POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

bürgerorientiert · professionell · rechtsstaatlich

Cybercrime

Lagebild NRW 2018

Kriminalitätsentwicklung im Überblick

Cybercrime

- Rückgang der Fallzahlen für den Bereich der Computerkriminalität (Cybercrime im engeren Sinne)
- Rückgang der Fallzahlen bei Straftaten mit Tatmittel Internet (Cybercrime im weiteren Sinne)
- Deutlicher Anstieg der Fallzahlen für den Deliktsbereich Erpressungen mit Tatmittel Internet

	2017	2018	Veränderung in %
Computerkriminalität (Cybercrime im engeren Sinne)	**22 913**	**19 693**	**- 14,1**
Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei der Datenverarbeitung	2 153	1 783	- 17,2
Datenveränderung/Computersabotage	1 408	909	- 35,4
Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen	2 893	2 528	- 12,6
Computerbetrug	16 321	14 421	- 11,6
Anzahl der aufgeklärten Fälle Cybercrime im engeren Sinne	8 210	6 994	- 0,3
Straftaten mit Tatmittel Internet (Cybercrime im weiteren Sinne)	**60 064**	**55 719**	**- 7,2**
Betrug mit Tatmittel Internet	43 817	40 208	- 8,2
Erpressung mit Tatmittel Internet	389	1 041	+ 167,6
Anzahl der aufgeklärten Fälle Cybercrime im weiteren Sinne	37 042	34 992	- 5,5

Inhaltsverzeichnis

1 Vorbemerkung

Zur Cybercrime gerechnet werden Straftaten, die sich gegen das Internet, andere Datennetze und informationstechnische Systeme oder deren Daten richten oder die mittels dieser Informationstechnik begangen werden. Die Definition steht im Einklang mit internationalen Begriffsbestimmungen wie der Convention on Cybercrime des Europarats[1].

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

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

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

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

> Datenhehlerei gemäß § 202d StGB

> Verletzung des Urheberrechtsgesetzes durch Softwarepiraterie[2] §§ 106 ff. UrhG (privates Handeln und gewerbsmäßiges Handeln)

> Computerbetrug gemäß § 263a StGB:

- Computerbetrug mittels rechtswidrig erlangter Zahlungskarten mit PIN
- Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten
- weitere Arten des Warenkreditbetruges.

Cybercrime im weiteren Sinne bezeichnet Straftaten, bei denen die Informations- und Kommunikationstechnik zur Planung, Vorbereitung oder Ausführung eingesetzt wird.

Die in Tabellen und Abbildungen aufgeführten Daten wurden in der Polizeilichen Kriminalstatistik (PKS) erfasst. Klammerwerte bei Zahlenangaben beziehen sich, soweit nicht anders angegeben, auf das Vorjahr.

In einzelnen Phänomenbereichen ist von einem großen Dunkelfeld auszugehen, da der Polizei viele Straftaten nicht bekannt bzw. nicht zur Anzeige gebracht werden.

Der Kriminalpolizeiliche Sondermeldedienst Cybercrime ermöglicht eine differenziertere Auswertung zu einzelnen Delikten. Um neue Tatbegehungsformen der Cybercrime zeitnah zu erkennen, bietet der Sondermeldedienst 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 (z. B. Kryptografie[3] oder Steganografie[4]) nutzen

> eine bundesweite oder internationale Bedeutung bestehen könnte

> ein überdurchschnittlich hoher Schaden vorliegt

> ein neuer oder abweichender Modus Operandi festgestellt wird.

[1] Übereinkommen des Europarats über Computerkriminalität vom 23. November 2001 in Budapest
[2] Die rechtswidrige Vervielfältigung und Verbreitung urheberrechtlich geschützter Software.
[3] Verschlüsselung von Daten
[4] Verborgene Speicherung oder Übermittlung von Informationen in einem Trägermedium (Container, z. B. in Fotos).

2 Lagedarstellung Cybercrime im engeren Sinne

2.1 Verfahrensdaten

2.1.1 Fallzahlen

2018 wurden 19 693 Cybercrime-Fälle erfasst. Dies entspricht einem Rückgang von 14,1 Prozent gegenüber dem Vorjahr (22 913). Die Anzahl der ermittelten Tatverdächtigen verringerte sich um 9 Prozent auf 5 068 (5 565). Die am häufigsten vertretenen Delikte waren der Computerbetrug gemäß § 263a StGB, das Ausspähen von Daten gemäß § 202a StGB und die Fälschung beweiserheblicher Daten gemäß § 269 StGB.

Tabelle 1
Entwicklung der Fallzahlen und Aufklärungsquoten der Cybercrime im engeren Sinne

Jahr	Erfasste Fälle	Zu-/Abnahme	aufgeklärte Fälle	Aufklärungsquote
2018	19 693	- 14,1 %	6 994	35,5 %
2017	22 913	+ 0,9 %	8 210	35,8 %
2016	22 708	+ 36,4 %	7 297	32,1 %
2015	16 645	- 19,6 %	4 393	26,4 %
2014	20 715	- 23,3 %	4 302	20,8 %
2013	27 016	+ 21,5 %	4 518	16,7 %
2012	22 228	+ 10,9 %	4 704	21,2 %
2011	20 036	+ 1,3 %	4 877	24,3 %
2010	19 775	+ 27,2 %	5 710	28,9 %
2009	15 541	+ 14,2 %	4 989	32,1 %

Tabelle 2
Fallzahlen in einzelnen Deliktsfeldern der Cybercrime im engeren Sinne

Delikt	2017	2018	Zu-/Abnahme	Prozent
Computerkriminalität (Cybercrime im engeren Sinne)	**22 913**	**19 693**	**-3 220**	**- 14,1 %**
Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei der Datenverarbeitung §§ 269, 270 StGB	2 153	1 783	- 370	-17,19
Datenveränderung, Computersabotage §§ 303a, 303bStGB	1 408	909	- 499	- 35,4 %
Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen und Datenhehlerei §§ 202a, 202b, 202c, 202d StGB	2 893	2 528	- 365	- 12,6 %
Softwarepiraterie (private Anwendung z. B. Computerspiele) § 106 ff. UrhG	20	27	7	+ 35,0 %
Softwarepiraterie in Form gewerbsmäßigen Handelns § 108a UrhG	118	25	- 93	- 78,8 %
Computerbetrug insgesamt § 263a StGB	16 321	14 421	- 1 900	- 11,6 %
Betrügerisches Erlangen von Kfz § 263a StGB	5	2	- 3	- 60,0 %
Weitere Arten des Warenkreditbetruges § 263a StGB	6 169	5 745	- 424	- 6,9 %
Computerbetrug mittels rechtswidrig erlangter Zahlungskarten mit PIN § 263a StGB	2 771	2 937	+ 166	+ 6,0 %
Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten § 263a StGB	1 806	1 530	- 276	- 15,3 %
Computerbetrug mittels rechtswidrig erlangter sonstiger unbarer Zahlungsmittel § 263a StGB	504	565	+ 61	+ 12,1 %
Leistungskreditbetrug § 263a StGB	1 274	1 049	- 225	- 17,7 %
Computerbetrug (sonstiger) § 263a StGB	3 552	2 368	- 1 184	- 33,3 %
Missbräuchliche Nutzung von Telekommunikationsdiensten § 263a StGB	67	68	+ 1	+ 1,5 %
Abrechnungsbetrug im Gesundheitswesen § 263a StGB	0	9	+ 9	
Überweisungsbetrug § 263a StGB	173	148	- 25	- 14,5 %

2.1.2 Aufklärungsquote

Von den im Jahr 2018 erfassten Straftaten wurden 6 994 aufgeklärt. Die Aufklärungsquote betrug 35,5 Prozent und verringerte sich gegenüber 2017 um 0,3 Prozentpunkte. Im Bereich des Computerbetrugs wurden 5 511 Fälle aufgeklärt. Dies entspricht einer Aufklärungsquote von 38,2 Prozent (41,2 Prozent).

Abbildung 1
Vergleich Fallzahlen und Aufklärungsquote

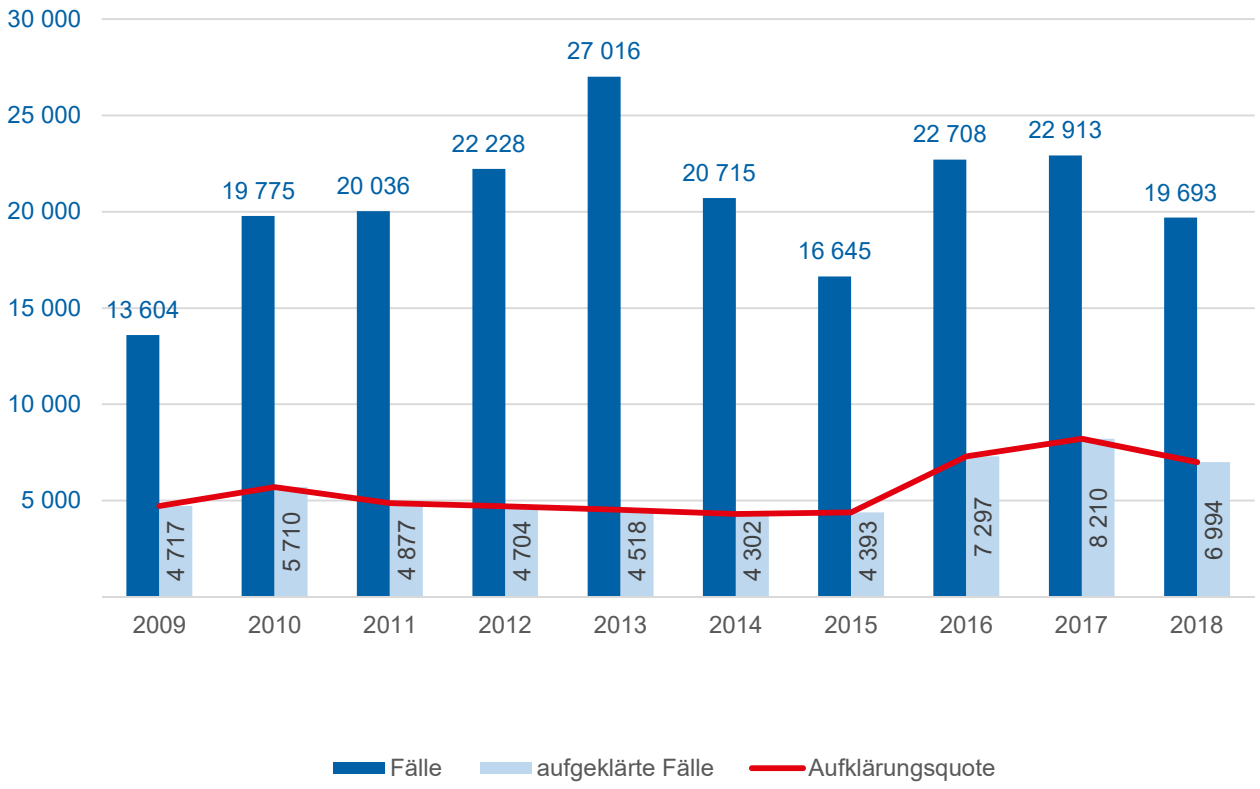


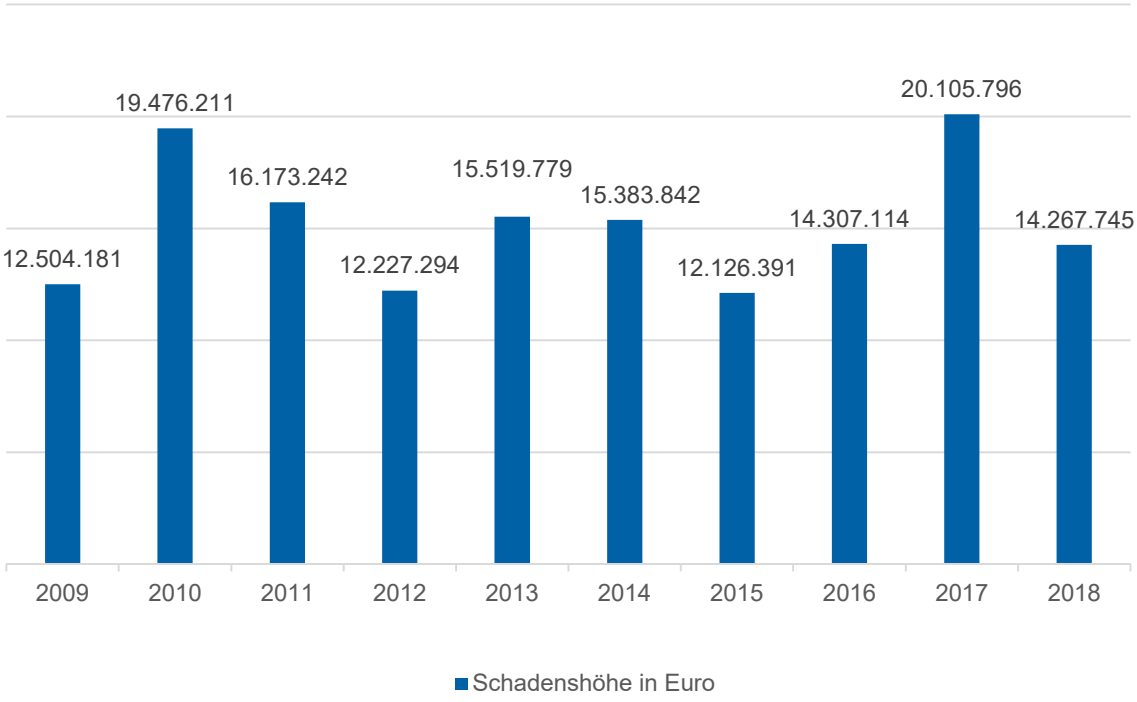
Tabelle 3
Aufklärungsquote

Delikt	Aufgeklärte Fälle		Aufklärungsquote		Zu-/Abnahme
	2017	2018	2017	2018	%-Punkte
Computerkriminalität (Cybercrime im engeren Sinne)	**8 210**	**6 994**	**35,8 %**	**35,5 %**	**- 0,3**
Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei der Datenverarbeitung §§ 269, 270 StGB	740	649	34,4 %	36,4 %	+ 2,0
Datenveränderung, Computersabotage §§ 303a, 303b StGB	241	185	17,1 %	20,4 %	+ 3,3
Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen und Datenhehlerei §§ 202a, 202b, 202c, 202d StGB	445	618	15,4 %	24,3 %	+ 8,9
Softwarepiraterie (private Anwendung z.B. Computerspiele) § 106 ff. UrhG	18	26	90 %	96,3%	+ 6,3
Softwarepiraterie in Form gewerbsmäßigen Handelns § 108a UrhG	45	10	38,1 %	40,0 %	+ 1,9
Computerbetrug insgesamt § 263a StGB	6 721	5 511	41,2 %	38,2 %	- 3,0
Betrügerisches Erlangen von Kfz § 263a StGB	3	1	60,0 %	50,0 %	- 10,0
Weitere Arten des Warenkreditbetruges § 263a StGB	3 679	2 703	59,6 %	47,1 %	- 12,5
Computerbetrug mittels rechtswidrig erlangter Zahlungskarten mit PIN § 263a StGB	921	953	33,2 %	32,5 %	- 0,7
Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten § 263a StGB	558	372	30,9 %	24,3 %	- 6,6
Computerbetrug mittels rechtswidrig erlangter sonstiger unbarer Zahlungsmittel § 263a StGB	142	274	28,2 %	48,5 %	+ 20,3
Leistungskreditbetrug § 263a StGB	332	385	26,1 %	36,7 %	+ 10,6
Computerbetrug (sonstiger) § 263a StGB	1 000	723	28,2 %	30,5 %	+ 2,3
Missbräuchliche Nutzung von Telekommunikationsdiensten § 263a StGB	9	37	13,4 %	54,4 %	+ 41,0
Abrechnungsbetrug im Gesundheitswesen § 263a StGB	0	9		100,0 %	
Überweisungsbetrug § 263a StGB	77	54	44,5 %	36,5 %	- 8,0

2.1.3 Schadensentwicklung

Schäden von Cybercrime werden in der PKS ausschließlich für Computerbetrug und für Softwarepiraterie abgebildet. Im Jahr 2018 verringerte sich der Gesamtschaden um 5 838 051 Euro auf 14 267 745 Euro. Dies entspricht einem Rückgang um 29 Prozent. Der Schaden beim Computerbetrug beträgt 13 457 859 Euro (17 070 328 Euro).

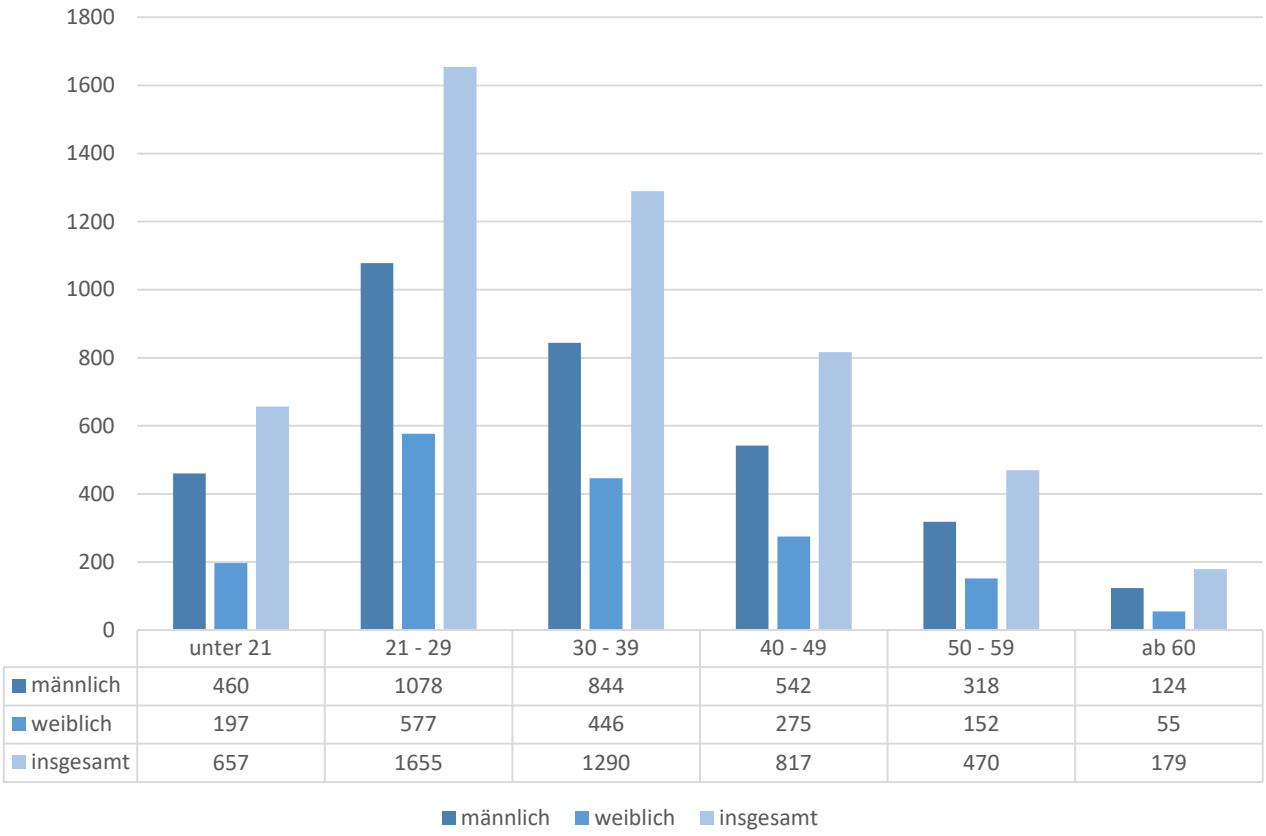
Abbildung 2
Schadensentwicklung



2.1.4 Tatverdächtige

Im Jahr 2018 wurden 5 068 (5 565) Tatverdächtige ermittelt. Den größten Anteil nahm mit 1 655 ermittelten Tatverdächtigen die Gruppe der Erwachsenen im Alter von 21 bis 29 Jahren ein. Der Anteil der männlichen Tatverdächtigen (1 078) betrug 65,1 Prozent.

Abbildung 3
Tatverdächtige



	unter 21	21 - 29	30 - 39	40 - 49	50 - 59	ab 60
männlich	460	1078	844	542	318	124
weiblich	197	577	446	275	152	55
insgesamt	657	1655	1290	817	470	179

2.2 Einzelne Deliktsfelder

Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei der Datenverarbeitung

Bei diesen Delikten wurden häufig E-Mails verschickt, die täuschend echt den real existierenden Banken, Zahlungsdienstleistern oder Online-Shops nachempfunden waren. Die ahnungslosen Opfer „klickten“ gutgläubig auf den darin enthaltenen Link und gelangten so auf fingierte Webseiten. Dort gaben sie ihre Zugangsdaten ein, die so in den Besitz der Täter gelangten.

Die Fallzahlen sind im Jahr 2018 (1 783) im Vergleich zum Vorjahr (2 153) um 17,2 Prozent gesunken. Die Aufklärungsquote im Jahr 2018 betrug 36,4 Prozent (34,4 Prozent). Im fünfjährigen Vergleichszeitraum sind die Fallzahlen um 32,1 Prozent gesunken. Die Aufklärungsquote ist im gleichen Zeitraum um 9,2 Prozentpunkte gestiegen.

Datenveränderung, Computersabotage

Die Delikte Datenveränderung und Computersabotage sind oftmals miteinander gekoppelt. So werden beispielsweise beim Phänomen Ransomware durch Täter Schadprogramme per E-Mail-Anhang in das anzugreifende System eingeschleust. Öffnet der Nutzer diesen Anhang, erfolgt eine Verschlüsselung der Daten auf dem System, so dass ein Zugriff durch den Nutzer nicht mehr möglich ist. Zur Freigabe dieser Daten wird ein Lösegeld erpresst.

Die Fallzahlen sind im Jahr 2018 (909) im Vergleich zum Vorjahr (1 408) um 35,4 Prozent gesunken. Die Aufklärungsquote im Jahr 2018 betrug 20,4 Prozent (17,1 Prozent). Im fünfjährigen Vergleichszeitraum sind die Fallzahlen um 68,5 Prozent gesunken. Die Aufklärungsquote ist im gleichen Zeitraum um 5,3 Prozentpunkte gestiegen.

Ausspähen, Abfangen von Daten einschließlich Vorbereitungshandlungen und Datenhehlerei

Eine Vielzahl von Personen macht keinen Unterschied zwischen ihrer analogen und ihrer digitalen Identität. Die tatsächlichen Identitätsattribute, wie Name, Vorname und Geburtsdatum, aber auch die Wohnanschrift, werden durch die Nutzer im digitalen Raum beispielsweise für Einkäufe in Onlineshops oder Vertragsabschlüsse im Versicherungssektor preisgegeben. Auch wenn diese Daten oftmals verschlüsselt übertragen werden, gelingt es den Tätern diese abzufangen und für anschließende Verwertungstaten zu nutzen. Auch das Sammeln von personenbezogenen Daten und die anschließende Veröffentlichung einer Vielzahl unterschiedlicher Datensätze (Doxing[5]) spielt in diesen Deliktsbereichen eine Rolle. Ein herausragender Fall des Doxings wurde im Januar 2019 bekannt, bei dem ein Einzeltäter eine Vielzahl von Datensätzen zu Personen des öffentlichen Lebens veröffentlichte. Für das Jahr 2018 ist kein Fall bekannt, der eine ähnliche öffentliche Aufmerksamkeit erreichte.

Die Fallzahlen sind im Jahr 2018 (2 528) im Vergleich zum Vorjahr (2 893) um 12,6 Prozent gesunken. Die Aufklärungsquote im Jahr 2018 betrug 24,3 Prozent (15,4 Prozent). Im fünfjährigen Vergleichszeitraum sind die Fallzahlen um 42,3 Prozent gesunken. Die Aufklärungsquote ist im gleichen Zeitraum um 9,6 Prozentpunkte gestiegen.

Computerbetrug mittels rechtswidrig erlangter Zahlungskarten mit PIN

Die Fallzahlen sind im Jahr 2018 (2 937) im Vergleich zum Vorjahr (2 771) um 6 Prozent gestiegen. Die Aufklärungsquote im Jahr 2018 betrug 32,5 Prozent (33,2 Prozent).

Im fünfjährigen Vergleichszeitraum sind die Fallzahlen um 23,5 Prozent gesunken. Die Aufklärungsquote ist im gleichen Zeitraum um 0,9 Prozentpunkte gestiegen. Grund für den Rückgang der Fallzahlen dürfte sein, dass der Umgang mit Zahlungskarten und die Aufbewahrung der dazugehörigen PIN zunehmend verantwortungsbewusster erfolgt.

[5] Das internetbasierte Zusammentragen und Veröffentlichen von personenbezogener Daten

Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten

Zahlungskartendaten, die durch Phishing oder Skimming rechtswidrig erlangt wurden, wurden zum Teil im Internet eingesetzt, um Waren zu erlangen. Auch wurden die Daten dazu genutzt um Karten aus Rohlingen herzustellen und so an Geldautomaten im außereuropäischen Ausland Geldverfügungen zu tätigen. Die Geschädigten erfuhren erst zeitversetzt bei Belastung ihrer Konten von dem Abfangen und dem Missbrauch ihrer Daten.

Die Fallzahlen sind im Jahr 2018 (1 530) im Vergleich zum Vorjahr (1 806) um 15,3 Prozent gesunken. Die Aufklärungsquote im Jahr 2018 betrug 24,3 Prozent (30,9 Prozent).

Computerbetrug mittels rechtswidrig erlangter sonstiger unbarer Zahlungsmittel

Unbare Zahlungsmittel sind u. a. Guthabenkarten, Schecks oder Bonuskarten. Zudem erfolgen Zahlungen zunehmend über PayPal-Konten. In den meisten Fällen wurden Waren im Online-Handel bestellt und über ein zuvor gehacktes oder ausgespähtes PayPal-Konto bezahlt.

Die Fallzahlen sind im Jahr 2018 (565) im Vergleich zum Vorjahr (504) um 12,1 Prozent gestiegen. Die Aufklärungsquote im Jahr 2018 betrug 48,5 Prozent (28,2 Prozent).

Leistungskreditbetrug

Beim Leistungskreditbetrug erbringt der Verkäufer eine Leistung im Voraus. Der Täter bestellt diese Leistung über das Internet, beauftragt er z. B. das Erstellen einer Webseite. Mit dem Täter wird eine spätere Zahlung vereinbart. Der Täter hat jedoch von Anfang an nicht die Absicht zu zahlen. Oft werden frei erfundene Personalien oder die existierender Personen missbräuchlich genutzt.

Die Fallzahlen sind im Jahr 2018 (1 049) im Vergleich zum Vorjahr (1 274) um 17,7 Prozent gesunken. Die Aufklärungsquote im Jahr 2018 betrug 36,7 Prozent (26,1 Prozent).

Missbräuchliche Nutzung von Telekommunikationsdiensten

Bei diesem Delikt steht die Manipulation von Telekommunikationsanlagen im Vordergrund. Durch die Ausnutzung von Sicherheitslücken oder unzureichenden Zugangssicherungen können Täter auf Router von Firmen oder Privatleuten zugreifen und so teure Verbindungen in das Ausland oder zu Mehrwertdiensten herstellen.

Die Fallzahlen sind im Jahr 2018 (68) im Vergleich zum Vorjahr (67) um einen Fall angestiegen. Die Aufklärungsquote im Jahr 2018 betrug 54,4 Prozent (13,4 Prozent). Im fünfjährigen Vergleichszeitraum sind die Fallzahlen um 77,5 Prozent gesunken. Die Aufklärungsquote ist im gleichen Zeitraum um 25,4 Prozentpunkte angestiegen. Die Schadenssumme reduzierte sich zum Vorjahr (278 246 Euro) auf 195 791 Euro.

Überweisungsbetrug

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 dies automatisiert, erfüllt dies den Tatbestand des § 263a StGB.

Die Fallzahlen sind im Jahr 2018 (148) im Vergleich zum Vorjahr (173) um 14,5 Prozent gesunken. Die Aufklärungsquote im Jahr 2018 betrug 36,5 Prozent (44,5 Prozent). Der Trend aus dem Vorjahr setzt sich somit für das Berichtsjahr 2018 fort.

3 Lagedarstellung Cybercrime im weiteren Sinne

3.1 Verfahrensdaten

Straftaten, bei denen das Internet als Tatmittel verwendet wird, werden in der PKS 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 werden (so genannte Äußerungs- bzw. Verbreitungsdelikte), als auch solche, bei denen das Internet zur Tatbestandsverwirklichung genutzt wird.

Der Unterschied zwischen Cybercrime im engeren und im weiteren Sinne wird beim Betrug deutlich: Erfolgt die Täuschungshandlung gegenüber einem datenverarbeitenden System, handelt es sich um einen Computerbetrug gemäß § 263a StGB und somit Cybercrime im engeren Sinne. Erfolgt die Täuschung unter Nutzung eins Computers gegenüber einem Menschen, liegt ein Betrug gemäß § 263 StGB vor und es handelt sich um Cybercrime im weiteren Sinne. Soweit das Internet im Hinblick auf die Tatverwirklichung nur eine untergeordnete Rolle hat, wird die Sonderkennung „Tatmittel Internet“ nicht verwendet. Dies ist beispielsweise der Fall, wenn Kontakte zwischen Täter und Opfer mittels Internet ausschließlich im Vorfeld der eigentlichen Tat stattfanden. 2018 wurden 55 719 Fälle mit dem Tatmittel Internet erfasst, 4 345 weniger als 2017. Den größten Anteil nahmen hierbei Betrugsdelikte mit 72 Prozent ein. Bei einer Aufklärungsquote von 62,8 Prozent wurden 34 992 Fälle aufgeklärt.

Abbildung 4
Tatmittel Internet - Fallzahlen und Aufklärungsquote

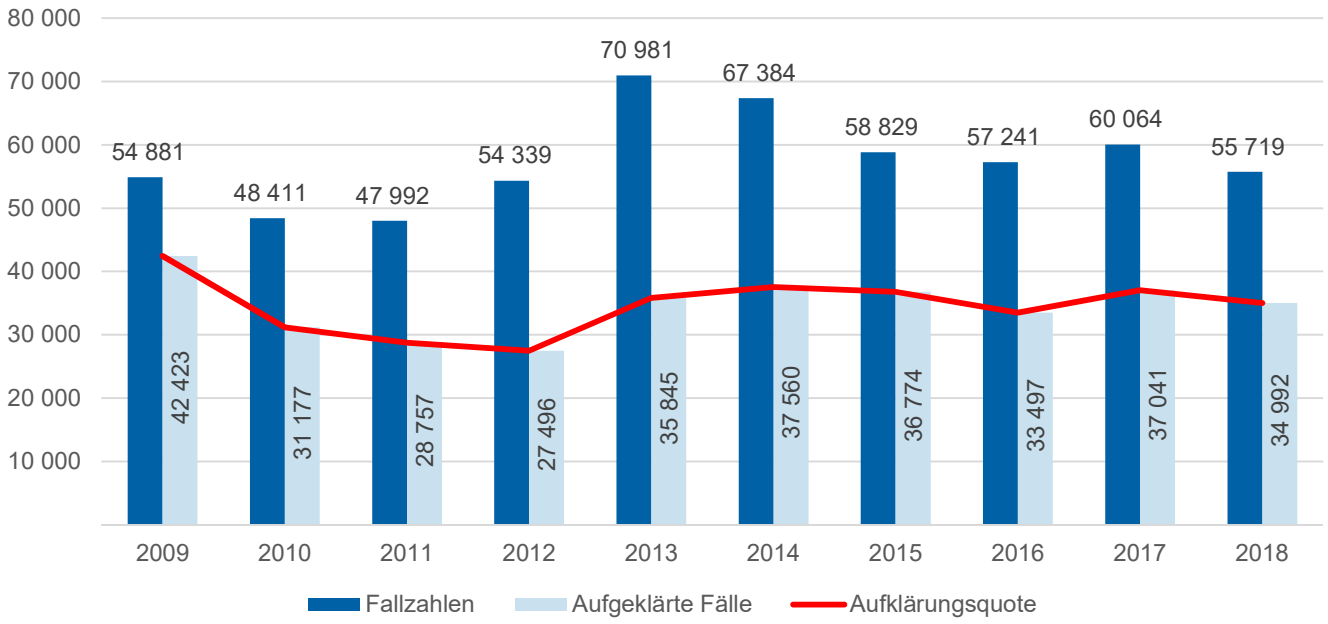


Tabelle 4
Tatmittel Internet

	Gesamt-kriminalität	darunter Tatmittel Internet	
Straftaten	**2018**	**Fälle**	**Anteil in %**
Alle Straftaten	**1 282 441**	**55 719**	**4,3**
Straftaten gegen die sexuelle Selbstbestimmung	14 076	1 857	13,2
Verbreitung pornografischer Schriften §§ 184, 184a, 184b, 184c, 184d, 184e StGB	2 164	1 501	69,4
Besitz/Verschaffen von Kinderpornografie § 184b StGB	1 412	1 064	75,4
Verbreitung von Kinderpornografie § 184b Abs. 1 Nr. 1	718	561	78,1
Betrug § 263 StGB	193 097	41 545	21,5
Waren- und Warenkreditbetrug § 263 StGB	69 204	30 535	44,1
Sonstiger Computerbetrug § 263a StGB	2 368	1 486	62,8
Betrügerisches Erlangen von Kfz § 263a StGB	2	0	
Weitere Arten des Warenkreditbetruges § 263a StGB	5 745	4 573	79,6
Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten § 263a StGB	1 530	933	61,0
Computerbetrug mittels rechtswidrig erlangter sonstiger unbarer Zahlungsmittel § 263a StGB	565	336	59,5
Leistungskreditbetrug § 263a StGB	1 049	773	73,7
Überweisungsbetrug § 263a StGB	148	37	25,0
Missbräuchliche Nutzung von Telekommunikations-diensten §263a StGB	68	39	57,4
Fälschung beweiserheblicher Daten, Täuschung im Rechts-verkehr bei Datenverarbeitung §§ 269, 270 StGB	1 783	1 194	67,0
Datenveränderung, Computersabotage §§ 303a, 303b StGB	909	708	77,9
Ausspähen, Abfangen von Daten einschl. Vorbereitungs-handlungen und Datenhehlerei §§ 202a, 202b, 202c, 202d StGB	2 528	1 739	68,8
Erpressung § 253 StGB	2 188	1 041	47,6

3.2 Einzelne Deliktsfelder

Kinderpornografie

2018 wurden für den Deliktsbereich „Verbreitung, Erwerb und Besitz kinderpornographischer Schriften“ gemäß § 184b StGB 1 412 (1 250) Fälle erfasst. Dies entspricht einer Zunahme von 13 Prozent. In diesem Deliktsbereich besitzt das Internet eine herausragende Rolle. Bei 1 064 Fällen (75,4 Prozent) war das Internet Tatmittel. Hiervon konnten 980 Taten (92 Prozent) aufgeklärt werden. Aus dem auch 2018 weiterhin hohen Hinweisaufkommen durch die teilstaatliche US-amerikanische Organisation „National Center for Missing and Exploited Children“ (NCMEC) wurden dem LKA NRW, nach Prüfung der strafrechtlichen Relevanz und erfolgversprechender Ermittlungsansätze durch das BKA, über 1 500 Verdachtsfälle bekannt und nordrhein-westfälischen Polizeibehörden zu weiteren Ermittlungen zugeleitet.

Einen weiteren Schwerpunkt bilden Umfangsverfahren mit einer Vielzahl von Einzeltaten. 2018 wurden dem LKA NRW 79, auch in anderen Ländern geführte, Umfangsverfahren bekannt, die sich u. a. gegen 1 114 Tatverdächtige aus NRW richteten.

Im Phänomenbereich Kinderpornographie nehmen die Fälle von „Cyber-Grooming“ ebenfalls stetig zu.

Das Phänomen „Cyber-Grooming“ bezeichnet die Kontaktaufnahme überwiegend erwachsener Männer mit Kindern oder Jugendlichen über das Internet mit dem Ziel, sexuelle Kontakte anzubahnen. Oftmals überreden sie Minderjährige, ihnen freizügige Selbstporträts o. ä. zuzusenden. Diese werden dann als Druckmittel eingesetzt, um die Minderjährigen dann zu weiteren sexuellen Handlungen zu nötigen.

In diesem Kontext wird darauf hingewiesen, dass die Universitäten Hohenheim und Münster[6] im Oktober 2017 im Rahmen einer Studie 1 048 Kinder und Jugendliche zum Erstkontakt mit Pornographie befragt. Der Erstkontakt mit Pornographie fand im Durchschnitt im Alter von 12,7 Jahren und zu 70 Prozent online statt. Mehrheitlich erfolgte der Erstkontakt zu Hause, zu rund 40 Prozent im Beisein von Freunden. Zu einer Aufarbeitung des Gesehenen z. B. mit Eltern oder Lehrern kam es regelmäßig nicht.

Digitale Erpressung - Pornomail

Den hochsensiblen privaten Bereich und das Schamgefühl der Betroffenen machen sich Täter oder Tätergruppierungen zu Nutze, um Geld bei Geschädigten zu erpressen. Hierbei wird täterseits eine Vielzahl an Mails an einen unbestimmten Empfängerkreis versandt. In diesen E-Mails suggerien die Täter dem Empfänger, dass man in das IT-System des Betroffenen ein Schadprogramm eingebracht habe, welches Zugriff auf die Web-Kamera habe. Dadurch hätte der Täter Videoaufnahmen von den Betroffenen machen können, die diese beim Besuch von Internetseiten mit pornographischen Inhalten zeige. Zusätzlich seien die Betroffenen beim Masturbieren gefilmt worden. Um der Forderung Nachdruck zu verleihen, liefern die Täter Passwörter und Benutzernamen der Betroffenen mit. Tatsächlich stammen diese Daten in der Regel aus dem so genannten „Darknet“, wo die Täter diese aus zurückliegenden Hackingattacken aufgekauft haben. Die Täter drohen mit der Veröffentlichung des kompromittierten Videomaterials an die Kontakte der Betroffenen. Dies könne nur mit der Zahlung eines „Lösegeldes“ in virtueller Währung, auf ein Wallet[7], verhindert werden.

Die PKS bildet dieses Phänomen nicht spezifisch ab.

Bislang ist in NRW kein Fall bekannt, in welchem tatsächlich eine Videoaufzeichnung angefertigt wurde oder das IT-System der Betroffenen kompromittiert wurde. Dennoch konnten auf Wallets Zahlungseingänge festgestellt werden.

[6] https://www.uni-hohenheim.de/pressemitteilung?tx_ttnews%5Btt_news%5D=37983&cHash=91bc3a6dc5c6b9304555ab08df7da545
[7] Bei einem Wallet handelt es sich um ein Programm, welches dem Nutzer die Möglichkeit bietet, Kryptowährungen aufzubewahren und zu verwalten.

Digitale Epressung - Sextortion

Beim Phänomen Sextortion besitzt der Täter tatsächlich Videoaufnahmen, die Betroffene bei sexuellen Handlungen zeigen. Auch hier versuchen die Täter durch Drohung der Veröffentlichung von Videomaterial Geld zu erpressen.In der „Anbahnungsphase“ chattet der Täter unter einer Legende zunächst in sozialen Netzwerken mit seinem späteren Opfer. Es präsentiert sich auf digitalen Plattformen (i. d. R. Facebook oder Onlinedatingplattformen) als attraktive Frau, macht seinem Opfer Komplimente und baut so eine Vertrauensbeziehung auf. Seitens des Täters erfolgt dann der Vorschlag, in einen Videochat zu wechseln. Das Opfer wird nach kurzer Zeit dazu aufgefordert, sich vor der Kamera zu entblößen oder an sich selbst sexuelle Handlungen vorzunehmen. Um die Hemmschwelle des Opfers zu senken, zeigt sich das Gegenüber ebenfalls nackt oder befriedigt sich selbst. Hierzu wird in der Regel ein Video eingespielt. Das Opfer handelt im Glauben einer tatsächlichen Chatbekanntschaft. Der Täter zeichnet den Videochat auf und erlangt dadurch kompromentierendes Bild- bzw. Videomaterial. Anschließend werden die Opfer zur Zahlung eines Geldbetrags auf ein ausländisches Konto oder auf ein Wallet aufgefordert. Sollte der Zahlungsaufforderung nicht nachgekommen werden, droht der Täter mit der Weitergabe des aufgenommenen Bild- und Videomaterials an den virtuellen Freundeskreis der Opfer in sozialen Netzwerken.

4 Prävention

Die Prävention von Cybercrime obliegt den Kreispolizeibehörden (KPB). Das LKA NRW unterstützt die KPB insbesondere durch Fortschreiben von Standards und Entwickeln von Medien sowie Initiieren und Koordinieren von überregionalen Präventionsmaßnahmen.

Während die Prävention von Cybercrime im weiteren Sinne (Tatmittel Internet) vollständig durch die KPB erfolgt, deckt das LKA NRW mit dem Cybercrime-Kompetenzzentrum den Bereich der Cybercrime Prävention im engeren Sinne ab. Hauptzielgruppe sind hierbei Wirtschaftsunternehmen, Behörden und vergleichbare Institutionen.

Im Bereich Cybercrime im engeren Sinne werden bewährte Netzwerke mit unterschiedlichen Kooperationspartnern wie dem Bitkom[8], dem VOICE[9] und der Sicherheitspartnerschaft mit dem ASW NRW[10] gestärkt und ausgebaut. Seit 2017 besteht eine Kooperationsvereinbarung mit dem eco e.V.[11] und dem networker NRW e.V.[12] Mit VOICE veranstaltete das LKA NRW einen gemeinsamen IT-Sicherheitstag, ebenso wurde mit dem Bitkom und weiteren Landeskriminalämtern eine Fachtagung in NRW zur „Sicherheitskooperation Cybercrime“ ausgerichtet. Durch die Kooperationen mit Bitkom und VOICE werden Präventionsbotschaften einem großen Spektrum von Personen und Firmen zugänglich gemacht.

Durch die enge Zusammenarbeit erreicht das LKA NRW Multiplikatoren innerhalb der Wirtschaft und sensibilisiert für die Prävention von Cybercrime. Hierbei werden Formate wie Informationsstände, Vorträge, Teilnahme an Kongressen und Messen genutzt. Die Beteiligung an „Round Tables“ und die Zusammenarbeit in Regionalgruppen reduzieren Berührungsängste zwischen Wirtschaft und Polizei, so dass die Anzeigebereitschaft und das Bewusstsein für die durch Cybercrime bestehenden Gefahren gesteigert werden.

Die Informations- und Wissensvermittlung umfasst neben den Möglichkeiten zum Schutz vor Angriffen, auch die Sensibilisierung zur Notwendigkeit der Vorbereitung auf den „Ernstfall“. Potentiell Betroffene, die Planentscheidungen treffen und Notfallplane erstellen, können Angriffe deutlich besser eindämmen, so dass nur geringere finanzielle Schäden entstehen oder diese ganz vermieden werden können.

Die Prävention von Cybercrime im weiteren Sinne ist auf eine Mehrzal von Deliktsbereichen ausgerichtet. Hier wird das LKA koordinierend tätig und setzt aktuelle Entwicklungen[13] in Empfehlungen und Standards um.

Das LKA NRW sensibilisierte im Jahr 2018 mit mehr als 70 Vorträgen bei verschiedenen Veranstaltungen von Behörden und in der Wirtschaft zu Gefahren durch Cybercrime.

Bei Großveranstaltungen wie der it-sa[14], dem Deutschen Präventionstag 2018, dem Tag der Medienkompetenz, dem NRW-Tag in Essen und der protekt[15] in Leipzig informierte das LKA NRW mit Vorträgen und Informationsständen, um eine breite Öffentlichkeit zu erreichen.

[8] Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.
[9] Bundesverband der IT-Anwender e.V.
[10] Allianz für Sicherheit in der Wirtschaft Nordrhein-Westfalen e.V.
[11] eco - Verband der Internetwirtschaft e.V.
[12] networker NRW - Das Netzwerk der IT-Kompetenz
[13] https://polizei.nrw/cybercrime-angriffe-aus-dem-netz
[14] Fachmesse mit begleitendem Kongress zum Thema Informationssicherheit
[15] Konferenz und Fachausstellung für den Schutz kritischer Infrastrukturen

Herausgeber

Landeskriminalamt Nordrhein-Westfalen
Völklinger Straße 49
40221 Düsseldorf

Abteilung 4
Cybercrime-Kompetenzzentrum
Dezernat 41

Redaktion: KR Dennis Boß
Telefon: +49 211 939-4100
Fax: +49 211 939-1941000
CNPol: 07-224-4100

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

Bildnachweis: Titelseite – KOKin Marita Segin