POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

bürgerorientiert · professionell · rechtsstaatlich

Cybercrime

Lagebild NRW 2022

Überblick Kriminalitätsentwicklung Cybercrime

- Rückgang der Fallzahlen für den Bereich der Computerkriminalität (Cybercrime im engeren Sinne) um 1,49 Prozent.
- Anstieg der ermittelten Tatverdächtigen um 9,36 Prozent.
- Anstieg der Fallzahlen bei Straftaten mit Tatmittel Internet (Cybercrime im weiteren Sinne) um 21,10 Prozent.
- Anstieg der Fallzahlen bei Betrug mit Tatmittel Internet um 16,86 Prozent.
- Rückgang der Fallzahlen für den Deliktsbereich Datenveränderung, Computersabotage um 27,77 Prozent.
- Rückgang der Fallzahlen für den Deliktsbereich Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen und Datenhehlerei um 12,61 Prozent.
- Rückgang der Fallzahlen bei Verbreitung, Erwerb, Besitz und Herstellung kinderpornografischer Inhalte um 1,28 Prozent.
- Anstieg der Fallzahlen für den Deliktsbereich Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten um 20,50 Prozent.
- Anstieg der Fallzahlen für den Deliktsbereich Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten mit PIN um 23,99 Prozent.
- Anstieg der Fallzahlen Deliktsbereich Computerbetrug mittels rechtswidrig erlangter sonstiger unbarer Zahlungsmittel um 33,07 Prozent.

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.[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

> 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 den Tabellen und Abbildungen aufgeführten Daten basieren auf der Polizeilichen Kriminalstatistik Nordrhein-Westfalen (PKS NRW). 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 sind beziehungsweise nicht zur Anzeige gebracht werden, wie unter Punkt 4 dargestellt wird.

Corona Pandemie

Die Entwicklungen im Kriminalitätsfeld Cybercrime wurden auch im Jahr 2022 durch die Corona-Pandemiesituation beeinflusst. Quarantäne, die Betreuungssituation von Kindern, Homeoffice und andere pandemiebedingte Anpassungen führten dazu, dass große Teile der Bevölkerung mehr Zeit mit der Nutzung von Onlinediensten verbrachten. Viele Geschäfte haben im Verlauf der Pandemie eigene Online Shops eröffnet beziehungsweise das bestehende Angebot erweitert. Einhergehend mit einer breiteren Nutzung digitaler Dienstleistungen, zum Beispiel Online-Banking und -Shopping, eröffneten sich für Cyberkriminelle vielfältige Gelegenheiten für ihre kriminellen Aktivitäten. Die Maßnahmen zur Eindämmung des Pandemiegeschehens boten insofern auch 2022 mittelbar Tatgelegenheiten im Bereich der Cyberkriminalität.

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

Auswirkungen des russischen Angriffskriegs auf die Ukraine

Mit Beginn des russischen Angriffskriegs auf die Ukraine am 24.02.2022 stellte das Bundesamt für Sicherheit in der Informationstechnik (BSI) in seiner Einschätzung der aktuellen Cyber-Sicherheitslage in Deutschland eine erhöhte Bedrohungslage fest. [2]

Dies gilt insbesondere für Unternehmen und Behörden, die als kritische Infrastrukturen (KRITIS) eingestuft sind. Die Bundesressorts definieren KRITIS wie folgt: „Kritische Infrastrukturen sind Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.“ Darunter fallen Institutionen aus dem Bereich Gesundheitswesen, Energie aber auch Lebensmittelversorgung und öffentliche Sicherheit.

Erschwernisse im Bereich der Cybercrime-Ermittlungen sind unter anderem Anonymisierungstechniken, fingierte digitale Spuren aber auch staatlich agierende Institutionen, die unter dem Deckmantel krimineller Gruppen agieren. Somit lässt sich in nur sehr wenigen Fällen ein direkter Bezug zum Ukrainekonflikt erkennen. Eine eindeutige Differenzierung von politisch motivierten Cyberangriffen und reinen Cybercrime-Vermögensdelikten ist daher oftmals nicht möglich. Gruppierungen wie KillNet bekannten sich unmittelbar nach Kriegsbeginn als solidarisch mit der russischen Föderation und erklärten alle Staaten, unter anderem Deutschland, die sich gegen den Angriffskrieg aussprechen, als direkte Ziele von Cyberangriffen. Hierbei kommen in erster Linie Distributed Denial of Service (DDoS)-Angriffe in Betracht, mit denen die Internetauftritte von Unternehmen und Behörden gestört werden, so dass sie nicht mehr erreichbar sind. Der angerichtete Schaden ist in der Regel gering.

Es ist möglich, dass auch unterschiedliche Ransomware-Gruppierungen ihr Verhalten nach Beginn des Angriffskriges gegen die Ukraine angepasst haben. Diese Gruppierungen dringen in die Systeme von Unternehmen ein, um deren Daten zu verschlüsseln. Eine Entschlüsselung erfolgt nur nach Zahlung eines Lösegelds (englisch: ransom). Auch wenn hier die monetäre Ausrichtung im Vordergrund steht, werden eventuell verstärkt Ziele in Ländern ausgewählt, die die Ukraine unterstützen.

Das Phänomen von verdeckten, politisch motivierten Cyberangriffen durch ausländische Organisationen und Staaten wird daher in Zukunft eine wachsende Herausforderung für die deutschen Sicherheitsbehörden bleiben.

2 Lagedarstellung Cybercrime im engeren Sinne

2.1 Verfahrensdaten

2.1.1 Fallzahlen

2022 wurden 29 667 Fälle von Cybercrime im engeren Sinne erfasst. Dies entspricht einem Rückgang von 1,49 Prozent gegenüber dem Vorjahr (30 115). Die häufigsten Delikte waren Computerbetrug gemäß § 263a StGB, Fälschung beweiserheblicher Daten gemäß § 269 StGB und Ausspähen von Daten gemäß § 202a StGB. Den größten Anstieg der Fallzahl gab es im Bereich der Zahlungskartenkriminalität gemäß § 263a StGB.

[2] https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2022/220225_Angriff-Ukraine-Statement.html?nn=1025778

Tabelle 1

Entwicklung der Fallzahlen und Aufklärungsquoten der Cybercrime im engeren Sinne

Jahr	Erfasste Fälle	Veränderung in %	aufgeklärte Fälle	Aufklärungsquote in %
2018	19 693	-14,05	6 994	35,52
2019	20 118	2,16	5 911	29,38
2020	24 294	20,76	6 963	28,66
2021	30 115	23,96	8 020	26,63
2022	29 667	-1,49	7 667	25,84

Quelle: PKS NRW

Hinweis: Seit dem Berichtsjahr 2021 werden die Delikte Softwarepiraterie (private Anwendung) und Softwarepiraterie in Form gewerbsmäßigen Handelns aufgrund geänderter Erfassungsrichtlinien nicht mehr in den Gesamtfallzahlen der Cybercrime im engeren Sinne erfasst.

Tabelle 2
Fallzahlen in einzelnen Deliktsfeldern der Cybercrime im engeren Sinne

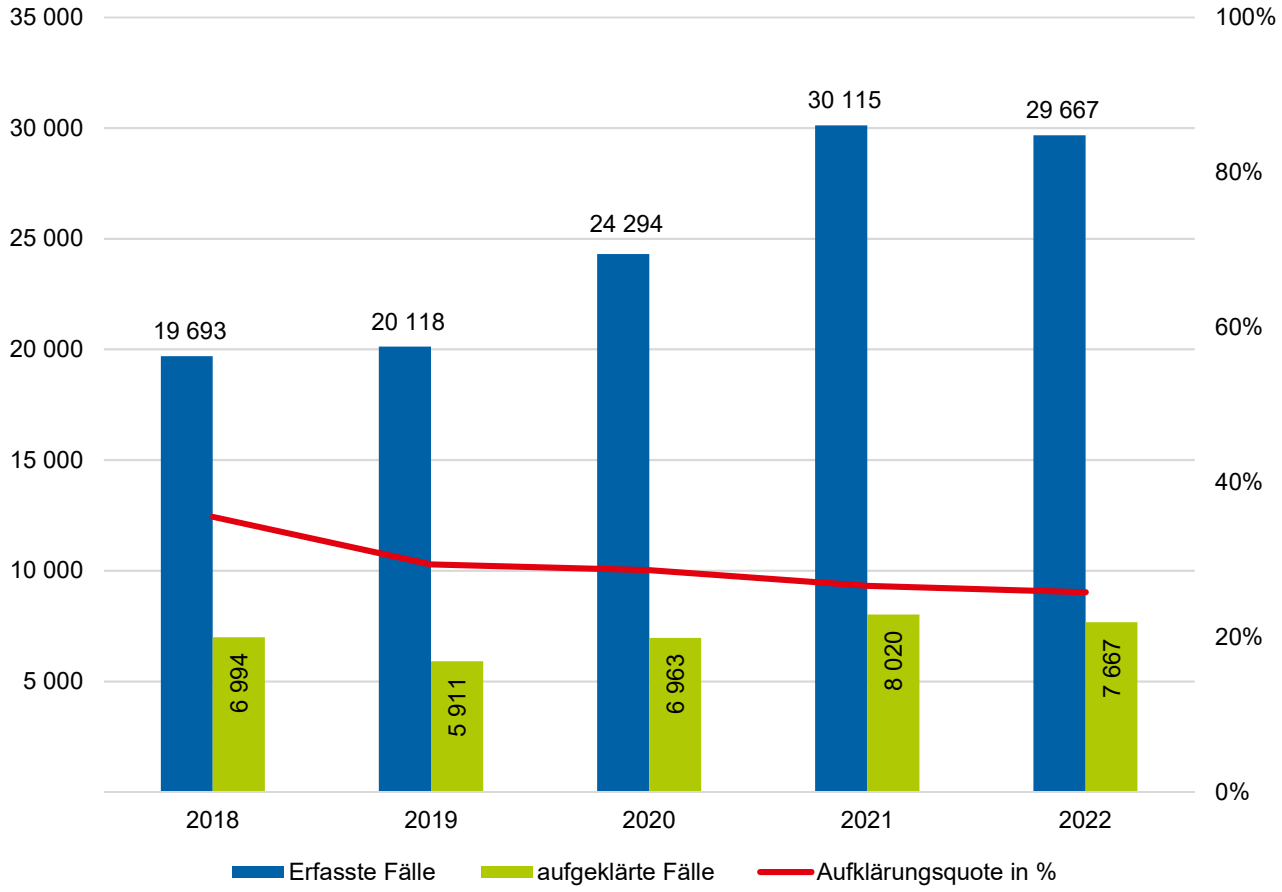
Delikt	2021	2022	Zu-/Abnahme	Veränderung in %
Computerkriminalität (Cybercrime im engeren Sinne)	**30 115**	**29 667**	**- 448**	**- 1,49**
Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei der Datenverarbeitung §§ 269, 270 StGB	4 106	4 129	23	0,56
Datenveränderung, Computersabotage §§ 303a, 303b StGB	1 653	1 194	- 459	- 27,77
Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen und Datenhehlerei §§ 202a, 202b, 202c, 202d StGB	4 752	4 153	- 599	- 12,61
Computerbetrug § 263a StGB	19 604	20 191	587	2,99
Betrügerisches Erlangen von Kfz § 263a StGB	10	13	3	30,00
Weitere Arten des Warenkreditbetruges § 263a StGB	6 888	5 999	- 889	- 12,91
Computerbetrug mittels rechtswidrig erlangter Zahlungskarten mit PIN § 263a StGB	3 356	4 161	805	23,99
Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten § 263a StGB	2 420	2 916	496	20,50
Computerbetrug mittels rechtswidrig erlangter sonstiger unbarer Zahlungsmittel § 263a StGB	1 376	1 831	455	33,07
Leistungskreditbetrug § 263a StGB	1 258	964	- 294	- 23,37
Computerbetrug (sonstiger) § 263a StGB	3 836	3 856	20	0,52
Missbräuchliche Nutzung von Telekommunikationsdiensten § 263a StGB	53	71	18	33,96
Abrechnungsbetrug im Gesundheitswesen § 263a StGB	4	11	7	175,00
Überweisungsbetrug § 263a StGB	403	369	- 34	- 8,44

Quelle: PKS NRW

2.1.2 Aufklärungsquote

Von den im Jahr 2022 erfassten Straftaten der Cybercrime im engeren Sinne wurden 7 667 aufgeklärt. Die Aufklärungsquote sank auf 25,84 Prozent (26,63 Prozent). Im Bereich des Computerbetrugs wurden 5 494 Fälle aufgeklärt. Dies entspricht einer Aufklärungsquote von 27,21 Prozent (29,83 Prozent).

Abbildung 1
Vergleich Fallzahlen und Aufklärungsquote Cybercrime im engeren Sinne



Quelle: PKS NRW

Tabelle 3
Aufklärungsquote (AQ)

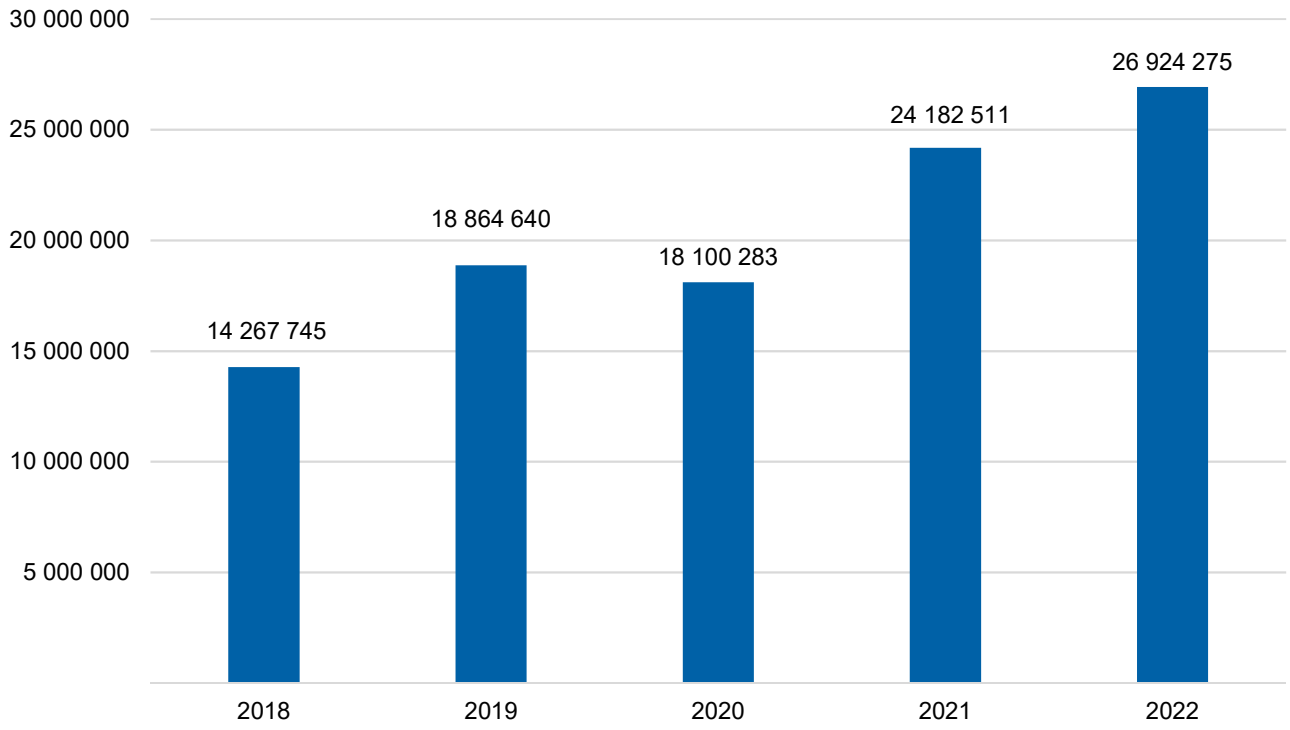
Delikt	Aufgeklärte Fälle		Aufklärungsquote		Zu-/Abnahme (AQ) %-Punkte
	2021	2022	2021	2022	
Computerkriminalität (Cybercrime im engeren Sinne)	**8 020**	**7 667**	**26,63**	**25,84**	**-0,79**
Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei der Datenverarbeitung §§ 269, 270 StGB	1 040	1 247	25,33	30,20	4,87
Datenveränderung, Computersabotage §§ 303a, 303b StGB	269	172	16,27	14,41	-1,86
Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen und Datenhehlerei §§ 202a, 202b, 202c, 202d StGB	864	754	18,18	18,16	-0,02
Computerbetrug § 263a StGB	5 847	5 494	29,83	27,21	-2,62
Betrügerisches Erlangen von Kfz § 263a StGB	6	7	60,00	53,85	-6,15
Weitere Arten des Warenkreditbetruges § 263a StGB	2 789	1 956	40,49	32,61	-7,88
Computerbetrug mittels rechtswidrig erlangter Zahlungskarten mit PIN § 263a StGB	718	814	21,39	19,56	-1,83
Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten § 263a StGB	455	426	18,80	14,61	-4,19
Computerbetrug mittels rechtswidrig erlangter sonstiger unbarer Zahlungsmittel § 263a StGB	315	557	22,89	30,42	7,53
Leistungskreditbetrug § 263a StGB	277	363	22,02	37,66	15,64
Computerbetrug (sonstiger) § 263a StGB	1 038	1 193	27,06	30,94	3,88
Missbräuchliche Nutzung von Telekommunikationsdiensten § 263a StGB	13	13	24,53	18,31	-6,22
Abrechnungsbetrug im Gesundheitswesen § 263a StGB	3	5	75,00	45,45	-29,55
Überweisungsbetrug § 263a StGB	233	160	57,82	43,36	-14,46

Quelle: PKS NRW

2.1.3 Schadensentwicklung

Schäden von Cybercrime werden in der PKS ausschließlich für Computerbetrug und Softwarepiraterie abgebildet. Eine separate statistische Erfassung von Cybercrime-Erpressungsdelikten gibt es nicht. Zudem werden erfolgreiche Erpressungen nur selten zur Anzeige gebracht. Im Jahr 2022 erhöhte sich der Gesamtschaden der Computerkriminalität um 2 741 764 Euro auf 26 924 275 Euro und erreicht somit einen neuen Höchstwert innerhalb der vergangenen fünf Jahre.

Abbildung 2
Schadensentwicklung Cybercrime

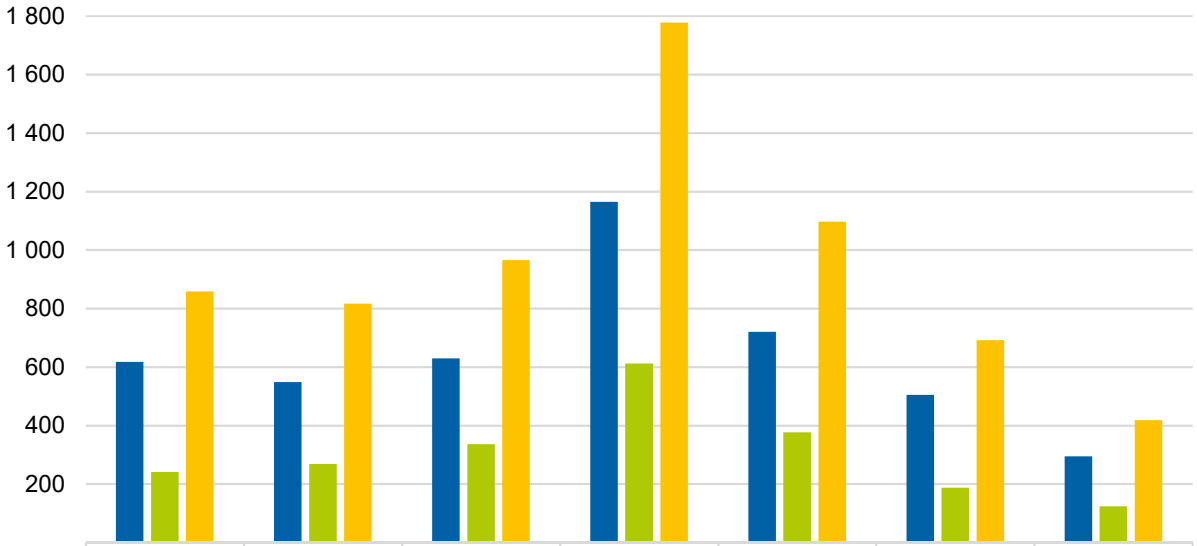


Quelle: PKS NRW

2.1.4 Tatverdächtige

Im Jahr 2022 wurden 6 623 (6 056) Tatverdächtige ermittelt. Die männlichen Tatverdächtigen sind mit 4 478 gegenüber den weiblichen Tatverdächtigen mit 2 145 überrepräsentiert. Den größten Anteil nahm mit 1 777 ermittelten Tatverdächtigen die Gruppe der Erwachsenen im Alter von 30 bis 39 Jahren ein.

Abbildung 3
Tatverdächtige Computerkriminalität nach Alter und Geschlecht



	unter 21	21-25	25-29	30-39	40-49	50-59	ab 60
männlich	617	548	629	1 165	720	505	294
weiblich	241	268	336	612	377	187	124
gesamt	858	816	965	1 777	1 097	692	418

Quelle: PKS NRW

2.2 Einzelne Deliktsfelder

Datenveränderung, Computersabotage

Die Fallzahlen im Deliktsbereich Datenveränderung, Computersabotage §§ 303a, 303b StGB sind im Jahr 2022 auf 1 194 um 27,77 Prozent gesunken. Die Aufklärungsquote im Jahr 2022 betrug 14,41 Prozent (16,27 Prozent).

Ransomware

Ransomware hat sich in den letzten Jahren zu einer der größten Bedrohungen im Bereich der IT-Sicherheit entwickelt. Dabei handelt es sich um Schadsoftware, die die Daten auf infizierten Systemen verschlüsselt. Die Täter fordern Lösegeld von den Opfern, um die Daten wieder freizugeben.

Die Ransomwaregruppierungen Conti und Lockbit 2.0 haben sich im Jahr 2022 in NRW als besonders gefährlich und erfolgreich erwiesen. Die Ziele dieser Gruppierungen sind in erster Linie finanzieller Natur. Mit Ransomware-Angriffen versuchen sie hohe Lösegeldsummen von ihren Opfern zu erpressen. Um der finanziellen Forderung Nachdruck zu verleihen, wird oftmals durch die Gruppierungen gedroht, das Image der betroffenen Unternehmen zu beschädigen, indem sie exfiltrierte Daten veröffentlichen (englisch: leaken). Das allgemeine Vorgehen bei einem Ransomware-Angriff besteht darin, dass die Angreifer zunächst in das Netzwerk ihrer Opfer eindringen und dann die Daten auf dem System verschlüsseln. Oft nutzen sie hierfür

eine sogenannte "Double Extortion"-Taktik. Dabei werden die Daten nicht nur auf dem infizierten System verschlüsselt, sondern auch auf den Servern der Angreifer gespeichert. Die Opfer erhalten nicht nur eine Lösegeldforderung für die Freigabe der Daten auf ihrem System, sondern auch für die Löschung der Datenkopie auf den Servern der Angreifer. Andernfalls drohen die Täter mit der Veröffentlichung auf Leakseiten oder dem Verkauf der Datenkopien.

Bei Lockbit 2.0 handelt es sich um eine Ransomware-as-a-Service-Gruppierung, die eine Vereinigung von Cyberkriminellen darstellt und seit einigen Jahren aktiv ist. Im Jahr 2020 schlossen sie sich mit der bekannteren Cyberkriminellen-Gruppierung Maze zusammen. Lockbit 2.0 setzt unterschiedliche Vorgehensweisen ein, um Netzwerke zu kompromittieren. Dazu gehören unter anderem das Ausnutzen von Sicherheitslücken, der Kauf von Zugängen, die Nutzung von Insider-Wissen sowie die Verwendung von Zero-Day-Exploits. Sobald Lockbit 2.0 in ein Netzwerk eingedrungen ist, nutzen die Drahtzieher frei verfügbare IT-Werkzeuge, um ihre Rechte auszuweiten. Anschließend löscht die Malware wichtige Dateien und sammelt Informationen zum System. Lockbit 2.0 verschlüsselt dann alle lokalen Daten und externe Speichermedien, lässt aber die Kerndateien des Systems unangetastet. Zusätzlich erpressen die Täter die Opfer mit der Veröffentlichung bestimmter Dateitypen, die vor der Verschlüsselung kopiert werden.

Im Januar 2022 wurde ein in NRW ansässiger Finanzdienstleister Opfer von Lockbit 2.0. Alle Firmendaten wurden verschlüsselt und die Täter forderten eine hohe Geldzahlung, um eine Entschlüsselung und Nichtveröffentlichung der Daten zu garantieren. Das Unternehmen konnte jedoch dank vorhandener Backups die Geschäftsfähigkeit aufrechterhalten und musste nicht auf die Forderungen der Täter eingehen.

Lockbit 2.0 hat auch andere Unternehmen aus verschiedenen Branchen verschlüsselt, darunter auch öffentliche Institutionen, wie das französische Justizministerium. Solche Vorfälle zeigen die Bedeutung von regelmäßigen Backups und dem Schutz von Daten durch eine sorgfältige Absicherung der IT-Systeme.

Bei der Gruppierung Conti zeichnete sich im Jahr 2022 eine Aufspaltung in kleinere Einheiten ab, mit dem Ziel, nicht in Gänze angreifbar und somit schwieriger zu fassen zu sein. Diese Entscheidung wurde mutmaßlich durch den Druck der Strafverfolgungsbehörden und den internen Datenabfluss initiiert. Auf das Ergreifen von Mitgliedern wurden mehrere Millionen US-Dollar Kopfgeld ausgelobt. Zudem sorgte ein großer Leak von internen Daten für zusätzlichen Druck auf die Gruppierung.

Im März 2022 kam es durch Conti zu einer Vollverschlüsselung der Server und Back-Up-Server eines Unternehmens in NRW. Das angegriffene Unternehmen hatte Kunden in verschiedenen Branchen, darunter auch Wasser- und Atomkraftwerke in Frankreich. Obwohl ausgelagerte Backups in Form von Band-Sicherungen vorhanden waren, entstand ein nicht unerheblicher Schaden. Die Verschlüsselung ging einher mit einer Ransomnote. Mittlerweile nutzen ehemalige Conti-Mitglieder ihr Know-how und weitreichende Kontakte in andere Gruppierungen, um dezentralisiert vorgehen zu können.

Insgesamt bleibt Ransomware eine der größten Bedrohungen im Bereich der IT-Sicherheit. Unternehmen sollten sich bewusst sein, dass sie jederzeit Ziel eines Angriffs werden können und entsprechende Maßnahmen ergreifen, um ihre Daten und Systeme zu schützen.

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. Die Fallzahlen sind im Berichtsjahr 2022 mit 4 153 Fällen im Vergleich zu 2021 mit 4 752 Fällen um 12,61 Prozent gesunken. Die Aufklärungsquote im Jahr 2022 betrug 18,16 Prozent (18,18 Prozent).

Abfangen von Daten – Phishing

Auch im Jahr 2022 versuchten Täter mittels des sogenannten Phishing („Password“ und „Fishing“) Nutzer dazu zu verleiten, sensible personenbezogene Informationen herauszugeben. Verwendet werden hierzu gefälschte E-Mails, SMS oder Websiten, die dem Nutzer vertäuschen, dass er mit einem seriösen Partner (zum Beispiel seiner Bank oder einem Paketzustelldienst) kommuniziert. Die Täter nutzen zudem Recherchen zum Beispiel in sozialen Netzwerken, um an Informationen über das Opfer zu gelangen, die eine Täuschung glaubwürdiger machen (social engineering). Darüber hinaus bergen Phishing-Mails immer öfter zusätzliche Gefahren durch Datei-Anhänge, die Malware beinhalten. So kann ein unbedachter Klick auf einen Link zu einer Infektion mit einem Schadprogramm führen. Dabei kann es sich unter anderem um einen Trojaner, einen Bot oder Ransomware handeln. Es ist eine zunehmende Professionalisierung der Phishing-Inhalte festzustellen. Tippfehler oder seltsame Umlaute im Text sind selten.

Nach wie vor ist eine der häufigsten Zielrichtungen von Phishing, vor allem einen Zugriff auf (Online-)Bankkonten zu erhalten. Neben den Wellen mit angeblichen Paketzustellungen und vermeintlichen neuen Sprachnachrichten zum Abhören, kommt es seit Mitte 2022 zunehmend häufiger zu betrügerischen SMS, die angeblich von Banken stammen. In diesen wird über angebliche Neuerungen oder Probleme beim Online-Banking hingewiesen und um Aktualisierung von Daten gebeten. Sollten die Geschädigten auf die SMS reagieren und Kontoinformationen preisgeben, folgen meist weitere Schritte, wie ein Telefonanruf, um Zugriff auf das Online-Banking zu erhalten.

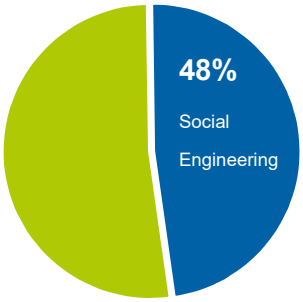
Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten, Zahlungskarten mit PIN und unbarer Zahlungsmittel

Insbesondere im zweiten Halbjahr 2022 trat vermehrt das Phänomen **„Digitale Zahlungskarte“** auf. Bei diesem Phänomen handelt es sich um eine Betrugsvariante mittels rechtswidrig erlangter Zahlungskarteninformation, welche zum Anstieg in den Fallzahlen im Deliktbereich Computerbetrug § 263a StGB beigetragen hat. Bankkunden haben die Möglichkeit ihre Zahlungskartendaten mit einer Pay-App in ihrem Smartphone oder ihrer Smartwatch als digitale Zahlungskarte zu hinterlegen. Das entsprechende Gerät muss dafür die Funktion NFC (Near Field Communication) besitzen und sollte ein aktuelles Betriebssystem aufweisen. Mittlerweile existieren einige Pay-Apps auf dem Markt. Zu den bekanntesten Pay-Apps gehört für Android-Nutzer „Google Pay“ und für iOS-Nutzer „Apple Pay“. Die Art der Kartenhinterlegung und Verifizierungsmethode liegt in der Hand der Bank oder des Kreditinstituts, das die Karte herausgibt. Entweder kann die Zahlungskarte direkt mit der Kartennummer und einem anschließenden Verifizierungscode hinterlegt werden oder über das Online-Banking beziehungsweise die Online-Banking-App des Kunden mittels TAN verifiziert und hinzugefügt werden. Meist gelangen Täter, wie oben beschrieben, an die Kontodaten und weitere vertrauliche Informationen mittels Phishing-Link per E-Mail oder SMS. Dieser führt auf eine gefälschte Webseite, welche den Anschein erweckt von der Hausbank zu stammen. Täter können darüber hinaus zum Erwerb der Daten auch illegale Bezugsquellen, wie kriminelle Marktplätze im Darknet, nutzen. Mit diesen Informationen geben sich die Täter telefonisch als angeblicher Bankmitarbeiter aus. Die Opfer werden mittels Social Engineering dazu gebracht, einen Push-TAN zu bestätigen oder einen Verifizierungscode zu übermitteln, welchen diese während des Gespräches erhalten. Wenn dies ausgeführt wird, kann die jeweilige Karte sofort auf dem Täterhandy freigeschaltet werden. Im Anschluss können die Täter das eigene Smartphone mit der fremden digitalen Karte beim Bezahlen einsetzen, ohne die physische Debit- oder Kreditkarte mit PIN zu besitzen. Die Verwertung einer digitalen Zahlungskarte kann durchaus von verschiedenen Tätern an verschiedenen Örtlichkeiten gemeinsam erfolgen. Dabei entstehen teilweise hohe Schadenssummen.

Im Deliktsbereich Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten § 263a StGB sind die Fallzahlen in 2022 um 20,50 Prozent zu 2021 gestiegen (Zunahme von 496 Fällen). Ebenfalls kommt es zu einem Anstieg im Bereich Computerbetrug mittels rechtswidrig erlangter, sonstiger unbarer Zahlungsmittel gemäß § 263a StGB von 33,07 Prozent (Zunahme von 455 Fällen) gegenüber 2021. Die Fallzahlen im Deliktsbereich „Computerbetrug mittels rechtswidrig erlangter Zahlungskarten mit PIN“ sind im Jahr 2022 um 23,99 Prozent (Zunahme von 805 Fällen) gestiegen. Die Aufklärungsquote im Jahr 2022 betrug 19,56 Prozent (21,39) Prozent. Die Fallzahlen dieser Delikte enthalten nicht nur Fallzahlen des Phänomens „Digitale Zahlungskarte“, sondern auch die Einsätze gestohlener oder unterschlagener physischer Zahlungskarten.

Social Engineering

Nach einer durch Bitcom e. V. beauftragten Studie haben 48 Prozent der im Jahr 2022 befragten Unternehmen Versuche von Social Engineering erlebt. In den Jahren 2021 und 2022 wurden Telefon, E-Mail und privates Umfeld als die drei häufigsten Bereiche genannt, über die Firmenmitarbeiter durch Social Engineering beeinflusst werden sollten. Bei jeweils mehr als einem Drittel der befragten Firmen waren Telefon und E-Mail die beiden häufigsten Einfallsvektoren.[3] Eine konstruktive Fehlerkultur in Unternehmen und Behörden kann Schäden verhindern. Mitarbeitende müssen Fehlverhalten zugeben können und dürfen. Angriffe auf Nutzer werden oft erst als Angriffe erkannt, wenn der Schaden ersichtlich wird. In E-Mails, Messenger-Nachrichten und Telefonaten wird die Hilfsbereitschaft, das Vertrauen, die Loyalität oder die Angst der Opfer ausgenutzt. Das Vortäuschen der Firmenzugehörigkeit, das „Vergessen“ von Zugangscode/Passwort, eine passende Legende aus Peinlichkeiten, warum man unmöglich noch einmal bei der IT anrufen kann, und das Appellieren an die Hilfsbereitschaft werden zum Schlüssel für Täter. Vermeintliche Gemeinsamkeiten über zuvor ausspionierte Tatsachen, wie eigene Kinder, Haustiere oder die Herkunft werden in dem Gespräch vorgespielt und so auch noch die „Schlüssel“ Loyalität und Vertrauen aktiviert. Der „Schlüssel“ Angst öffnet die Türen über die Varianten „Geldverlust“ und „Jobverlust“, für viele gleichbedeutend mit Existenzverlust. Wenn der angebliche Bankmitarbeiter anruft und mitteilt, dass im Online-Banking eine Überweisung über mehrere Tausend Euro ins Ausland angewiesen wurde, lässt die plötzliche Angst vor hohem Geldverlust kritische Gedanken und Fragen nach der Echtheit des Anrufers und der Information ausblenden. Der sich als Bankmitarbeiter ausgebende Täter vermittelt glaubhaft, eine TAN des Opfers zu benötigen, um die Überweisung aufzuhalten. Die Opfer werden massiv unter Druck gesetzt. Hinweise der Banken, „Mitarbeiter werden sie niemals nach ihrem Passwort oder einer TAN fragen“, und Sicherheitsmechanismen im Online-Banking werden ausgeblendet, das kritische Hinterfragen der Situation oder Identität des Anrufers bleibt aus.



Bei der Variante „Jobverlust“ sind ebenfalls Anrufer und Legende erfunden. Eine bestimmte Handlung soll von Angestellten vorgenommen werden (Überweisung, Passwortherausgabe et cetera). Wenn nicht, droht der Jobverlust. Der seitens der Täter erzeugte Stress lässt die Opfer kritische Fragen ausblenden.

Durch die Mithilfe der Opfer und Preisgabe von Passwort, PIN, TAN et cetera sind IT-Sicherheit, Firewalls und Virenschutz wirkungslos und Sicherheitshürden werden ausgehebelt. Social Engineering Angriffe können auch analog, physisch vor Ort stattfinden. Täter verschaffen sich durch zwischenmenschliche Beeinflussungen Zugang zu Firmengebäuden, indem ihnen mit geschickter Manipulation Berechtigte den Zugang gewähren. Bis in einzelne Büros eingedrungen, können Rechner bedient, Unterlagen kopiert oder gestohlen und die IT-Sicherheit oder Infrastruktur sabotiert werden. Aber auch Geschenke von vermeintlichen Geschäftspartnern oder Referenten können Schadsoftware ins Unternehmen bringen. Wer hat noch nicht bei Terminen oder Konferenzen einen USB-Stick „geschenkt“ bekommen?

[3] Bitkom e.V. (Hrsg.), Bitkom Research 2022.

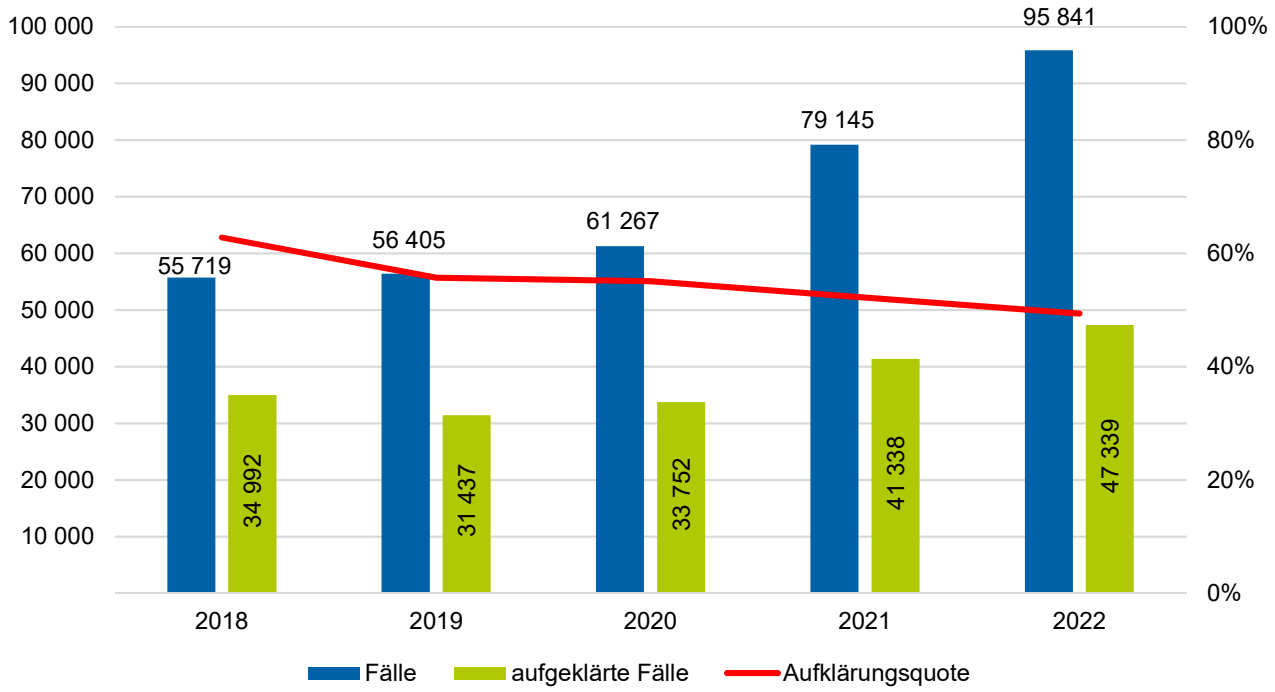
3 Lagedarstellung Cybercrime im weiteren Sinne

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 (sogenannte Äußerungs- beziehungsweise 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. 2022 wurden 95 841 Fälle mit dem Tatmittel Internet erfasst, 16 696 mehr als 2021. Den größten Anteil nahmen hierbei Betrugsdelikte mit 60 557 Fällen ein. Bei einer Aufklärungsquote von 49,39 Prozent wurden 47 339 Straftaten mit „Tatmittel Internet“ aufgeklärt.

Abbildung 4
Straftaten mit Tatmittel Internet (Cybercrime im weiteren Sinne)



Quelle: PKS NRW

Tabelle 4
Straftaten mit Tatmittel Internet

	Gesamt	davon mit Tatmittel Internet	
	Fälle	Fälle	Anteil in %
Alle Straftaten	**1 366 601**	**95 841**	**7,01**
Straftaten gegen die sexuelle Selbstbestimmung	31 520	15 098	47,90
Verbreitung pornografischer Inhalte (Erzeugnisse) gem. §§ 184, 184a, 184b, 184c, 184d, 184e StGB	14 440	14 142	97,94
Verbreitung, Erwerb, Besitz und Herstellung kinderpornographischer Inhalte gemäß § 184b StGB	11 183	10 977	98,16
Verbreitung von Kinderpornographie gemäß § 184b Abs. 1 Nr. 1	5 124	5 059	98,73
Betrug §§ 263, 263a, 264, 264a, 265, 265a, 265b StGB	200 424	60 577	30,22
Waren- und Warenkreditbetrug	76 687	34 262	44,68
Computerbetrug (sonstiger) §263a StGB	3 856	2 673	69,32
Betrügerisches Erlangen von Kfz § 263a StGB	13	4	30,77
Weitere Arten des Warenkreditbetruges § 263a StGB	5 999	4 604	76,75
Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten § 263a StGB	2 916	1 534	52,61
Computerbetrug mittels rechtswidrig erlangter sonstiger unbarer Zahlungsmittel § 263a StGB	1 831	1 038	56,69
Leistungskreditbetrug § 263a StGB	964	660	68,46
Überweisungsbetrug § 263a StGB	369	206	55,83
Missbräuchliche Nutzung von Telekommunikationsdiensten § 263a StGB	71	44	61,97
Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung §§ 269, 270 StGB	4 129	2 901	70,26
Datenveränderung, Computersabotage §§ 303a, 303b StGB	1 194	1 003	84,00
Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen und Datenhehlerei §§ 202a, 202b, 202c, 202d StGB	4 153	4 078	98,19
Erpressung § 253 StGB	3 601	1 690	46,93

Quelle: PKS NRW

Hinweis: Die Steigerung der Fallzahlen mit Tatmittel Internet in den Bereichen der Kinderpornographie und des Ausspähens von Daten sind auf die in 2022 durchgeführten Qualitätssicherungsmaßnahmen in diesen Bereichen zurückzuführen. Unterjährig durchgeführte Prüfungen auf Fälle, bei denen das Tatmittel Internet nicht gesetzt wurde, führten zu umfangreichen Korrekturen und einer verbesserten Lagedarstellung in den oben genannten Bereichen.

Tabelle 5
Entwicklung der Straftaten mit Tatmittel Internet

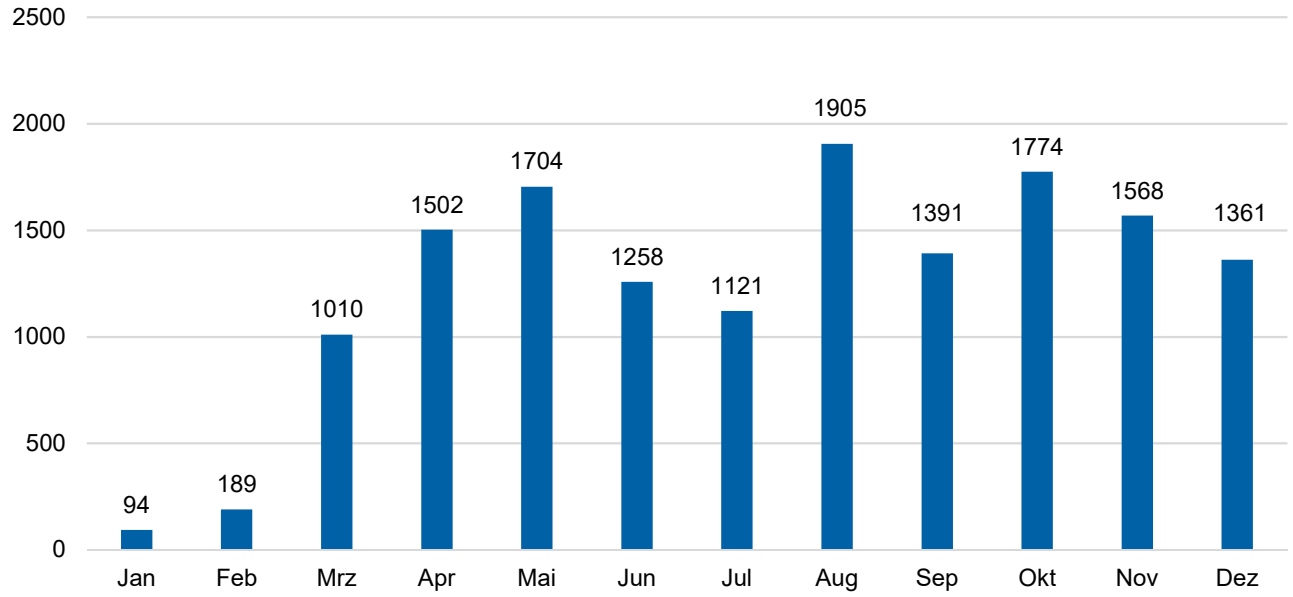
	2021	2022	Zu-/Abnahme	Veränderung in %
Straftaten mit Tatmittel Internet	**79 145**	**95 841**	16 696	21,10
Straftaten gegen die sexuelle Selbstbestimmung	11 056	15 098	4 042	36,56
Verbreitung pornografischer Inhalte (Erzeugnisse) gem. §§ 184, 184a, 184b, 184c, 184d, 184e StGB	9 828	14 142	4 314	43,89
Verbreitung, Erwerb, Besitz und Herstellung kinderpornographischer Inhalte gemäß § 184b StGB	8 133	10 977	2 844	34,97
Verbreitung von Kinderpornographie gemäß § 184b Abs. 1 Nr. 1	3 714	5 059	1 345	36,21
Betrug §§ 263, 263a, 264, 264a, 265, 265a, 265b StGB	51 839	60 577	8 738	16,86
Waren- und Warenkreditbetrug	35 124	34 262	- 862	- 2,45
Computerbetrug (sonstiger) §263a StGB	2 397	2 673	276	11,51
Betrügerisches Erlangen von Kfz § 263a StGB	5	4	- 1	- 20,00
Weitere Arten des Warenkreditbetruges § 263a StGB	4 608	4 604	- 4	- 0,09
Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten § 263a StGB	1 151	1 534	383	33,28
Computerbetrug mittels rechtswidrig erlangter sonstiger unbarer Zahlungsmittel § 263a StGB	637	1 038	401	62,95
Leistungskreditbetrug § 263a StGB	577	660	83	14,38
Überweisungsbetrug § 263a StGB	229	206	- 23	- 10,04
Missbräuchliche Nutzung von Telekommunikationsdiensten § 263a StGB	15	44	29	193,33
Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung §§ 269, 270 StGB	2 760	2 901	141	5,11
Datenveränderung, Computersabotage §§ 303a, 303b StGB	1 161	1 003	- 158	- 13,61
Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen und Datenhehlerei §§ 202a, 202b, 202c, 202d StGB	3 100	4 078	978	31,55
Erpressung § 253 StGB	1 573	1 690	117	7,44

Quelle: PKS NRW

3.2 Messenger-Betrug

Im ersten Halbjahr 2022 verzeichnete die Polizei NRW einen deutlichen Anstieg der Fallzahlen im Bereich Messenger-Betrug, welcher zu diesem Zeitpunkt noch als „WhatsApp-Betrug“ bezeichnet wurde. Im Januar 2022 lagen die im Rahmen der kriminalstrategischen Auswertung festgestellten Fallzahlen bei 94 Fällen und im Februar bei 189 Fällen. Ab dem Monat März 2022 konnten bis zum Jahresende 2022 durchgängig Fallzahlen im vierstelligen Bereich festgestellt werden. Sie unterlagen teils größeren Schwankungen und sanken im letzten Quartal stetig ab. Die für das Jahr 2022 erkannten Fallzahlen stellen sich wie folgt dar:

Abbildung 5
Fallzahlen Betrug mittels Messengerdiensten



Quelle: Vorgangsbearbeitungssystem der Polizei NRW

Zur Absprache effektiver Präventionsmaßnahmen zur Bekämpfung dieses Deliktfeldes erfolgte zeitnah ein Austausch mit Vertreterinnen und Vertretern der Kreditwirtschaft sowie dem Landeskriminalamt Berlin und dem Geschäftsführer der Polizeilichen Kriminalprävention der Länder und des Bundes (ProPK). Die vorliegende Thematik wurde als Tagesordnungspunkt in die 88. Arbeitstagung der Kommission Polizeiliche Kriminalprävention (KPK) am 6. und 7. Oktober 2022 in Hannover mit Beschlussvorschlag (Gründung einer KPK - Projektgruppe mit dem Ziel, das Phänomen bundeseinheitlich präventiv zu bekämpfen) eingebracht. In der vorgenannten Arbeitstagung wurde die Bund-Länder-Projektgruppe (BLPG) „Mediensicherheit“ (unter Beteiligung von NRW) damit beauftragt, ein Maßnahmenpaket zu dieser Betrugsvariante zu erstellen. Auf der in der 42. KW 2022 erfolgten Fachtagung der BLPG wurde zunächst beschlossen, aus Neutralitätsgründen künftig bei dieser Betrugsvariante von „Messenger-Betrug“ zu sprechen. Eine seitens der BLPG entworfene Konzeption, welche eine Bündelung verschiedener Maßnahmen vorsieht, befindet sich in der Fertigstellung. Zur erfolgreichen Bekämpfung des Phänomens gehört die Minimierung/Verhinderung der Schadenssummen. Neben dem Schutz der Opfer werden die Täter hierdurch empfindlich in ihrer Tatausführung und dem Erlangen der Beute gestört. Dies kann unter anderem dadurch erreicht werden, dass die Geldinstitute so früh wie möglich über erfolgte Geldtransaktionen informiert werden und durch frühzeitiges Agieren eine Rückholung des Geldes erfolgt.

3.3 Kinderpornografie

2022 wurden für den Deliktsbereich „Verbreitung, Erwerb, Besitz und Herstellung kinderpornographischer Inhalte“ gemäß § 184b StGB 11 183 (11 328) Fälle erfasst. Dies entspricht einer Abnahme von 1,28 Prozent. Die Fallzahlen bleiben damit auf einem konstant sehr hohen Niveau. Im Jahr 2021 hatten sich die Fallzahlen gegenüber dem Vorjahr mehr als verdoppelt (Steigerung um 137,19 Prozent). Die Aufklärungsquote lag im Jahr 2022 mit 9 434 aufgeklärten Fällen bei 84,36 Prozent und sank damit im Vergleich zum Vorjahr (90,46 Prozent).

Mit einer Anzahl von 10 977 Fällen (98,16 Prozent) nimmt das Internet als Tatmittel für den Deliktsbereich der Kinderpornografie eine herausragende Bedeutung ein. Von den erfassten Fällen konnten 9 219 Taten und somit 83,98 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. Die Anzahl der in Nordrhein-Westfalen eingehenden Hinweise hat sich im Jahr 2022 im Vergleich zum Vorjahr um 2,5 Prozent gesteigert. Dies ist einerseits noch immer Ausläufer der im Jahre 2020 vorgenommenen Verfahrensumstellung beim Bundeskriminalamt und der Justiz, andererseits auf eine deutliche Steigerung der Meldungen des NCMEC insgesamt zurückzuführen. Nicht zuletzt ist aber auch die seit dem 01.07.2021 in Kraft getretende Strafrechtsverschärfung und damit einhergehender Einstufung als Verbrechenstatbestand mitursächlich. Nach Prüfung der strafrechtlichen Relevanz und erfolgversprechender Ermittlungsansätze durch das Bundeskriminalamt wurden dem LKA NRW im Jahr 2022 16 736 (6 668) Verdachtsfälle bekannt. Diese werden nach Erstbearbeitung durch das LKA NRW über die Zentral- und Ansprechstelle Cybercrime der Staatsanwaltschaft Köln den nordrhein-westfälischen Kreispolizeibehörden (KPB) zu weiteren Ermittlungen zugeleitet.

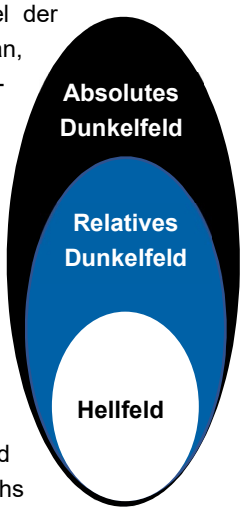
Die Zahl der Tatverdächtigen aus Nordrhein-Westfalen in bundesweiten Umfangsverfahren sank von 1 774 im Jahr 2021 auf 591.

Mit 1 546 Tatverdächtigen unter 14 Jahren (1 191) und 2 718 Tatverdächtigen zwischen 14 und 18 Jahren (2 773) stieg die Anzahl Tatverdächtiger in diesen beiden Altersgruppen im Vergleich zum Vorjahr deutlich an. Somit handelt es sich bei 54,60 Prozent (38,74 Prozent) aller bekannten Tatverdächtigen um Kinder und Jugendliche.

Seit Sommer 2021 gibt es im In- und Ausland eine unbekannte Anzahl von Fällen, bei denen Facebook-Accounts gehackt und anschließend inkriminierte Bilder oder Videos hochgeladen wurden. Dies führte zur Sperrung der betroffenen Accounts und zur Erstellung eines NCMEC-Reports. Sofern Betroffene das Hacken ihrer Accounts nicht zur Anzeige brachten und die Ermittlungsbehörden auch nicht auf anderem Wege Kenntnis von der Manipulation erhielten, richteten sich die Strafverfahren und die damit verbundenen strafprozessualen Maßnahmen folglich gegen die regulären Accountinhaber. Hintergründe und Absichten dieser Hacking Angriffe sind bisher nicht bekannt. Forderungen oder einen finanziellen Schaden gab es in diesem Zusammenhang in sehr seltenen Fällen. Unter Federführung von EUROPOL werden Erfahrungen und Erkenntnisse zu dem Phänomen ausgetauscht und Präventionsmöglichkeiten mit Facebook und dem NCMEC erörtert. Das LKA NRW sammelt alle Hinweise zum Erkennen entsprechender Indizien in den NCMEC-Meldungen.

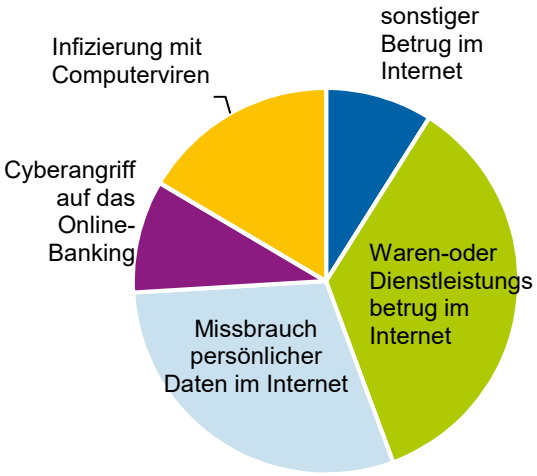
4 Dunkelfeld

Das Hellfeld umfasst die den Strafverfolgungsbehörden bekannt gewordene Kriminalität, abgebildet in der PKS. Das Dunkelfeld ist die „[…] Summe jener Delikte, die den Strafverfolgungsbehörden nicht bekannt werden und deshalb in der Kriminalstatistik auch gar nicht erscheinen. Nicht bekannt werden vor allem solche Straftaten, die von den Opfern oder anderen nicht angezeigt werden […].“[4] Gründe für das Nichtanzeigen eines Cyberangriffs auf Unternehmen zeigen Ergebnisse einer repräsentativen Unternehmensbefragung in den Jahren 2018/2019. Danach gaben knapp drei Viertel der befragten Unternehmen als Grund die fehlende Aussicht auf Ermittlungserfolg, und etwa ein Fünftel an, nicht zu wissen, an wen man sich wenden muss. Rund elf Prozent der befragten Unternehmen befürchteten Arbeitsbehinderungen durch eine Anzeige und fünf Prozent, dass Behörden Einsicht in vertrauliche Daten fordern könnten. Drei Prozent befürchteten einen Imageschaden durch eine Anzeige.[5]



Für den Bereich Cybercrime zum Nachteil von Unternehmen waren laut einer jährlichen Befragung von Unternehmen im Jahr 2022 84 Prozent in den letzten zwölf Monaten von Diebstahl, Industriespionage oder Sabotage betroffen. Ebenfalls 84 Prozent der Unternehmen gaben an, dass die Anzahl der Cyberattacken in diesem Zeitraum eher oder stark zugenommen hat. Die Arten von Cyberangriffen waren bei einem Viertel der befragten Unternehmen Angriffe auf Passwörter, Phishing und die Infizierung mit Schadsoftware beziehungsweise Malware. Schäden durch DDoS- und Ransomware-Angriffe wurden bei jeweils sechs Prozent weniger Unternehmen als im Vorjahr verursacht. Für den Bereich Cybercrime zum Nachteil von Bürgerinnen und Bürgern liefern Befragungen im Jahr 2020 der Studie „Sicherheit und Kriminalität in Deutschland“ der Kriminalistisch- Kriminologischen Forschungsstelle NRW Ergebnisse.[6] Danach wurden in den letzten zwölf Monaten vor der Befragung 1,9 Prozent der Befragten Opfer von sonstigem Betrug im Internet. 7,5 Prozent der Befragten gaben an, in den der Befragung vorausgegangenen zwölf Monaten Opfer von Waren- oder Dienstleistungsbetrug geworden zu sein, 1,9 Prozent berichteten von Erfahrungen mit sonstigem Betrug im Internet. Von 6,3 Prozent der Befragten wurden die persönlichen Daten missbraucht, bei 2,0 Prozent erfolgte ein Cyberangriff auf das Online-Banking, und die Infizierung mit Computerviren erfolgte bei 3,5 Prozent.

In den letzten 12 Monaten vor Befragung Opfer geworden von…



4 Schwind, Hans-Dieter: Kriminologie, 2011, 38.
5 Dreißigacker, Arne/von Skarczinski, Bennet/Wollinger, Gina Rosa: Forschungsbericht Nr. 152, Cyberangriffe gegen Unternehmen, 2020, 150.
6 Landeskriminalamt NRW (2022): Sicherheit und Kriminalität in Deutschland 2020. Erste Ergebnisse für Nordrhein-Westfalen. https://polizei.nrw/sites/default/files/2022-11/SKiD%202020%20-%20Erste%20Ergebnisse%20f%C3%BCr%20Nordrhein-Westfalen.pdf.

5 Prävention

Die Prävention von Cybercrime obliegt in Nordrhein-Westfalen grundsätzlich den KPB. Das LKA NRW unterstützt die KPB insbesondere durch das Fortschreiben von Standards und das Entwickeln von Medien sowie durch die Initiierung und Koordination von überregionalen Präventionsmaßnahmen.

Bei der Prävention von Cybercrime wird zwischen Cybercrime im weiteren Sinne und Cybercrime im engeren Sinne unterschieden. Während die Prävention von Cybercrime im weiteren Sinne den KPB obliegt, nimmt das LKA NRW mit dem Cybercrime-Kompetenzzentrum die Prävention von Cybercrime im engeren Sinne wahr. Adressaten sind 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. Die Präventionsarbeit des LKA NRW umfasste auch im Jahr 2022 Präventionskampagnen, Veranstaltungen und Vorträge zur Sensibilisierung im Bereich Cybercrime, sowie Networking im Rahmen von Sicherheitspartnerschaften. Das LKA NRW entwickelte bereits 2021 die breit angelegte Kampagne **www.mach-dein-passwort-stark.de** zum Passwortschutz. Die Kooperationspartner Verbraucherzentrale NRW, eco-Verband der Internetwirtschaft e. V. und Bundesverband Verbraucherinitiative e. V. sind darin 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. Die Präventionskampagne lief auch im Jahr 2022 durchgehend und wird weiter fortgeschrieben.

Im Bereich der Cybercrime im engeren Sinne ist das LKA NRW in Kooperationen mit unterschiedlichsten Partnern wie dem Bitkom und dem Voice - Bundesverband der IT-Anwender e. V. Darüber hinaus besteht eine Sicherheitspartnerschaft mit der Allianz für Sicherheit in der Wirtschaft West NRW. Seit 2017 besteht eine gleichgelagerte Kooperationsvereinbarung mit dem eco-Verband der Internetwirtschaft e. V. und dem Networker NRW e. V. Ziel dieser Kooperationen ist die Sensibilisierung kleiner und mittelständischer Unternehmen für die durch Cybercrime bestehenden Gefahren und die Erhöhung der Anzeigebereitschaft. 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.

Im Rahmen der bestehenden Sicherheitskooperation hat das Landeskriminalamt NRW auch 2022 wieder an den jährlich stattfindenden Fachmessen teilgenommen, unter anderem als Aussteller bei der General Police Equipment Exhibition & Conference Messe (GPEC) in Frankfurt und bei der Internet Security Messe (it-sa) in Nürnberg.

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, EKHK
Telefon: +49 211 939-4110
Fax: +49 211 939-194110

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

Bildnachweis: © Adobe Stock Polizei NRW