POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

bürgerorientiert · professionell · rechtsstaatlich

Cybercrime

Lagebild NRW 2020

Überblick Kriminalitätsentwicklung - Cybercrime

- Anstieg der Fallzahlen für den Bereich der Computerkriminalität (Cybercrime im engeren Sinne) um 20,76 Prozent
- Anstieg der Fallzahlen bei Straftaten mit Tatmittel Internet (Cybercrime im weiteren Sinne) um 8,62 Prozent
- Anstieg der Fallzahlen für den Deliktsbereich Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei der Datenverarbeitung um 64,27 Prozent
- Anstieg der Fallzahlen bei Betrug mit Tatmittel Internet um 13,18 Prozent
- Anstieg der Fallzahlen bei Verbreitung, Erwerb und Besitz kinderpornografischer Schriften um 102,46 Prozent

	2019	2020	Veränderung in %
Computerkriminalität (Cybercrime im engeren Sinne)	**20 118**	**24 294**	**+ 20,76**
Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei der Datenverarbeitung	1 699	2 791	+ 64,27
Datenveränderung/Computersabotage	969	1 258	+ 29,82
Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen und Datenhehlerei	2 544	2 292	- 9,91
Computerbetrug	14 886	17 934	+ 20,48
Softwarepiraterie (private Anwendung z.B. Computerspiele)	11	13	+ 18,18
Softwarepiraterie in Form gewerbsmäßigen Handelns	9	6	- 33,33
Anzahl der aufgeklärten Fälle der Cybercrime im engeren Sinne (AQ)	5 911	6 963	+ 17,80
Aufklärungsquote (AQ)	29,38%	28,66%	- 0,72
Straftaten mit Tatmittel Internet (Cybercrime im weiteren Sinne)	**56 405**	**61 267**	**+ 8,62**
Betrug mit Tatmittel Internet	40 249	45 554	+ 13,18
Erpressung mit Tatmittel Internet	1 732	1 226	- 29,21
Anzahl der aufgeklärten Fälle Cybercrime im weiteren Sinne (AQ)	31 437	33 752	+ 7,36
Aufklärungsquote (AQ)	55,73%	55,09%	- 0,64
Verbreitung, Erwerb und Besitz kinderpornografischer Schriften	**2 359**	**4 776**	**+ 102,46**

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 Europarats1.

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 basieren auf der Polizeilichen Kriminalstatistik (PKS). Klammerwerte bei Zahlenangaben beziehen sich, soweit nicht anders angegeben, auf das Vorjahr.

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

Der länderübergreifende Polizeiliche Informations- und Analyseverbund (PIAV) erlaubt eine differenziertere Auswertung zu einzelnen Delikten. Um neue Tatbegehungsformen der Cybercrime zeitnah zu erkennen, bietet PIAV den sachbearbeitenden Dienststellen auch die Möglichkeit, Straftaten über den deliktsspezifischen Katalog hinaus zu melden, wenn

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

[2] Die rechtswidrige Vervielfältigung und Verbreitung urheberrechtlich geschützter Software.

- 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.

Die Entwicklungen in diesem Kriminalitätsfeld im Jahr 2020 wurden durch die Corona - Pandemiesituation beeinflusst.

Kurzarbeit, Quarantäne, die Betreuungssituation von Kindern, Homeoffice und andere pandemiebedingten Anpassungen bewirkten, dass große Teile der Bevölkerung bedeutend mehr Zeit mit der Nutzung von Onlinediensten verbrachten. Viele Geschäfte konnten ihre Waren und Dienstleistungen zeitweise nur online anbieten.

Mit einer breiteren Nutzung von digitalen Dienstleistungen, z. B. Online-Banking und -Shopping, eröffnete sich für Cyberkriminelle ein weites Feld für kriminelle Aktivitäten. Die zwischen Bund und Ländern abgestimmten Lock-Down-Maßnahmen boten insofern mittelbar erweiterte Tatgelegenheiten im Bereich der Cyberkriminalität.

[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

2020 wurden 24 294 Cybercrime-Fälle erfasst. Dies entspricht einem Anstieg von 20,76 Prozent gegenüber dem Vorjahr (20 118). Die Anzahl der ermittelten Tatverdächtigen erhöhte sich um 11,62 Prozent auf 5 166 (4 628). Die am häufigsten vertretenen Delikte waren der Computerbetrug gemäß § 263a StGB, die Fälschung beweiserheblicher Daten gemäß § 269 StGB und das Ausspähen von Daten gemäß § 202a StGB.

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

Jahr	Erfasste Fälle	Veränderung in %	aufgeklärte Fälle	Aufklärungsquote
2010	19 775	+45,36	5 710	28,87 %
2011	20 036	+1,32	4 877	24,34 %
2012	22 228	+10,94	4 704	21,16 %
2013	27 016	+21,54	4 518	16,72 %
2014	20 715	-23,32	4 302	20,77 %
2015	16 645	-19,65	4 393	26,39 %
2016	22 708	+36,43	7 297	32,13 %
2017	22 913	+0,90	8 210	35,83 %
2018	19 693	-14,15	6 994	35,52 %
2019	20 118	+2,16	5 911	29,38 %
2020	24 294	+20,76	6 963	28,66 %

Tabelle 2
Fallzahlen in einzelnen Deliktsfeldern der Cybercrime im engeren Sinne

Delikt	2019	2020	Zu-/Abnahme	Veränderung
Computerkriminalität (Cybercrime im engeren Sinne)	**20 118**	**24 294**	**+ 4 176**	**+ 20,76 %**
Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei der Datenverarbeitung §§ 269, 270 StGB	1 699	2 791	+ 1 092	+ 64,27 %
Datenveränderung, Computersabotage §§ 303a, 303b StGB	969	1 258	+ 289	+ 29,82 %
Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen und Datenhehlerei §§ 202a, 202b, 202c, 202d StGB	2 544	2 292	- 252	- 9,91 %
Softwarepiraterie (private Anwendung z. B. Computerspiele) § 106 ff. UrhG	11	13	+ 2	+ 18,18 %
Softwarepiraterie in Form gewerbsmäßigen Handelns § 108a UrhG	9	6	- 3	- 33,33 %
Computerbetrug insgesamt § 263a StGB	14 886	17 934	+ 3 048	+ 20,48 %
Weitere Arten des Warenkreditbetruges § 263a StGB	5 748	6 257	+ 509	+ 8,86 %
Computerbetrug mittels rechtswidrig erlangter Zahlungskarten mit PIN § 263a StGB	2 749	2 583	- 166	- 6,04 %
Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten § 263a StGB	1 790	2 612	+ 822	+ 45,92 %
Computerbetrug mittels rechtswidrig erlangter sonstiger unbarer Zahlungsmittel § 263a StGB	510	1 098	+ 588	+ 115,29 %
Leistungskreditbetrug § 263a StGB	1 237	1 078	- 159	- 12,85 %
Computerbetrug (sonstiger) § 263a StGB	2 672	4 038	+ 1 366	+ 51,12 %
Missbräuchliche Nutzung von Telekommunikationsdiensten § 263a StGB	43	49	+ 6	+ 13,95 %
Abrechnungsbetrug im Gesundheitswesen § 263a StGB	1	1	0	0
Überweisungsbetrug § 263a StGB	125	208	+ 83	+ 66,4 %

2.1.2 Aufklärungsquote

Von den im Jahr 2020 erfassten Straftaten wurden 6 963 (5 911) aufgeklärt. Die Aufklärungsquote betrug 28,66 Prozent und verringerte sich gegenüber 2019 um 0,72 Prozentpunkte. Im Bereich des Computerbetrugs wurden 5 372 Fälle aufgeklärt. Dies entspricht einer Aufklärungsquote von 29,95 Prozent (31,04 Prozent).

Abbildung 1
Vergleich Fallzahlen und Aufklärungsquote Cybercrime im engeren Sinne

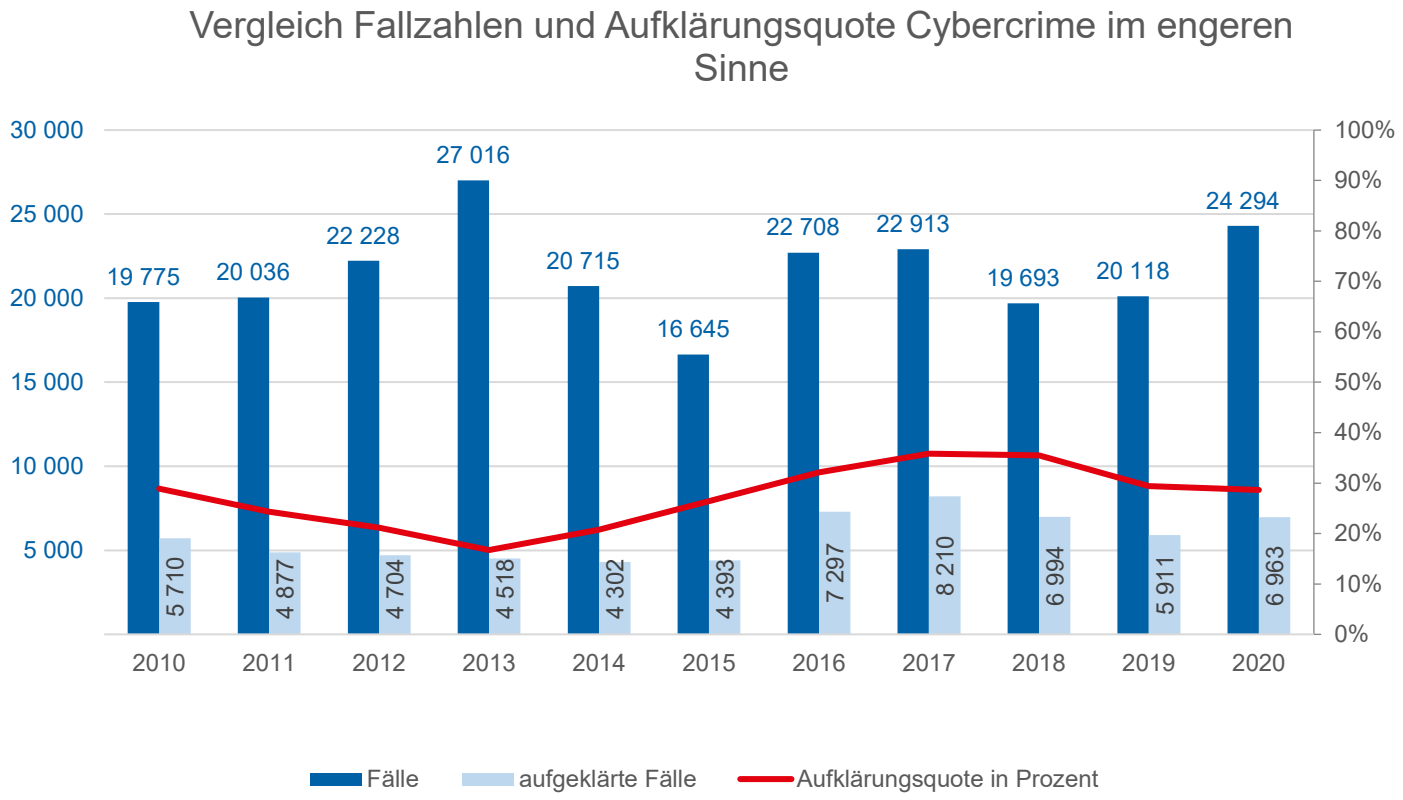


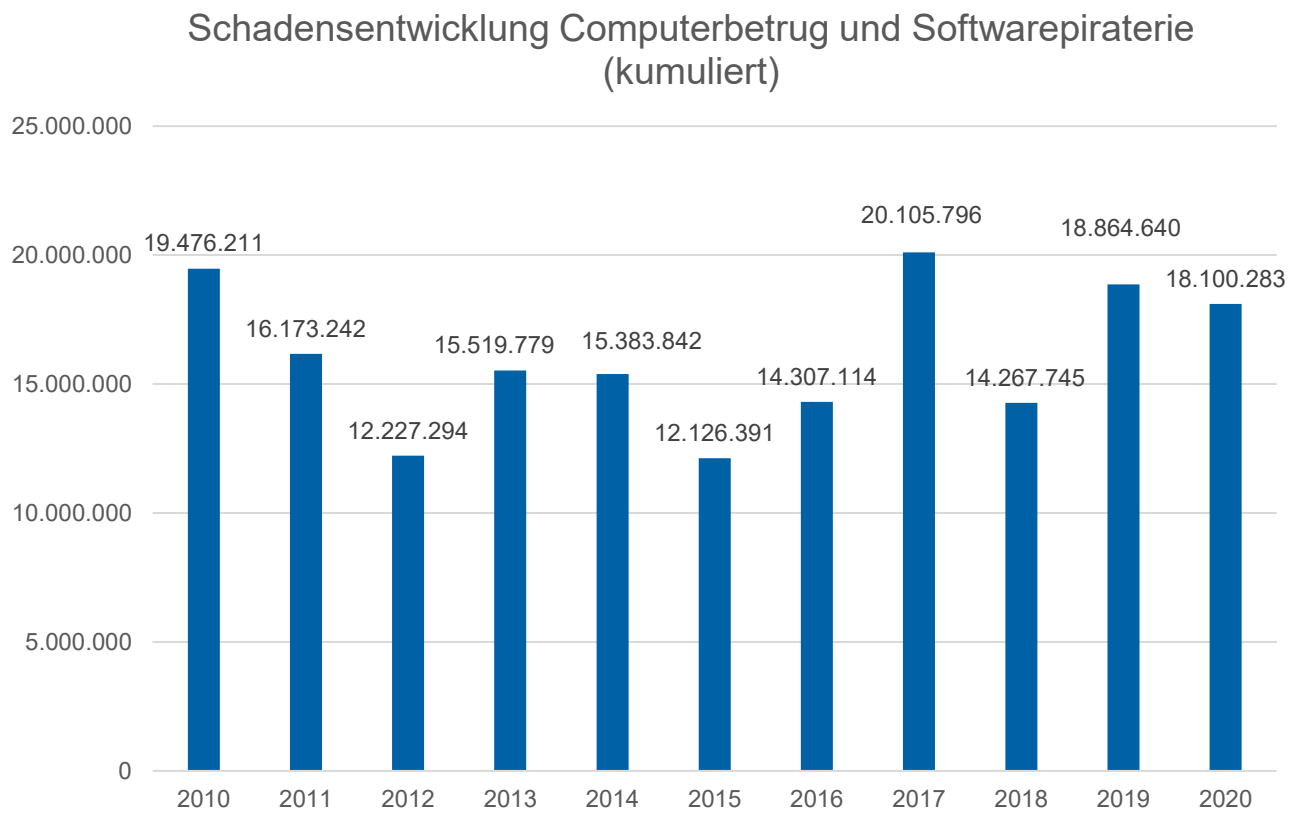
Tabelle 3
Aufklärungsquote (AQ)

Delikt	Aufgeklärte Fälle		Aufklärungsquote		Zu-/Abnahme (AQ)
	2019	2020	2019	2020	%-Punkte
Computerkriminalität (Cybercrime im engeren Sinne)	**5 911**	**6 963**	**29,38 %**	**28,66 %**	**- 0,72**
Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei der Datenverarbeitung §§ 269, 270 StGB	567	707	33,37 %	25,33 %	- 8,04
Datenveränderung, Computersabotage §§ 303a, 303b StGB	190	198	19,61 %	15,74 %	- 3,87
Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen und Datenhehlerei §§ 202a, 202b, 202c, 202d StGB	513	668	20,17 %	29,14 %	+ 8,97
Softwarepiraterie (private Anwendung z. B. Computerspiele) § 106 ff. UrhG	11	12	100,0 %	92,31 %	- 7,69
Softwarepiraterie in Form gewerbsmäßigen Handelns § 108a UrhG	9	6	100,0 %	100,0 %	/
Computerbetrug insgesamt § 263a StGB	4 621	5 372	31,04 %	29,95 %	- 1,09
Weitere Arten des Warenkreditbetruges § 263a StGB	2 179	2 506	37,91 %	40,05 %	+ 2,14
Computerbetrug mittels rechtswidrig erlangter Zahlungskarten mit PIN § 263a StGB	901	607	32,78 %	23,50 %	- 9,28
Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten § 263a StGB	354	450	19,78 %	17,23 %	- 2,55
Computerbetrug mittels rechtswidrig erlangter sonstiger unbarer Zahlungsmittel § 263a StGB	176	242	34,51 %	22,04 %	- 12,47
Leistungskreditbetrug § 263a StGB	279	331	22,55 %	30,71 %	+ 8,16
Computerbetrug (sonstiger) § 263a StGB	687	1 160	25,71 %	29,00 %	+ 3,29
Missbräuchliche Nutzung von Telekommunikationsdiensten § 263a StGB	8	10	18,60 %	20,41 %	+ 1,81
Abrechnungsbetrug im Gesundheitswesen § 263a StGB	1	1	100,0 %	100,0 %	/
Überweisungsbetrug § 263a StGB	31	58	24,80 %	27,88 %	+ 3,08

2.1.3 Schadensentwicklung

Schäden von Cybercrime werden in der PKS ausschließlich für Computerbetrug und Softwarepiraterie abgebildet. Im Jahr 2020 verringerte sich der Gesamtschaden um 764.357 Euro auf 18.100.283 Euro und bleibt somit auf ähnlich hohen Niveau. 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.

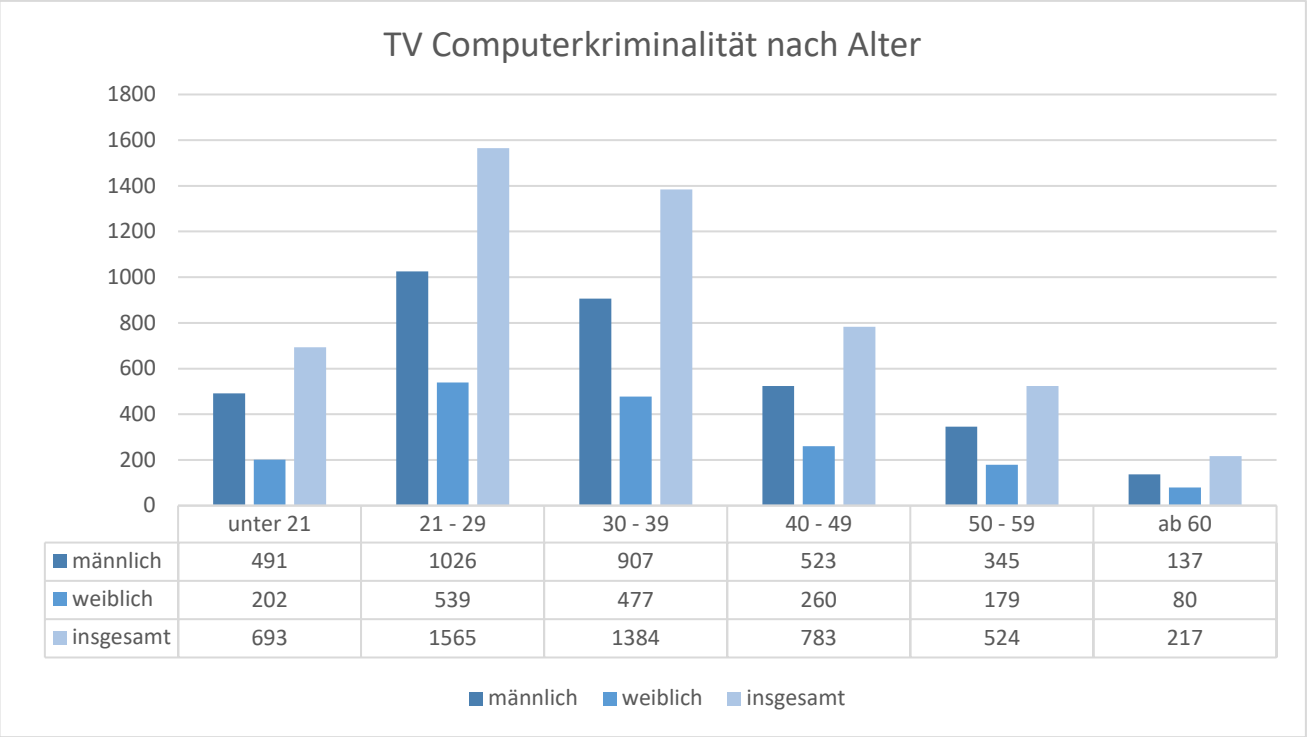
Abbildung 2
Schadensentwicklung Computerbetrug und Softwarepiraterie (kumuliert)



2.1.4 Tatverdächtige

Im Jahr 2020 wurden 5 166 (vorher 4 628) Tatverdächtige ermittelt. Den größten Anteil nahm mit 1 565 ermittelten Tatverdächtigen die Gruppe der Erwachsenen im Alter von 21 bis 29 Jahren ein. Der Anteil an männlichen Tatverdächtigen ist mit 3 429 im Verhältnis zur Gesamtzahl von 5 166 überrepräsentiert.

Abbildung 3
Tatverdächtige



	unter 21	21 - 29	30 - 39	40 - 49	50 - 59	ab 60
männlich	491	1026	907	523	345	137
weiblich	202	539	477	260	179	80
insgesamt	693	1565	1384	783	524	217

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.

Das Land NRW hat am 27. März 2020 für die Bewilligung von Soforthilfen im Rahmen der Corona-Krise für betroffene Unternehmen und Selbständige die Internetseite https://soforthilfe-corona.nrw.de gestartet. Darauf wurde ein Antragsvordruck zur Verfügung gestellt, mit dem die sogenannte „Corona-Soforthilfe“ beantragt werden konnte.

Am 07. April 2020 erreichten das LKA NRW erste Hinweise auf eine betrügerische Website, die der offiziellen Internetseite täuschend echt nachempfunden war. Damit gelangten Kriminelle an die persönlichen Daten der Betroffenen. Mit diesen Daten füllten die Kriminellen ihrerseits auf der realen Internetseite den Soforthilfe Antrag aus. Sie ersetzten die Bankverbindung durch ihre eigene und versuchten auf diese Weise betrügerisch an die staatliche Soforthilfe zu gelangen.

Das LKA NRW richtete am 08. April 2020 eine Ermittlungskommission für landeszentrale Ermittlungen ein. Die EK Klon konnte mehrere Fake-Website ermitteln, die die offizielle Internetseite der Landesregierung nachahmten. Bis Ende des Jahres 2020 wurden 1 158 Strafanzeigen in diesem Ermittlungskomplex erstattet. In 20 Fällen kam es tatsächlich zur Auszahlung auf Konten der Betrüger. Dadurch entstand ein wirtschaftlicher Schaden von 308.000 Euro.

Ihre große Reichweite im Internet erreichten die Kriminellen durch die Platzierung von Fake-Webseiten an prominenter Position der Google-Trefferseite. Der Sachverhalt verdeutlicht, dass Kriminelle auf besondere Situationen schnell und professionell reagieren und solche Umstände für ihre Zwecke auszunutzen können.

Die Fallzahlen im Deliktsbereich „Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei der Datenverarbeitung §§ 269, 270 StGB“ sind im Jahr 2020 (2 791) im Vergleich zum Vorjahr (1 699) um 64,27 Prozent gestiegen. Die Aufklärungsquote im Jahr 2020 betrug 25,3 Prozent (vorher 36,4 Prozent). Im fünfjährigen Vergleichszeitraum sind die Fallzahlen um 48,54 Prozent gestiegen. Die Aufklärungsquote ist im gleichen Zeitraum um 7,24 Prozentpunkte gefallen.

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, wird Software auf sein System installiert, die den Abfluss und die Verschlüsselung von Daten durch den Täter ermöglicht. Initiiert der Täter die Verschlüsselung, so sind die Daten für den Inhaber nicht mehr nutzbar. Zur Entschlüsselung der Daten wird ein Lösegeld gefordert. Mit den zuvor gewonnen Daten verleiht der Täter mit dem Hinweis auf eine ihm mögliche Veröffentlichung seiner Forderung Nachdruck.

Die Fallzahlen im Deliktsbereich „Datenveränderung, Computersabotage §§ 303a, 303b StGB“ sind im Jahr 2020 (1 258) im Vergleich zum Vorjahr (969) um 29,82 Prozent gestiegen. Die Aufklärungsquote im Jahr 2020 betrug 15,74 Prozent (vorher 19,61 Prozent).

Straftaten durch Ransomware betreffen Privatpersonen, Wirtschaftsunternehmen und Institutionen der öffentlichen Hand. So wurden im Jahr 2020 mehrere Server des Universitätsklinikums in Düsseldorf verschlüsselt, sodass die Versorgung durch das Universitätsklinikum nicht gewährleistet werden konnte. Operationen mussten verlegt und Notfälle auf umliegende Krankenhäuser umgeleitet werden. Die Wiederherstellung der IT-Infrastruktur nahm mehrere Wochen in Anspruch. Bei der Schadsoftware handelt es sich um die Ransomware „DoppelPaymer“. Mit derselben Schadsoftware wurden einige Wochen später Serversysteme der Funke Mediengruppe verschlüsselt. Die Täter drohten mit der Veröffentlichung der zuvor abgeflossenen Daten, sollte die Medienagentur nicht auf die Lösegeldforderung eingehen.

Die durch Berichterstattung in den Medien bekannte Ransomware „EMOTET“ gelangte ebenfalls als Anhang von E-Mails auf die Rechner von Geschädigten. EMOTET lädt selbständig weitere Schadsoftware wie TRICKBOT und Ryuk nach. Dabei ist EMOTET so programmiert, dass sich die Software nach dem initialen Befall des IT-Systems zunächst unauffällig verhält. Bis zu mehrere Monate kann es dauern, bis EMOTET aktiv wird und TRICKBOT und Ryuk nachlädt. TRICKBOT kopiert den Datenbestand des betroffenen IT-Systems auf IT-Systeme der Tätergruppierung. Nachdem dies geschehen ist, wird durch Ryuk das betroffene IT-System verschlüsselt und eine Erpressernachricht (engl. Ransomnote) hinterlassen, die eine Geldforderung in Bitcoin und eine Drohung bzgl. einer Datenveröffentlichung enthält.

Wie hoch der Schaden für Unternehmen, öffentliche Verwaltung und Privathaushalte ist, kann aufgrund des Dunkelfelds nicht beziffert werden. Am Anfang des Jahres 2021 wurde das EMOTET-Netzwerk durch ein internationales Polizeibündnis, das durch EUROPOL koordiniert wurde, zerschlagen.

Insgesamt ist eine hohe Professionalisierung der Täter festzustellen, welche sich u. a. durch Arbeitsteilung verschiedener krimineller Akteure auszeichnet. Unterschiedliche Handlungsfelder sind die Entwicklung und Vermarktung der Schadsoftware, die Einschleusung in die Fremdsysteme und die Korrespondenz mit den Betroffenen. Letztere findet in einigen Fälle im Stil eines IT-Support-Services statt, der durch den Prozess der Lösegeldzahlung und Wiederinbetriebnahme der IT-Systeme begleitet.

Unter der Überschrift „Cybercrime as a Service“ kann man im Internet auf diese kriminellen Dienstleister zugreifen, die gegen Bezahlung u. a. Schadsoftware zur Verfügung stellen oder DDoS-Angriffe als Auftragsleistung durchführen. Die Initiierung entsprechender Angriffe bedarf damit keiner fundierten Kenntnisse oder eigner technischer Infrastruktur.

Mit der fortschreitenden Digitalisierung und der einhergehenden Abhängigkeit unserer Gesellschaft wächst das Schadenspotential durch kriminelle Aktivitäten weiter an. Die Entwicklungen um das Pandemiegeschehen haben die Digitalisierung, beispielsweise durch Homeoffice und Homeschooling, weiter vorangetrieben. Demzufolge waren 2020 auch Schulen von DDoS-Angriffen betroffen, sodass es zeitweise zu Ausfällen kam. In mindestens einem Fall wurde die Störung durch einen Schüler initiiert.

Ausspähen, Abfangen von Daten einschließlich Vorbereitungshandlungen und Datenhehlerei

Identitätsattribute wie Name, Vorname, Geburtsdatum und Wohnanschrift aber auch Zugangsdaten, wie Benutzername und Kennwort werden durch Nutzer im digitalen Raum beispielsweise für Einkäufe in Onlineshops oder Vertragsabschlüsse im Versicherungssektor preisgegeben. Tätern gelingt es durch unterschiedliche Methoden diese Daten abzufangen und für anschließende Verwertungstaten zu nutzen. Das Sammeln von personenbezogenen Daten und die anschließende Veröffentlichung, sogenanntes Doxing, spielt in diesen Deliktsbereich ebenfalls eine Rolle.

Die Fallzahlen sind im Berichtsjahr 2020 mit 2 292 Fällen im Vergleich zu 2019 mit 2 544 Fällen um 9,91 Prozent gesunken. Die Aufklärungsquote im Jahr 2020 betrug 29,14 Prozent (20,17 Prozent).

Eine Ursache für den Rückgang der Fallzahlen könnte ein geändertes Anzeigenverhalten sein. So werden weniger Versuche der Datenausspähung mittels Phishing-Mail zur Anzeige gebracht. Daneben werden die eingesetzten Virenscanner und Nachrichtenfilter immer besser bei der Erkennung solcher E-Mails.

Bei der Bewilligung von Soforthilfen der Landesregierung im Rahmen der Corona-Krise für besonders betroffene Unternehmen nutzte eine unbekannte Täterschaft die Verunsicherungen zum Zeitpunkt der Antragstellung und Bewilligung der Corona-Soforthilfen aus und versendete Phishing-Emails. Diese erweckten den Eindruck von der Landesregierung NRW zu stammen. Die E-Mails stammten von der E-Mail Adresse corona-zuschuss@nrw.de.com (später: corona-zuschuss@bmwi.de.com).

Mit den Phishing-Mails wurde bei den Betroffenen der Eindruck erweckt, sie hätten von der Landesregierung Leistungen im Rahmen der Corona-Soforthilfe erhalten. In der E-Mail wurden die Betroffenen persönlich angesprochen und aufgefordert, die erhaltene Soforthilfe ihrem zuständigen Finanzamt mitzuteilen. Passend dazu verschicken die Täter eine Rechtsbelehrung und eine Bescheinigung für das Finanzamt. Diese sei auszufüllen und an o. g. E-Mail Adresse zurück zu schicken. Als Drohgebärde wiesen die Täter darauf hin, dass zu Unrecht erhaltene Zuschüsse und Falschangaben im Rahmen der Antragstellung zu Geld- und Freiheitsstrafen von bis zu fünf Jahren führen können.

Die Betroffenen, die auf diese Phishing-Mail reagierten und die Dokumente ausgefüllt an die Täter sendeten, erhielten eine zweite E-Mail. Darin waren Bankverbindungen angegeben, auf die die vorgeblich unrechtmäßig erlangte Soforthilfe zu überweisen sei. Zu diesem Modus Operandi wurden 111 Strafanzeigen erstattet.

Computerbetrug mittels rechtswidrig erlangter Zahlungskarten mit PIN

Die Fallzahlen im Deliktsbereich „Computerbetrug mittels rechtswidrig erlangter Zahlungskarten mit PIN“ sind im Jahr 2020 (2 583) im Vergleich zum Vorjahr (2 749) um 6,04 Prozent gesunken. Die Aufklärungsquote im Jahr 2020 betrug 23,50 Prozent (vorher 32,78 Prozent).

Grund für den Rückgang der Fallzahlen dürfte sein, dass der Umgang mit Zahlungskarten und 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 dienten die Daten dazu, 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 2020 (2 612) im Vergleich zum Vorjahr (1 790) um 45,92 Prozent gestiegen. Die Aufklärungsquote im Jahr 2020 betrug 17,23 Prozent (19,78 Prozent).

Computerbetrug mittels rechtswidrig erlangter sonstiger unbarer Zahlungsmittel

Sonstige 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 2020 (1 098) im Vergleich zum Vorjahr (510) um 115,29 Prozent gestiegen.

Die Aufklärungsquote im Jahr 2020 betrug 22,04 Prozent (34,51 Prozent). Im Jahr 2020 wurden vermehrt die Kontodaten von Payback-Kunden ausgespäht und die angesammelten Punkte durch die Täter zum Einkaufen mittels Gutscheinen bzw. zur Barauszahlung verwendet.

Leistungskreditbetrug

Beim Leistungskreditbetrug erbringt der Verkäufer eine Leistung im Voraus. Der Täter bestellt diese Leistung über das Internet, z. B. Auftrag zum 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 missbräuchlich verwendete reale Personalien genutzt. Die Fallzahlen sind im Jahr 2020 (1 078) im Vergleich zum Vorjahr (1 237) um 12,85 Prozent gesunken. Die Aufklärungsquote im Jahr 2020 betrug 30,71 Prozent (22,55 Prozent).

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 2020 (208) im Vergleich zum Vorjahr (125) um 66,40 Prozent gestiegen. Die Aufklärungsquote im Jahr 2020 betrug 27,88 Prozent (24,80 Prozent).

2.3 Kritische Infrastruktur - KRITIS

In Deutschland gibt es zahlreiche Institutionen und Einrichtungen, die die Basis für die Gewährleistung der grundlegenden Versorgung der Bevölkerung sind. Daher haben sie eine wichtige Bedeutung für das staatliche Gemeinwesen oder die öffentliche Sicherheit. Aus diesem Grund werden sie der sogenannten Kritischen Infrastruktur (KRITIS) zugerechnet.

Durch die fortschreitende Digitalisierung und Vernetzung können Ausfälle oder Beeinträchtigungen von IT-Komponenten unter Umständen auch eine Beeinträchtigung der Versorgungsdienstleistungen zur Folge haben und im schlimmsten Fall zu einer vollständigen Unterbrechung der Versorgung führen.

Dies kann sowohl den Energiesektor, die Abfallbeseitigung, den Gesundheitssektor oder auch die Lebensmittel- und Trinkwasserversorgung betreffen.

Anhand des oben beschriebenen Cybersicherheitsvorfalls im Universitätsklinikum Düsseldorf (Nr. 2.2), sind das Ausmaß und die Bedeutung solcher Vorfälle, bis hin zur Bedrohung von Menschenleben, sehr deutlich geworden.

Besonders durch die Corona-Pandemie stehen der Gesundheitssektor und die mit der Impfstoffentwicklung involvierten Wirtschaftsbereiche, wie beispielsweise Impfstoffhersteller, Impfzentren oder Zulieferfirmen im Fokus der gesellschaftlichen Aufmerksamkeit und somit auch im besonderen Interesse von Cyberkriminellen. Der Täterkreis kann dabei Einzeltäter mit monetären Zielen bis hin zu staatlichen gesteuerten Akteuren umfassen.

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 Straftaten in Betracht, deren Tatbestände durch das bloße Einstellen von Informationen in das Internet bereits erfüllt werden (so genannte Äußerungs- bzw. Verbreitungsdelikte) und 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 eines 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. 2020 wurden 61 267 Fälle mit dem Tatmittel Internet erfasst, 4 862 mehr als 2019. Den größten Anteil nahmen hierbei Betrugsdelikte mit 74,35 Prozent ein. Bei einer Aufklärungsquote von 55,1 Prozent wurden 33 752 Fälle aufgeklärt.

Abbildung 4
Tatmittel Internet - Fallzahlen und Aufklärungsquote

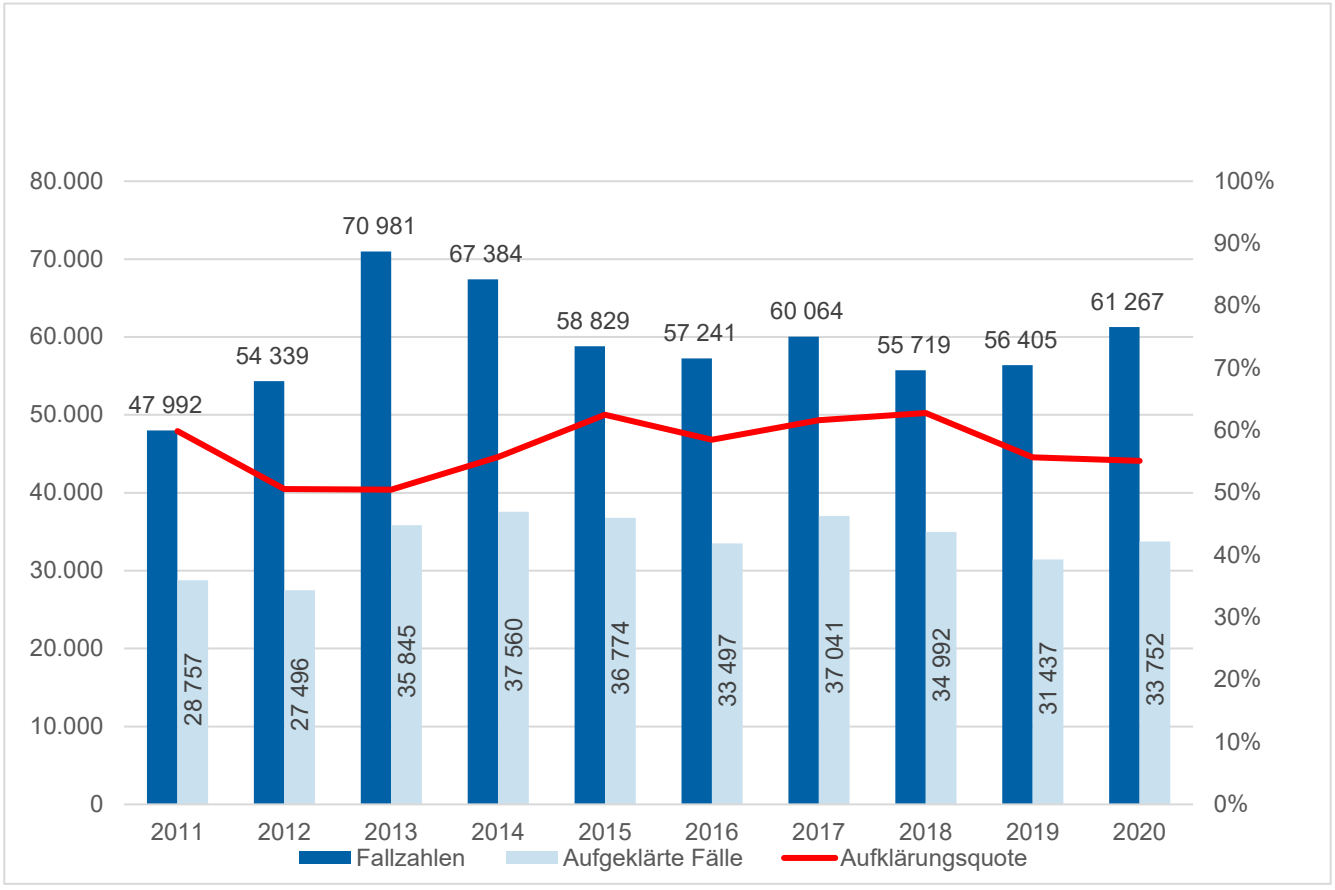


Tabelle 4
Tatmittel Internet

	Gesamt-kriminalität	darunter Tatmittel Internet	
Straftaten	**2020**	**Fälle**	**Anteil in %**
Alle Straftaten	**1 215 763**	**61 267**	**5,04**
Straftaten gegen die sexuelle Selbstbestimmung	19 736	4 177	21,16
Verbreitung pornografischer Schriften §§ 184, 184a, 184b, 184c, 184d, 184e StGB	6 434	3 585	55,72
Besitz/Verschaffen von Kinderpornografie § 184b StGB	4 776	2 758	57,75
Verbreitung von Kinderpornografie § 184b Abs. 1 Nr. 1	1 817	1 088	59,88
Betrug § 263 StGB	192 037	45 554	23,72
Waren- und Warenkreditbetrug § 263 StGB	64 891	30 842	47,53
Sonstiger Computerbetrug § 263a StGB	4 038	2 116	52,40
Weitere Arten des Warenkreditbetruges § 263a StGB	6 257	4 509	72,06
Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten § 263a StGB	2 612	1 257	48,12
Computerbetrug mittels rechtswidrig erlangter sonstiger unbarer Zahlungsmittel § 263a StGB	1 098	511	46,54
Leistungskreditbetrug § 263a StGB	1 078	701	65,03
Überweisungsbetrug § 263a StGB	208	73	35,09
Missbräuchliche Nutzung von Telekommunikations-diensten §263a StGB	49	21	42,86
Fälschung beweiserheblicher Daten, Täuschung im Rechts-verkehr bei Datenverarbeitung §§ 269, 270 StGB	2 791	1 747	62,59
Datenveränderung, Computersabotage §§ 303a, 303b StGB	1 258	770	61,21
Ausspähen, Abfangen von Daten einschl. Vorbereitungs-handlungen und Datenhehlerei §§ 202a, 202b, 202c, 202d StGB	2 292	1 239	54,06
Erpressung § 253 StGB	2 956	1 226	41,47

Kinderpornografie

2020 wurden für den Deliktsbereich „Verbreitung, Erwerb und Besitz kinderpornographischer Schriften“ gemäß § 184b StGB 4 776 (2 359) Fälle erfasst. Dies entspricht einer Zunahme von 102,46 Prozent, somit einer Verdoppelung der Fallzahlen. In diesem Deliktsbereich besitzt das Internet eine herausragende Rolle. Bei 2 758 Fällen (57,75 Prozent) war das Internet Tatmittel. Hiervon konnten 2 495 Taten (90,46 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 3 099 Verdachtsfälle bekannt und den nordrhein-westfälischen Kreispolizeibehörden (KPB) zu weiteren Ermittlungen zugeleitet. Korrespondierend stieg die Zahl der Tatverdächtigen aus NRW in bundesweiten Umfangsverfahren von 971 im Jahr 2019 auf 1 809 im Jahr 2020.

Besorgniserregend bleibt die hohe Anzahl der Tatverdächtigen unter 14 Jahren (428) und der Gruppe zwischen 14 und unter 18 Jahren (1 125). Dies macht insgesamt 43 % der bekannten Tatverdächtigen aus. Insbesondere in sozialen Netzwerken, wie z. B. Facebook, Instagram und Snapchat werden in Gruppen Bilder, Videos oder Links mit kinderpornografischem Inhalt in großen Mengen 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. Diese erwecken jedoch den Eindruck, dass die Kinder und Jugendlichen in ihrer sexuellen Experimentier- und Entdeckungsphase aufgenommen wurden oder sich gegenseitig bei Sexualpraktiken aufgenommen haben.

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

- Die Verbreiter finden die Darstellung lustig; Dateien sind oft nachträglich mit entsprechenden Texten oder mit Musik/Geräuschen hinterlegt.
- Die Verbreiter leiten die Datei 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 mehrheitlich nicht über die Folgen für sich selbst oder die Empfänger im Klaren sind.

4 Prävention

Die Prävention von Cybercrime obliegt den KPBn. Das 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. Adressaten sind in insbesondere 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.

Das LKA NRW entwickelte eine breit angelegte Kampagne zum Passwortschutz. Die Kooperationspartner Verbraucherzentrale NRW, eco-Verband der Internetwirtschaft e. V. und Bundesverband Verbraucherinitiative e. V. sind konzeptionell eingebunden. Die crossmediale Kampagne hat die Aufgabe, Präventionshinweise zu vermitteln, die auf Grundlage einer umfassenden Analyse der Schwachstellen bei den digitalen Endgeräten erstellt wurden. Am 26.10.2020 stellte der Minister des Innern des Landes Nordrhein-Westfalen, Herbert Reul, die Präventionskampagne www.mach-dein-passwort-stark.de der Öffentlichkeit vor und setzte den Startschuss.

Im Bereich Cybercrime im engeren Sinn wird ein bewährtes Netzwerk unterschiedlichster Kooperationspartner wie dem Bitkom, dem Voice - Bundesverband der IT-Anwender und der Sicherheitspartnerschaft mit dem ASW NRW bedient. Seit 2017 besteht eine gleichgelagerte Kooperationsvereinbarung mit dem eco - Verband der Internetwirtschaft e. V. und dem networker NRW e. V. Dieses Netzwerk wurde im Zusammenhang mit den Herausforderungen der aktuellen Pandemie genutzt, um auf die Gefahren der sprunghaft angestie-

genen Digitalisierung und die damit verbundenen Risiken aufmerksam zu machen. Insbesondere der Bereich Homeoffice und Sicherheit unternehmenskritischer Daten wurden vorangestellt.

Zudem wird durch die enge Zusammenarbeit erreicht, dass das LKA NRW unterschiedlichste Akteure als Multiplikatoren innerhalb der Wirtschaft für den Bereich Prävention von Cybercrime sensibilisiert. Durch die Beteiligung an „Round Tables“ und die Zusammenarbeit in Regionalgruppen verbessert das LKA NRW die vertrauensvolle Zusammenarbeit zwischen Wirtschaft und Polizei 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 Schäden entstehen oder ganz vermieden werden können.

Durch die vorherrschenden Distanzregeln im Coronajahr 2020 wurden nahezu alle Kontakte via Video-Konferenztechnik realisiert. Dieser Technikeinsatz ermöglicht eine noch höhere Kontaktdichte und Reichweite und wird dauerhaft ein wichtiger Kommunikationskanal der polizeilichen Präventionsarbeit. Dabei gab es beinahe wöchentliche Veranstaltungen mit einer Teilnehmerzahl im dreistelligen Bereich.

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

Herausgeber

Landeskriminalamt Nordrhein-Westfalen
Völklinger Straße 49
40221 Düsseldorf

Abteilung 4
Cybercrime-Kompetenzzentrum
Dezernat 41

Redaktion: Klaus Kisters
Telefon: +49 211 939-4110
Fax: +49 211 939-194110

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

Bildnachweis: Titelseite – Marita Segin