POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

bürgerorientiert · professionell · rechtsstaatlich

Cybercrime

Lagebild NRW 2019

Kriminalitätsentwicklung im Überblick

Cybercrime

- Anstieg der Fallzahlen für den Bereich der Computerkriminalität (Cybercrime im engeren Sinne)
- Anstieg der Fallzahlen bei Straftaten mit Tatmittel Internet (Cybercrime im weiteren Sinne)
- Deutlicher Anstieg der Fallzahlen für den Deliktsbereich Erpressungen mit Tatmittel Internet
- Deutlicher Anstieg der Fallzahlen bei Verbreitung, Erwerb und Besitz kinderpornografischer Schriften

	2018	2019	Veränderung in %
Computerkriminalität (Cybercrime im engeren Sinne)	**19 693**	**20 118**	**+ 2,2**
Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei der Datenverarbeitung	1 783	1 699	- 4,7
Datenveränderung/Computersabotage	909	969	+ 6,6
Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen	2 528	2 544	+ 0,6
Computerbetrug	14 421	14 886	+ 3,2
Softwarepiraterie (private Anwendung z.B. Computerspiele)	27	11	- 59,3
Softwarepiraterie in Form gewerbsmäßigen Handelns	25	9	- 64,0
Anzahl der aufgeklärten Fälle Cybercrime im engeren Sinne	6 994	5 911	- 15,5
Straftaten mit Tatmittel Internet (Cybercrime im weiteren Sinne)	**55 719**	**56 405**	**+ 1,2**
Betrug mit Tatmittel Internet	40 208	40 249	+ 0,1
Erpressung mit Tatmittel Internet	1 041	1 732	+ 66,4
Anzahl der aufgeklärten Fälle Cybercrime im weiteren Sinne	34 992	31 437	- 10,2
Verbreitung, Erwerb und Besitz kinderpornografischer Schriften	**1 412**	**2 359**	**+ 67,1**

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

2019 wurden 20 118 Cybercrime-Fälle erfasst. Dies entspricht einem Anstieg von 2,2 Prozent gegenüber dem Vorjahr (19 693). Die Anzahl der ermittelten Tatverdächtigen verringerte sich um 8,7 Prozent auf 4 628 (5 068). 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
2019	20 118	+ 2,2 %	5 911	29,4 %
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	2018	2019	Zu-/Abnahme	Prozent
Computerkriminalität (Cybercrime im engeren Sinne)	**19 693**	**20 118**	**+ 425**	**+ 2,2 %**
Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei der Datenverarbeitung §§ 269, 270 StGB	1 783	1 699	- 84	- 4,7 %
Datenveränderung, Computersabotage §§ 303a, 303b StGB	909	969	+ 60	+ 6,6 %
Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen und Datenhehlerei §§ 202a, 202b, 202c, 202d StGB	2 528	2 544	+ 16	+ 0,6 %
Softwarepiraterie (private Anwendung z. B. Computerspiele) § 106 ff. UrhG	27	11	- 16	- 59,3 %
Softwarepiraterie in Form gewerbsmäßigen Handelns § 108a UrhG	25	99	+ 74	+ 296,0 %
Computerbetrug insgesamt § 263a StGB	14 421	14 886	+ 465	+ 3,2 %
Betrügerisches Erlangen von Kfz § 263a StGB	2	11	+ 9	+ 450,0 %
Weitere Arten des Warenkreditbetruges § 263a StGB	5 745	5 748	+ 3	+ 0,1 %
Computerbetrug mittels rechtswidrig erlangter Zahlungskarten mit PIN § 263a StGB	2 937	2 749	- 188	- 6,4 %
Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten § 263a StGB	1 530	1 790	+ 260	+ 17,0 %
Computerbetrug mittels rechtswidrig erlangter sonstiger unbarer Zahlungsmittel § 263a StGB	565	510	- 55	- 9,7 %
Leistungskreditbetrug § 263a StGB	1 049	1 237	+ 188	+ 17,9 %
Computerbetrug (sonstiger) § 263a StGB	2 368	2 672	+ 304	+ 12,8 %
Missbräuchliche Nutzung von Telekommunikationsdiensten § 263a StGB	68	43	- 25	- 36,8 %
Abrechnungsbetrug im Gesundheitswesen § 263a StGB	9	1	- 8	- 88,9 %
Überweisungsbetrug § 263a StGB	148	125	- 23	- 15,5 %

2.1.2 Aufklärungsquote

Von den im Jahr 2019 erfassten Straftaten wurden 5 911 aufgeklärt. Die Aufklärungsquote betrug 29,4 Prozent und verringerte sich gegenüber 2018 um 6,1 Prozentpunkte. Im Bereich des Computerbetrugs wurden 4 621 Fälle aufgeklärt. Dies entspricht einer Aufklärungsquote von 31,0 Prozent (38,2 Prozent).

Abbildung 1
Vergleich Fallzahlen und Aufklärungsquote

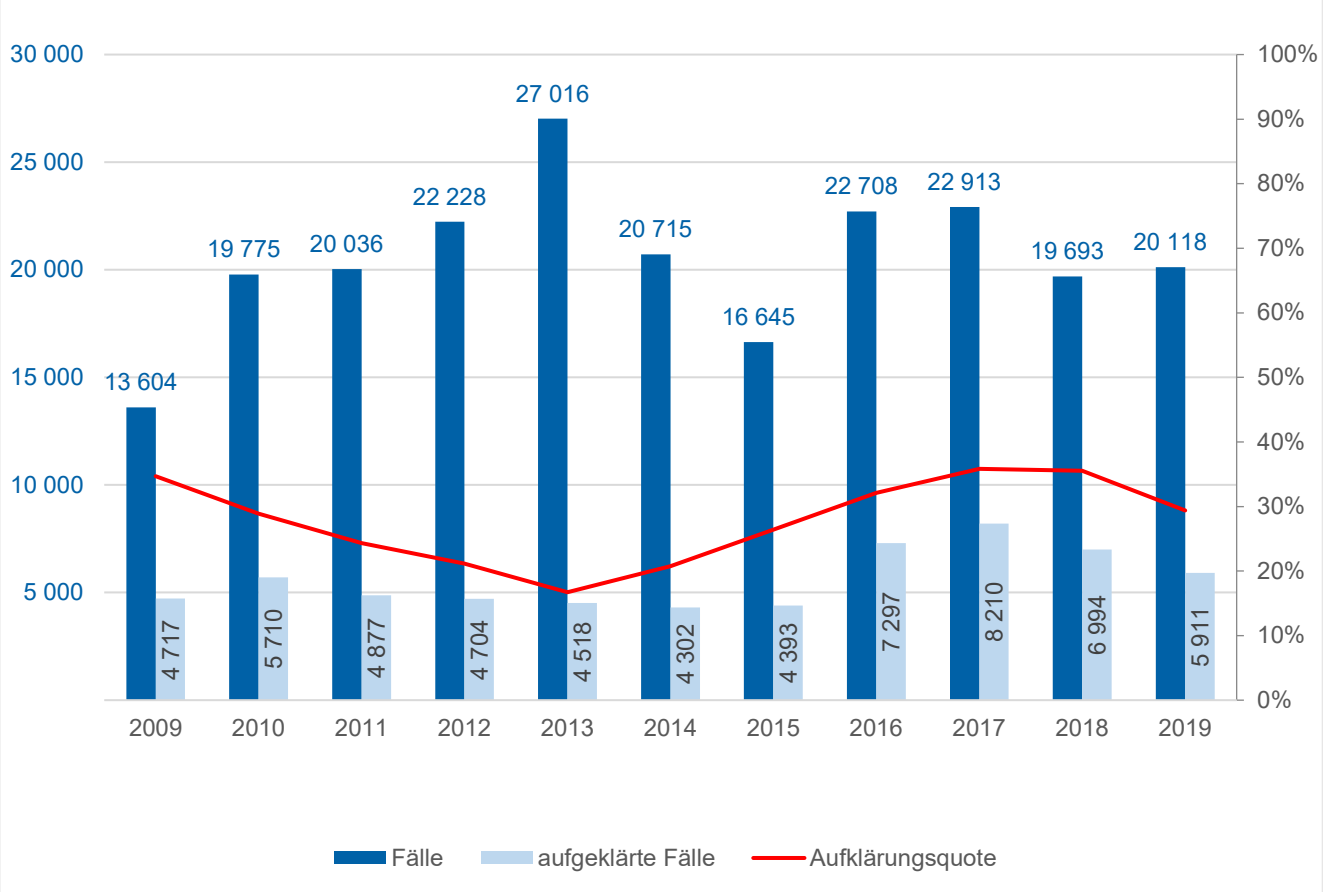


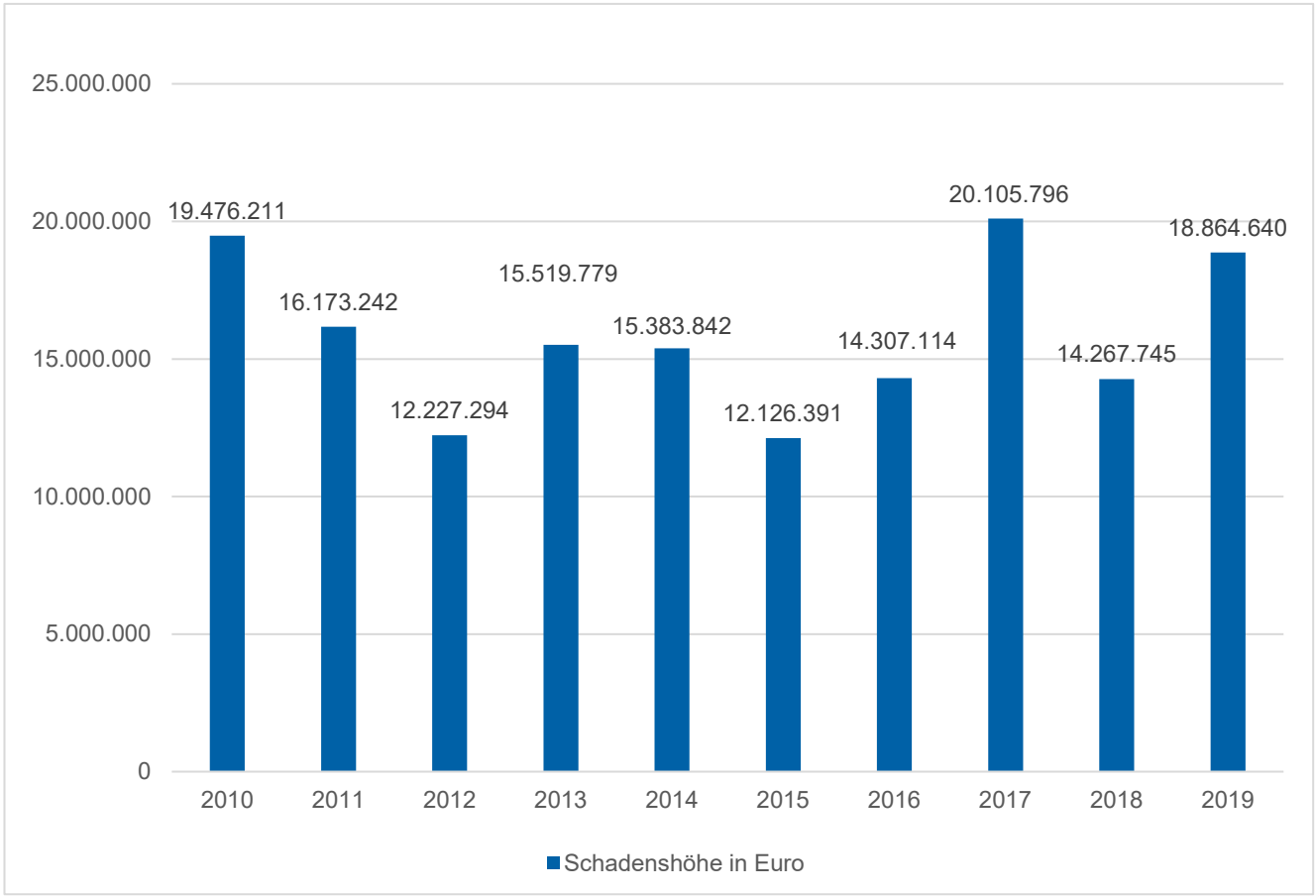
Tabelle 3
Aufklärungsquote

Delikt	Aufgeklärte Fälle		Aufklärungsquote		Zu-/Abnahme
	2018	2019	2018	2019	%-Punkte
Computerkriminalität (Cybercrime im engeren Sinne)	**6 994**	**5 911**	**35,5 %**	**29,4 %**	- 6,1
Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei der Datenverarbeitung §§ 269, 270 StGB	649	567	36,4 %	33,4 %	- 3,0
Datenveränderung, Computersabotage §§ 303a, 303b StGB	185	190	20,4 %	19,6 %	- 0,8
Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen und Datenhehlerei §§ 202a, 202b, 202c, 202d StGB	613	513	24,3 %	20,2 %	- 4,1
Softwarepiraterie (private Anwendung z. B. Computerspiele) § 106 ff. UrhG	26	11	96,3%	100,0 %	+ 3,7
Softwarepiraterie in Form gewerbsmäßigen Handelns § 108a UrhG	10	9	40,0 %	100,0 %	+ 60,0
Computerbetrug insgesamt § 263a StGB	5 511	4 621	38,2 %	31,0 %	- 7,2
Betrügerisches Erlangen von Kfz § 263a StGB	1	5	50,0 %	45,5 %	- 4,5
Weitere Arten des Warenkreditbetruges § 263a StGB	2 703	2 179	47,1 %	37,9 %	- 9,2
Computerbetrug mittels rechtswidrig erlangter Zahlungskarten mit PIN § 263a StGB	953	901	32,5 %	32,8 %	+ 0,3
Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten § 263a StGB	372	354	24,3 %	19,8 %	- 4,5
Computerbetrug mittels rechtswidrig erlangter sonstiger unbarer Zahlungsmittel § 263a StGB	274	176	48,5 %	34,5 %	- 14,0
Leistungskreditbetrug § 263a StGB	385	279	36,7 %	22,6 %	- 14,1
Computerbetrug (sonstiger) § 263a StGB	723	687	30,5 %	25,7 %	- 4,8
Missbräuchliche Nutzung von Telekommunikationsdiensten § 263a StGB	37	8	54,4 %	18,6 %	- 35,8
Abrechnungsbetrug im Gesundheitswesen § 263a StGB	9	1	100,0 %	100,0 %	0
Überweisungsbetrug § 263a StGB	54	31	36,5 %	24,8 %	- 11,7

2.1.3 Schadensentwicklung

Schäden von Cybercrime werden in der PKS ausschließlich für Computerbetrug und Softwarepiraterie abgebildet. Im Jahr 2019 erhöhte sich der Gesamtschaden um 4.596.895 Euro auf 18.864.640 Euro. Dies entspricht einem Anstieg von 32,2 Prozent.
Ein hohes Dunkelfeld existiert bei Schäden, die durch Erpressungsdelikte wie Ransomware zum Nachteil von Firmen entstehen. Die PKS weist lediglich Schadensummen für Erpressungen allgemein aus. Eine separate statistische Erfassung von Cybercrime-Erpressungsdelikten gibt es nicht. Zudem werden erfolgreiche Erpressungen nur selten zur Anzeige gebracht.

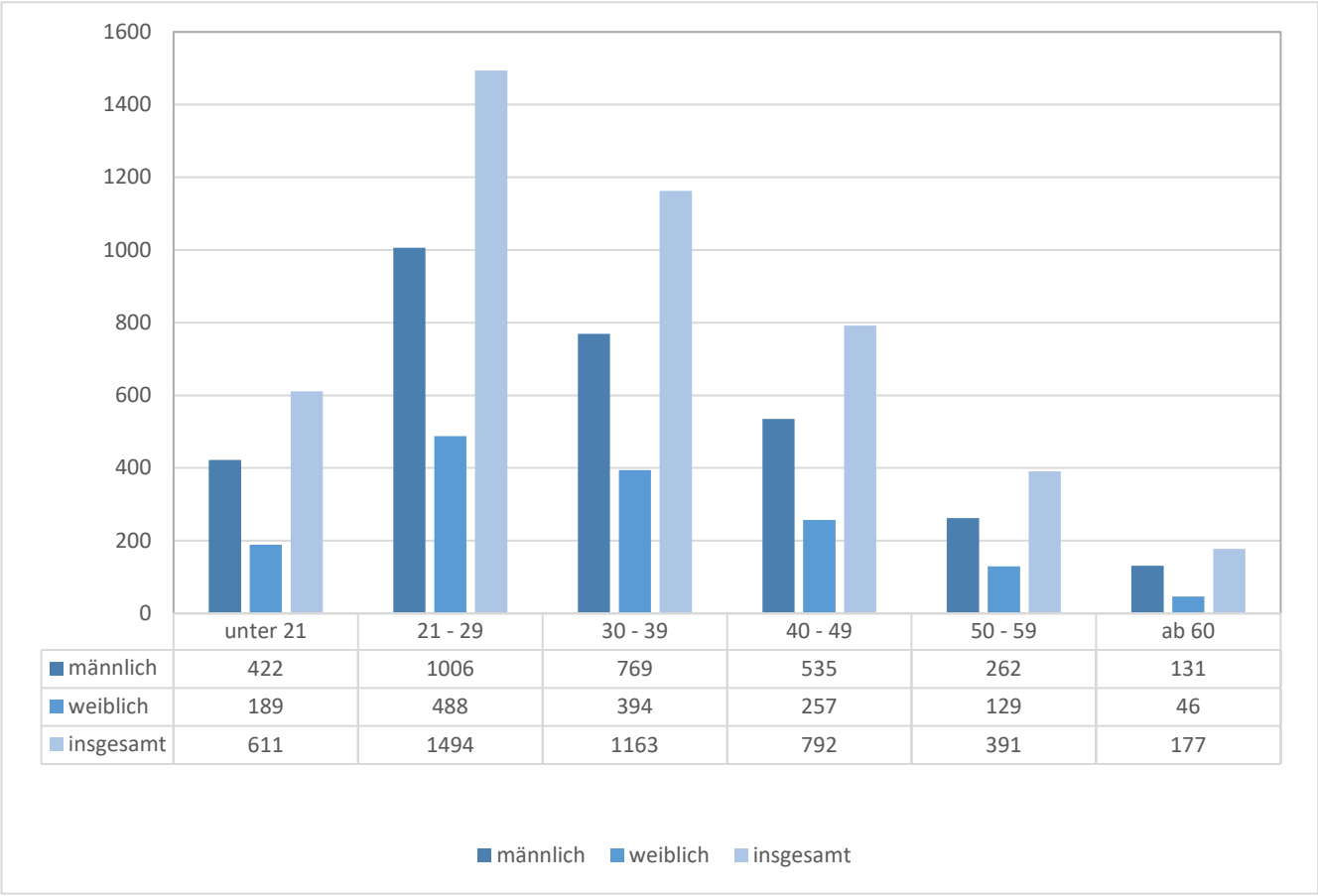
Abbildung 2
Schadensentwicklung



2.1.4 Tatverdächtige

Im Jahr 2019 wurden 4 628 (5 068) Tatverdächtige ermittelt. Den größten Anteil nahm mit 1 494 ermittelten Tatverdächtigen die Gruppe der Erwachsenen im Alter von 21 bis 29 Jahren ein. Der Anteil an männlichen Tatverdächtigen ist mit 3 125 im Verhältnis zur Gesamtzahl deutlich überrepräsentiert.

Abbildung 3
Tatverdächtige



	unter 21	21 - 29	30 - 39	40 - 49	50 - 59	ab 60
männlich	422	1006	769	535	262	131
weiblich	189	488	394	257	129	46
insgesamt	611	1494	1163	792	391	177

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 2019 (1 699) im Vergleich zum Vorjahr (1 783) um 4,7 Prozent gesunken. Die Aufklärungsquote im Jahr 2019 betrug 33,4 Prozent (36,4 Prozent). Im fünfjährigen Vergleichszeitraum sind die Fallzahlen um 18,8 Prozent gesunken. Die Aufklärungsquote ist im gleichen Zeitraum um 3,5 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.

Der Phänomenbereich Ransomware betrifft nicht nur Privatpersonen und Firmen in der Privatwirtschaft. Ebenso Institutionen der öffentlichen Hand sind Ziel entsprechender Angriffe. So wurden im Jahr 2019 der Dateiserver eines Gerichts wie auch das Dateisystem einer städtischen Grundschule verschlüsselt. In beiden Fällen wurde nicht auf die Geldforderung eingegangen und die Daten konnten durch externe Dienstleister wiederhergestellt werden.

Die Fallzahlen sind im Jahr 2019 (969) im Vergleich zum Vorjahr (909) um 6,6 Prozent gestiegen. Die Aufklärungsquote im Jahr 2019 betrug 19,6 Prozent (20,4 Prozent). Im fünfjährigen Vergleichszeitraum sind die Fallzahlen um 28,3 Prozent gesunken. Die Aufklärungsquote ist im gleichen Zeitraum um 4,6 Prozentpunkte gestiegen.

Eine besondere Form der Schadsoftware stellt EMOTET dar. Die Software gelangte als Word- oder PDF-Anhang von Spam-Mails auf die Rechner der Geschädigten. Ist EMOTET auf dem IT-System, lädt es selbständig weiter Schadsoftware nach. EMOTET fungierte sozusagen als „Vorbereiter“.

Eine weitere beliebte Software der Täter ist TRICKBOT. TRICKBOT spioniert das betroffene System aus. Dabei gelangen sensible Informationen in die Hände der Täter. Auf Grundlage dieser Daten suchen sich Täter ihre Opfer aus. Entscheiden sich die Täter im nächsten Schritt für eine Erpressung, wird die Ransomware RUYK nachgeladen und das IT-System verschlüsselt. Forderungen im sechsstelligen Bereich sind keine Seltenheit. Zwischen dem ersten Kontakt und der endgültigen Verschlüsselung vergehen oft Wochen oder Monate.

EMOTET, TRICKBOT und RUYK „arbeiten“ als aufeinander abgestimmtes System zusammen.

Wie hoch der monetäre Schaden für Unternehmen, öffentliche Verwaltung und Privathaushalten ist, kann aufgrund des Dunkelfelds nicht beziffert werden.

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.

Die Fallzahlen sind im Jahr 2019 (2 544) im Vergleich zum Vorjahr (2 528) um 0,6 Prozent gestiegen. Die Aufklärungsquote im Jahr 2019 betrug 20,2 Prozent (24,3 Prozent). Im fünfjährigen Vergleichszeitraum sind die Fallzahlen um 18,3

[5] Das internetbasierte Zusammentragen und Veröffentlichen von personenbezogener Daten

Prozent gesunken. Die Aufklärungsquote ist im gleichen Zeitraum um 5,6 Prozentpunkte gestiegen.

Eine Ursache für den Rückgang der Fallzahlen im Fünf-Jahres-Vergleich könnte ein geändertes Anzeigenverhalten sein. So wird nicht mehr jeder Versuch/jede Vorbereitung mittels Phishing-Mail Daten auszuspähen zur Anzeige gebracht. Daneben werden auch die eingesetzten Virenscanner immer besser bei der Erkennung solcher E-Mails.

Computerbetrug mittels rechtswidrig erlangter Zahlungskarten mit PIN

Die Fallzahlen sind im Jahr 2019 (2 749) im Vergleich zum Vorjahr (2 937) um 6,4 Prozent gesunken. Die Aufklärungsquote im Jahr 2019 betrug 32,8 Prozent (32,5 Prozent).

Im fünfjährigen Vergleichszeitraum sind die Fallzahlen um 28,2 Prozent gesunken. Die Aufklärungsquote ist im gleichen Zeitraum um 1,3 Prozentpunkte gestiegen. Grund für den Rückgang der Fallzahlen dürfte sein, dass der Umgang mit Zahlungskarten und die Aufbewahrung der dazugehörigen PIN zunehmend verantwortungsbewusster erfolgt.

Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten

Zahlungskartendaten, die durch Phishing oder Skimming rechtswidrig abhandenkamen, wurden zum Teil im Internet eingesetzt, um Waren zu erlangen. Auch dienen die Daten dazu 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 2019 (1 790) im Vergleich zum Vorjahr (1 530) um 17 Prozent gestiegen. Die Aufklärungsquote im Jahr 2019 betrug 19,8 Prozent (24,3 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 2019 (510) im Vergleich zum Vorjahr (565) um 9,7 Prozent gesunken. Die Aufklärungsquote im Jahr 2019 betrug 34,5 Prozent (48,5 Prozent).

Leistungskreditbetrug

Beim Leistungskreditbetrug erbringt der Verkäufer eine Leistung im Voraus. Der Täter bestellt diese Leistung über das Internet, beauftragt 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 2019 (1 237) im Vergleich zum Vorjahr (1 049) um 17,9 Prozent gestiegen. Die Aufklärungsquote im Jahr 2019 betrug 22,6 Prozent (36,7 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 oder Telefonanlagen von Firmen oder Privatleuten zugreifen und so teure Verbindungen in das Ausland oder zu Mehrwertdiensten herstellen.

Die Fallzahlen sind im Jahr 2019 (43) im Vergleich zum Vorjahr (68) um 25 Fälle gesunken. Die Aufklärungsquote im Jahr 2019 betrug 18,6 Prozent (54,4 Prozent). Im fünfjährigen Vergleichszeitraum sind die Fallzahlen um 85,8 Prozent gesunken. Die Aufklärungsquote ist im gleichen Zeitraum um 3 Prozentpunkte angestiegen. Die Schadenssumme reduzierte sich zum Vorjahr (195.791 Euro) auf 114.235 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 der Vorgang automatisiert, erfüllt dies den Tatbestand des § 263a StGB.

Die Fallzahlen sind im Jahr 2019 (125) im Vergleich zum Vorjahr (148) um 15,5 Prozent gesunken. Die Aufklärungsquote im Jahr 2019 betrug 24,8 Prozent (36,5 Prozent).

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. 2019 wurden 56 405 Fälle mit dem Tatmittel Internet erfasst, 686 mehr als 2018. Den größten Anteil nahmen hierbei Betrugsdelikte mit 71,4 Prozent ein. Bei einer Aufklärungsquote von 55,7 Prozent wurden 31 437 Fälle aufgeklärt.

Abbildung 4
Tatmittel Internet - Fallzahlen und Aufklärungsquote

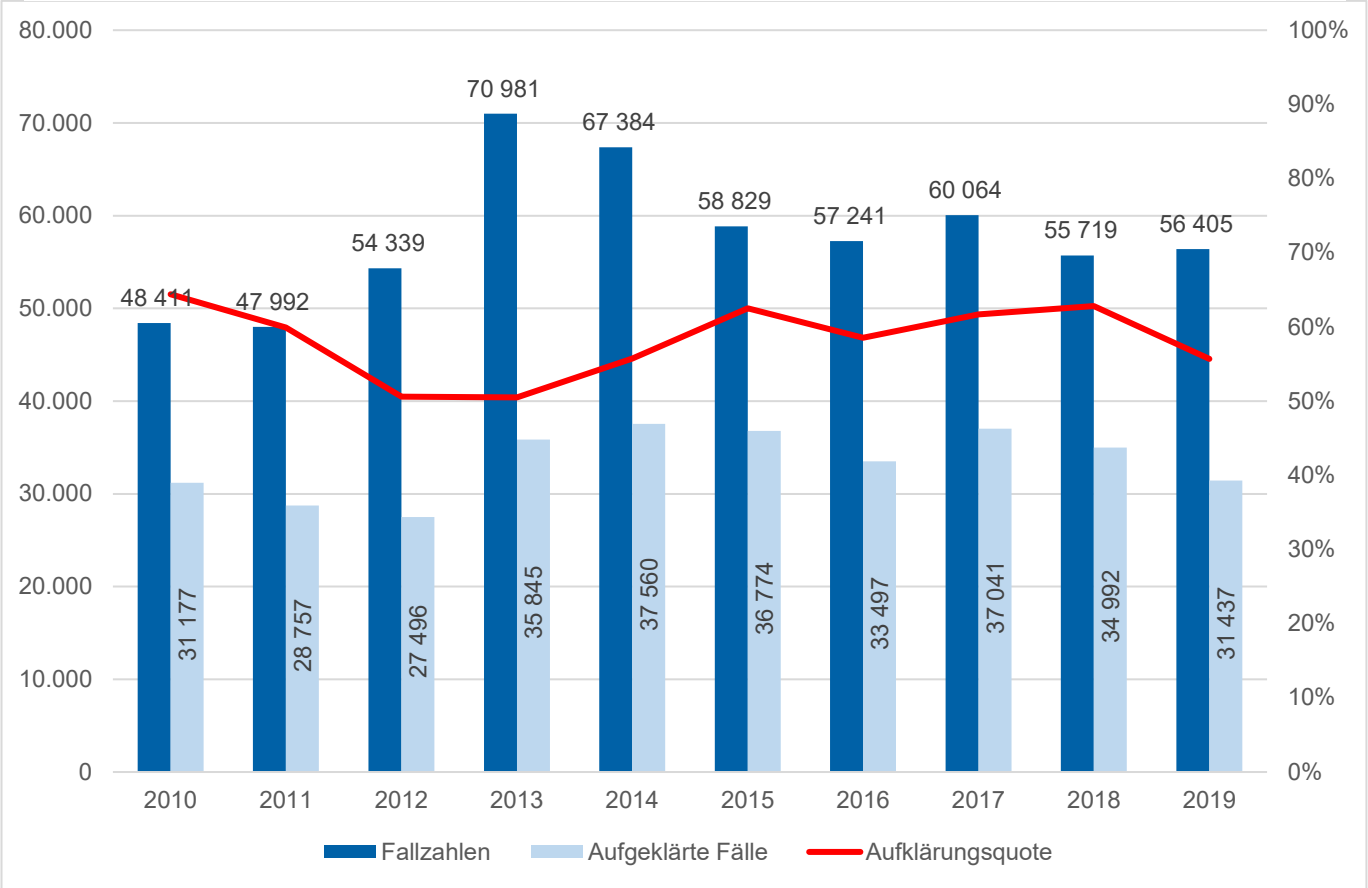


Tabelle 4
Tatmittel Internet

	Gesamt-kriminalität	darunter Tatmittel Internet	
Straftaten	**2019**	**Fälle**	**Anteil in %**
Alle Straftaten	**1 227 929**	**56 405**	**4,6**
Straftaten gegen die sexuelle Selbstbestimmung	15 174	2 512	16,6
Verbreitung pornografischer Schriften §§ 184, 184a, 184b, 184c, 184d, 184e StGB	3 250	2 056	63,3
Besitz/Verschaffen von Kinderpornografie § 184b StGB	2 359	1 531	64,9
Verbreitung von Kinderpornografie § 184b Abs. 1 Nr. 1	1 176	852	72,4
Betrug § 263 StGB	182 979	40 249	22,0
Waren- und Warenkreditbetrug § 263 StGB	64 891	27 912	43,0
Sonstiger Computerbetrug § 263a StGB	2 672	1 678	62,8
Betrügerisches Erlangen von Kfz § 263a StGB	11	2	18,2
Weitere Arten des Warenkreditbetruges § 263a StGB	5 748	4 485	78,0
Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten § 263a StGB	1 790	1 054	58,9
Computerbetrug mittels rechtswidrig erlangter sonstiger unbarer Zahlungsmittel § 263a StGB	510	245	48,0
Leistungskreditbetrug § 263a StGB	1 237	1 006	81,3
Überweisungsbetrug § 263a StGB	125	44	35,2
Missbräuchliche Nutzung von Telekommunikations-diensten §263a StGB	43	13	30,2
Fälschung beweiserheblicher Daten, Täuschung im Rechts-verkehr bei Datenverarbeitung §§ 269, 270 StGB	1 699	1 223	72,0
Datenveränderung, Computersabotage §§ 303a, 303b StGB	969	660	68,1
Ausspähen, Abfangen von Daten einschl. Vorbereitungs-handlungen und Datenhehlerei §§ 202a, 202b, 202c, 202d StGB	2 544	1 634	64,2
Erpressung § 253 StGB	3 461	1 732	50,0

3.2 Kinderpornografie

2019 wurden für den Deliktsbereich „Verbreitung, Erwerb und Besitz kinderpornografischer Schriften“ gemäß § 184b StGB 2 359 (1 412) Fälle erfasst. Dies entspricht einer Zunahme von 67 Prozent. In diesem Deliktsbereich besitzt das Internet eine herausragende Rolle. Bei 1 531 Fällen (64,9 Prozent) war das Internet Tatmittel. Hiervon konnten 1 422 Taten (92,9 Prozent) aufgeklärt werden. Ein Großteil der Ermittlungsverfahren ist auf das Hinweisaufkommen durch die teilstaatliche US-amerikanische Organisation „National Center for Missing and Exploited Children“ (NCMEC) zurückzuführen. Dabei war zu beobachten, dass die Anzahl der Hinweise leicht zurück ging, die Qualität der übermittelten Hinweise jedoch zunahm. Nach Prüfung der strafrechtlichen Relevanz und erfolgversprechender Ermittlungsansätze durch das BKA wurden dem LKA NRW über 1 100 Verdachtsfälle bekannt und nordrhein-westfälischen Polizeibehörden zu weiteren Ermittlungen zugeleitet.

Einen weiteren Schwerpunkt bilden Umfangsverfahren mit einer Vielzahl von Einzeltaten. 2019 wurden dem LKA NRW 66, auch in anderen Ländern geführte, Umfangsverfahren bekannt, die sich u. a. gegen 971 Tatverdächtige aus NRW richteten. Auffällig ist die hohe Anzahl der Tatverdächtigen unter 14 Jahren (217) und zwischen 14 und unter 18 Jahren (630). Insbesondere in sozialen Netzwerken wie z. B. Facebook, Instagram und Snapchat werden in Gruppen Bilder, Videos oder Links weitergeleitet.

Dabei ist zu beobachten, dass in den geteilten Bildern und Videos häufig Handlungen von Kindern zu sehen sind, die objektiv dem Bereich der Kinderpornografie zuzurechnen sind, aber den Eindruck erwecken, als seien die Kinder und Jugendlichen in ihrer sexuellen Experimentier- und Entdeckungsphase aufgenommen worden bzw. als hätten sie sich gegenseitig bei Sexualpraktiken aufgenommen.

Die Verbreitung dieser Dateien erfolgt aufgrund einer heterogenen Motivlage, die sich im Wesentlichen in drei Kategorien unterteilen lässt:

> Die Verbreiter finden die Darstellungen unterhaltsam (Dateien sind oft nachträglich mit entsprechenden Texten, Musik oder Geräuschen hinterlegt)

> Die Verbreiter leiten Dateien unreflektiert weiter (z. B. in WhatsApp-Gruppen mit vielen Teilnehmern und einem hohen Aufkommen an ausgetauschten Dateien)

> Die Verbreiter verfolgen einen „deliktsfremden“ Zweck (z. B. mit dem Ziel, den Empfängern zu schaden oder diesen die Abscheulichkeit der Inhalte zu vergegenwärtigen).

Gemeinsam ist diesen Fällen, dass sich die Versender über die Strafbarkeit und Sozialschädlichkeit ihres Handelns und die Folgen für die Empfänger und die Opfer häufig nicht im Klaren sind.

Als herausragend sind die Verfahren wegen (schweren) sexuellen Missbrauchs von Kindern und Verbreitung, Erwerb und Besitz kinderpornografischer Schriften in Lügde (BAO Eichwald) und Bergisch Gladbach (BAO Berg), zu nennen.

Die BAO Eichwald ermittelte seit Januar 2019 (vorher Ermittlungskommission „Camping“) mit bis zu 80 Mitarbeiterinnen und Mitarbeitern gegen mehrere Tatverdächtige. Die beiden hauptangeklagten Männer wurden zu 12 bzw. 13 Jahren Haft mit anschließender Sicherungsverwahrung verurteilt.

Die BAO Berg wurden im Oktober 2019 eingesetzt, nachdem bei Durchsuchungen in Bergisch Gladbach große Mengen kinderpornografischen Materials sichergestellt wurden. In der Spitze waren annähernd 350 Mitarbeiterinnen und Mitarbeiter an den Ermittlungen beteiligt. Stand 06.2020 wurden 28 Tatverdächtige und 31 Opfer identifiziert. Zwischenzeitlich erging ein erstes Urteil wegen schweren sexuellen Missbrauchs gegen einen der Hauptangeklagten: 10 Jahre Haft mit anschließender Sicherungsverwahrung. Die Ermittlungen dauern noch an.

In den vorgenannten Fällen wurden annähernd 100 Terabyte an Daten sichergestellt. Bereits 2018 hatte eine landesweite Arbeitsgruppe festgestellt, dass die IT-Ausstattung der Polizei NRW zur Auswertung und Bewertung derartiger Datenmengen nicht mehr zeitgemäß und kriminalfachlich nicht vertretbar ist[6].

[6] Abschlussbericht der Stabstelle „ Revision der kiminalpolizeilichen Bearbeitung von sexuellem Missbrauch von Kindern und Kinderpornografie“, des Ministerium des Innern NRW, Mai 2020

Als Konsequenz daraus hat das Land NRW zusätzlich Personalstellen geschaffen, vorhandenes Personal umorganisiert und eine Stabsstelle im Innenministerium zur „Revision der kriminalpolizeilichen Bearbeitung von sexuellen Missbrauch an Kindern und Kinderpornografie“ eingerichtet. Als eine der ersten Maßnahmen wurde leistungsstarke Hard- und Software beschafft.

Bei allem technischen Fortschritt und Ausstattung mit modernster Technik, muss ein Großteil der Arbeit dennoch „händisch“ erfolgen. Das Lesen und Bewerten tausender Chatprotokolle und das Erkennen von Zusammenhängen bleibt nach wie vor eine Herausforderung für Computer. Hier ist der Mensch unersetzbar.

4 Prävention

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

Bei der Prävention von Cybercrime wird zwischen Cybercrime im weiteren Sinn und Cybercrime im engeren Sinn unterschieden. Während die Prävention von Cybercrime im weiteren Sinn (Tatmittel Internet) vollständig in der Hand der KPB liegt, deckt das LKA NRW mit dem Cybercrime-Kompetenzzentrum den Bereich der Cybercrime-Prävention im engeren Sinn ab. Schwerpunkt sind in diesem Zusammenhang Wirtschaftsunternehmen, aber auch Behörden und vergleichbare Institutionen.

Die Prävention von Cybercrime im weiteren Sinne ist vor dem Hintergrund der vielfältigen Deliktsbereiche durch intensive Kooperationen geprägt. Hier wird das LKA NRW koordinierend tätig und setzt die Entwicklungen in diesem Deliktsbereich in Empfehlungen und Standards um.

Im Bereich Cybercrime im engeren Sinn wird ein bewährtes Netzwerk unterschiedlichster Kooperationspartner wie dem Bitkom[7], dem Voice[8] - Bundesverband der IT-Anwender und der Sicherheitspartnerschaft mit dem ASW NRW[9] bedient. Seit 2017 besteht eine gleichgelagerte Kooperationsvereinbarung mit dem eco[10] - Verband der Internetwirtschaft e.V. und dem networker NRW e.V.[11]

Durch die enge Zusammenarbeit erreicht das LKA unterschiedlichste Akteure als Multiplikatoren innerhalb der Wirtschaft, sensibilisiert für die Prävention von Cybercrime und nutzt hierbei Formate wie Informationsstände, Vorträge, Teilnahme an Kongressen und Messen. Durch die Beteiligung an „Round Tables“ und die Zusammenarbeit in Regionalgruppen baut das LKA Berührungsängste zwischen Wirtschaft und Polizei ab und steigert so die Anzeigebereitschaft und das Bewusstsein für die durch Cybercrime bestehenden Gefahren (Awareness). 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 sich mit geplanten Reaktionsmustern und Notfallplänen wappnen, können Angriffe deutlich besser abwehren, so dass geringere finanzielle Schäden entstehen oder ganz vermieden werden können.

Das LKA NRW sensibilisierte im Jahr 2019 durch über 100 Vorträge bei verschiedenen Veranstaltungen von Behörden und in der Wirtschaft zu den Gefahren durch Cybercrime.

Mit Voice und dem EU Gremium EMPACT veranstaltete das LKA NRW eine gemeinsame europäische Sicherheitstagung. Mit dem Bitkom und weiteren Landeskriminalämtern

[7] Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.
[8] Bundesverband der IT-Anwender e.V.
[9] Allianz für Sicherheit in der Wirtschaft Nordrhein-Westfalen e.V.
[10] eco - Verband der Internetwirtschaft e.V.
[11] networker NRW - Das Netzwerk der IT-Kompetenz

richtete das LKA NRW eine Fachtagung in Baden-Württemberg zur „Sicherheitskooperation Cybercrime“ aus.

Der Besuch von Großveranstaltungen wie der it-sa[12], dem Deutschen Präventionstag 2019, dem Tag der Medienkompetenz und weiteren Konferenzen wurden genutzt, um mit Vorträgen und Informationsständen die breite Öffentlichkeit zu erreichen.

Die Bekämpfung von Cybercrime ist eine Gesamtgesellschaftliche Aufgabe, bei der die Maßnahmen der polizeilichen Präventionsarbeit einen wesentlichen Beitrag leisten.

[12] Fachmesse mit begleitendem Kongress zum Thema Informationssicherheit

Herausgeber

Landeskriminalamt Nordrhein-Westfalen
Völklinger Straße 49
40221 Düsseldorf

Abteilung 4
Cybercrime-Kompetenzzentrum
Dezernat 41

Redaktion: Tobias Ulm
Telefon: +49 211 939-4118
Fax: +49 211 939-194118

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

Bildnachweis: Titelseite – Marita Segin