gab.)

Straftaten	2015	2016	in Zahlen	in %
Betrügerisches Erlangen von Kfz § 263a StGB		26		
Weitere Arten des Warenkreditbetruges § 263a StGB		4 062		
Computerbetrug mittels rechtswidrig erlangter Zahlungskarten mit PIN § 263a StGB	4 440	3 827	- 613	-13,81
Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten § 263a StGB		1 894		
Computerbetrug mittels rechtswidrig erlangter sonstiger unbarer Zahlungsmittel § 263a StGB		432		
Leistungskreditbetrug § 263a StGB		1 046		
Computerbetrug (sonstiger) §263a StGB (soweit nicht unter den Schlüssel 511120, 511212, 516300, 516520, 516920, 517220, 517220, 517900, 518112 bzw. 518302 zu erfassen)	5 289	3 780	-1 509	-28,53
Missbräuchliche Nutzung von Telekommunikationsdiensten § 263a StGB	302	154	- 148	-49,01
Abrechnungsbetrug im Gesundheitswesen § 263a StGB		3		
Überweisungsbetrug § 263a StGB		575		
Computerbetrug insgesamt § 263a StGB		**15 799**		
Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung §§ 269, 270 StGB	2 092	1 879	- 213	-10,18
Datenveränderung, Computersabotage §§ 303a, 303b StGB	1 351	1 764	+ 413	+30,57
Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen gem. § 202a, 202b, 202c StGB	3 115	3 215	+ 100	+3,21
Softwarepiraterie (private Anwendung z.B. Computerspiele)	35	31	- 4	-11,43
Softwarepiraterie in Form gewerbsmäßigen Handelns	21	20	- 1	-4,76
Computerkriminalität insgesamt	**16 645**	**22 708**	**+6 063**	**+36,43**

Tabelle 02
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
2016	22 708	+ 36,4	7 297	32,1

Tabelle 03
Aufklärungsquoten

	Aufgeklärte Fälle		Aufklärungsquote in %		Zu-/ Abnahme
Straftaten	**2015**	**2016**	**2015**	**2016**	**%-Punkte**
Betrügerisches Erlangen von Kfz § 263a StGB		22		84,62	
Weitere Arten des Warenkreditbetruges § 263a StGB		2 168		53,37	
Computerbetrug mittels rechtswidrig erlangter Zahlungskarten mit PIN § 263a StGB	1 324	1 205	29,82	31,49	+1,67
Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten § 263a StGB		777		41,02	
Computerbetrug mittels rechtswidrig erlangter sonstiger unbarer Zahlungsmittel § 263a StGB		123		28,47	
Leistungskreditbetrug § 263a StGB		331		31,64	
Computerbetrug (sonstiger) §263a StGB (soweit nicht unter den Schlüssel 511120, 511212, 516300, 516520, 516920, 517220, 517220, 517900, 518112 bzw. 518302 zu erfassen)	1 688	1 190	31,92	31,48	-0,44
Missbräuchliche Nutzung von Telekommunikationsdiensten § 263a StGB	47	33	15,56	21,43	+5,87

Abrechnungsbetrug im Gesundheitswesen § 263a StGB		3		100,00	
Überweisungsbetrug § 263a StGB		120		20,87	
Computerbetrug insgesamt als neuer Summenschlüssel § 263a StGB		**5 972**		**37,80**	
Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung §§ 269, 270 StGB	624	612	29,83	32,57	+2,74
Datenveränderung, Computersabotage §§ 303a, 303b StGB	203	198	15,03	11,22	-3,81
Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen gem. § 202a, 202b, 202c StGB	455	471	14,61	14,65	+0,04
Softwarepiraterie (private Anwendung z.B. Computerspiele)	33	26	94,29	83,87	-10,42
Softwarepiraterie in Form gewerbsmäßigen Handelns	19	18	90,48	90,00	-0,48
Computerkriminalität insgesamt	**4 393**	**7 297**	**26,39**	**32,13**	**+5,74**

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
2016	23	0,4	263	4,5	557	9,6	4947	85,4	5790

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
2016	843	14,6	1 919	33,1	1439	24,9	923	15,9	483	8,3	183	3,2	5 790

Tabelle 05
Tatmittel Internet

	erfasste Fälle	darunter Tatmittel Internet	
Straftaten	2016	Fälle	Anteil in %
Insgesamt	1 469 426	57 241	3,9
gegen die sexuelle Selbstbestimmung	10 376	1 434	13,2
> Verbreitung pornografischer Erzeugnisse	1 660	1 187	71,5
- Besitz/Verschaffen von Kinderpornografie	neue PKS		
- Verbreitung von Kinderpornografie	neue PKS		
Betrug	226 719	40 905	18,0
> Waren- und Warenkreditbetrug	75 150	28 155	37,5
> Sonstiger Computerbetrug	3 780	2 718	71,9
> Betrügerisches Erlangen von Kfz § 263a StGB	26	2	7,7
> Weitere Arten des Warenkreditbetruges § 263a StGB	4062	2546	62,7
> Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten § 263a StGB	1894	1387	73,2
> Computerbetrug mittels rechtswidrig erlangter sonstiger unbarer Zahlungsmittel § 263a StGB	432	215	49,8
> Leistungskreditbetrug § 263a StGB	1046	644	61,6
> Überweisungsbetrug § 263a StGB	575	42	7,3
> Missbräuchliche Nutzung von Telekommunikationsdiensten	154	70	45,5
Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung	1 879	1 393	74,1
Datenveränderung, Computersabotage	1 764	1 472	83,4
Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen	3 215	2 360	73,4
Erpressung	1 854	557	30,0
Überweisungsbetrug § 263a StGB	575	42	7,3

Herausgeber

Landeskriminalamt Nordrhein-Westfalen
Völklinger Straße 49
40221 Düsseldorf

Abteilung 4
Cybercrime-Kompetenzzentrum
Dezernat 41

Redaktion EKHK Andreas Bruns
Telefon +49 211 939-4100
Fax +49 211 939-194100
CNPol 07-224-4100

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