POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

bürgerorientiert · professionell · rechtsstaatlich

Cybercrime
Lagebild LKA NRW 2023

GEMEINSAM
EINEN SCHRITT VORAUS
Vielfältig. Zukunftsweisend. Vernetzt.

Cybercrime 2023 im Überblick

57 973 Straftaten
Cybercrime im engeren Sinne

91 479 Straftaten
mit Tatmittel Internet

7 062
ermittelte Tatverdächtige (Inland)

16,38 %
Aufklärungsquote (Inland)

1 536
ermittelte Tatverdächtige (Ausland)

3,72 %
Aufklärungsquote (Ausland)

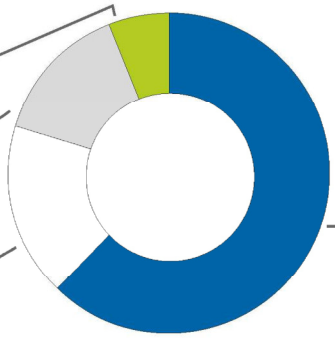
81 001 778 Euro Schaden, davon 24 001 664 Euro in einem Verfahren

Häufigste Delikte

Datenveränderung, Computersabotage
5,97 %

Ausspähen von Daten
17,53 %

Fälschung beweiserheblicher Daten
14,23 %

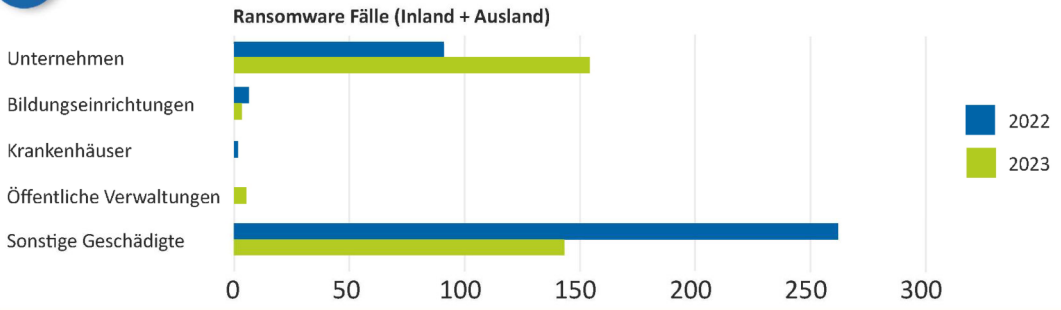


Dominierendes Delikt

Computerbetrug
36 103 (+21,17 %)

Computerbetrug
62,28 %

Ransomware



Kinderpornografie

10 728 Straftaten (-455 Fälle)
Verbreitung, Erwerb, Besitz und Herstellung „kinderpornographischer Inhalte“ gemäß § 184b StGB

84,83 % Aufklärungsquote

davon 9 519 Straftaten mit Tatmittel Internet

41,80 % der Tatverdächtigen sind Kinder und Jugendliche

Inhaltsverzeichnis

Vorbemerkung		5
1	**Lagedarstellung Cybercrime im engeren Sinne**	**7**
1.1	Entwicklung der Fallzahlen	7
1.1.1	Auslandsstraftaten	7
1.1.2	Fallzahlen Cybercrime im engeren Sinne	7
1.1.3	Aufklärungsquote	11
1.1.4	Schadensentwicklung	12
1.1.5	Tatverdächtige	13
1.2	Darstellung ausgewählter Phänomenbereiche	14
2	**Lagedarstellung Straftaten mit Tatmittel Internet**	**17**
2.1	Darstellung ausgewählter Phänomenbereiche	20
2.1.1	Immobilienbetrug	20
2.1.2	Fake-Shops	20
2.2	Kinderpornographie	21
3	**Dunkelfeld**	**21**
4	**Interventionsteams Digitale Tatorte**	**22**
5	**Prävention**	**23**
5.1	Zuständigkeiten und Geltungsbereich	23
5.2	Rückblick in ausgewählten Bereichen	23
5.2.1	Landeskampagne „Mach-Dein-Passwort-stark“	24
5.2.2	Messenger-Betrug	24
5.2.3	Kooperationen und Prävention im Bereich Wirtschaft und Unternehmen	24

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 und es sich um eine Tat handelt, die auch in der analogen Welt begangen werden könnte, wie etwa Drogenhandel oder Betrugsdelikte gemäß §263 StGB.

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 bzw. nicht zur Anzeige gebracht werden.

Auswirkung staatlicher Akteure auf die Cybersicherheitslage

Cyberangriffe haben sich bei ausländischen Nachrichtendiensten als Einsatzmittel etabliert. Insbesondere autokratische Staaten verfügen inzwischen über hochqualifizierte Hackergruppierungen, die nachrichtendienstliche Operationen im Cyber- und Informationsraum durchführen. Klassische Handlungsfelder sind politische, wirtschaftliche und militärische Spionage, Einflussnahme und Desinformation. Darüber hinaus werden digitale Möglichkeiten genutzt, Oppositionelle und Dissidenten auszuspionieren und einzuschüchtern.

Exemplarisch sei in diesem Zusammenhang auf die Veröffentlichung der US-Administration im Rahmen der Münchner Sicherheitskonferenz 2024 hingewiesen, wonach die Gruppierung APT28 des russischen militärischen Auslandsnachrichtendienstes GRU kompromittierte Ubiquiti-Router für die Vorbereitung von Cyberangriffen genutzt hat. Solche Gruppierungen werden staatlich finanziert und haben Zugang zu erheblichen Ressourcen und Informationen. In der Regel versuchen die Gruppierungen, unbemerkt in Netzwerke einzudringen und dort zu verbleiben. Ihre Ziele sind das Sammeln von Informationen oder die Störung von Betriebsabläufen. Dabei nutzen sie fortgeschrittene Angriffsmethoden. Angriffe staatlich gesteuerter Hackergruppierungen werden deshalb oft als Advanced Persistent Threat (APT) bezeichnet.

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

Gerade im Kontext des Russland-Ukraine- sowie des Nahostkonfliktes treten verstärkt politisch motivierte Cyberakteure, sog. Hacktivisten, in Erscheinung. Hacktivismus ist eine Form des Aktivismus, die sich der Computertechnologie bedient, um politische oder soziale Ziele zu propagieren. Hacktivisten nutzen häufig illegale Methoden wie das Hacken von Webseiten, das Durchführen von Distributed Denial of Service (DDoS) - Angriffen oder das Veröffentlichen vertraulicher Daten. Immer wieder besteht der Verdacht, dass ausländische Staaten den Deckmantel des Hacktivismus nutzen, um eigene Cyberangriffe und Hack- and Leak-Operationen unter falscher Flagge durchzuführen.

Eine Attribution dieser Angriffe zu einem bestimmten Staat wird jedoch in der Regel durch den Einsatz anonymisierender Dienste wie Virtual Private Networks (VPN) erschwert. Cybercrime-Gruppierungen sind äußerst versiert darin ihre Aktivität in der digitalen Welt zu verschleiern. Sie nutzen Server über verschiedene Länder und Kontinente hinweg, um geografische Spuren zu manipulieren, sodass der polizeiliche Nachweis einer staatlichen Steuerung politisch motivierter Cybercrime nur in seltenen Fällen zu führen ist.

1 Lagedarstellung Cybercrime im engeren Sinne

1.1 Entwicklung der Fallzahlen

1.1.1 Auslandsstraftaten

In der PKS NRW werden ausschließlich Straftaten erfasst, bei denen der Handlungsort nachweislich in Deutschland liegt. Durch die weltweite Vernetzung ist es möglich, dass der Ort an dem der bzw. die Täter handelten nicht mit dem Erfolgsort, dort wo das schädigende Ereignis sich verwirklicht, identisch ist. In vielen Fällen liegt der Ort der Handlung im Ausland oder ist nicht festzustellen. Liegt in diesen Fällen einer der Erfolgsorte in Deutschland, handelt es sich um eine in der erweiterten PKS NRW zu erfassenden Auslandsstraftat. Auslandsstraftaten sind u. a. zunehmend bei den Straftaten im Bereich des Cybercrime festzustellen. Um dieser Entwicklung Rechnung zu tragen, wurde erstmalig im Jahr 2022 mit der statistischen Erfassung der Auslandsstraftaten im Bereich der Cybercrime im engeren Sinne begonnen.

Um einen annähernden Vergleich zum Vorjahr zu ermöglichen, werden erstmalig in diesem Lagebild die Fallzahlen der PKS NRW und der Auslandsstraftaten des Jahres 2023 gemeinsam im Vergleich zu den entsprechenden Fallzahlen des Vorjahres dargestellt.

1.1.2 Fallzahlen Cybercrime im engeren Sinne

Im Jahr 2023 wurden 21 181 (29 667) inländische Fälle von Cybercrime im engeren Sinne erfasst (Inland). Die Anzahl der Auslandsstraftaten stieg im gleichen Zeitraum von 21 941 im Jahr 2022 auf 36 792 Fälle. Somit stieg die Gesamtzahl der in NRW erfassten Fälle von Cybercrime im engeren Sinne von 51 608 im Jahr 2022 auf 57 973 im Jahr 2023. Die häufigsten Delikte waren der Computerbetrug gemäß § 263a StGB, das Ausspähen von Daten gemäß § 202a StGB und Fälschung beweiserheblicher Daten gemäß § 269 StGB. Den größten Anstieg der Fallzahl gab es im Bereich des Computerbetruges mittels rechtswidrig erlangter Daten von Zahlungskarten gemäß § 263a StGB.

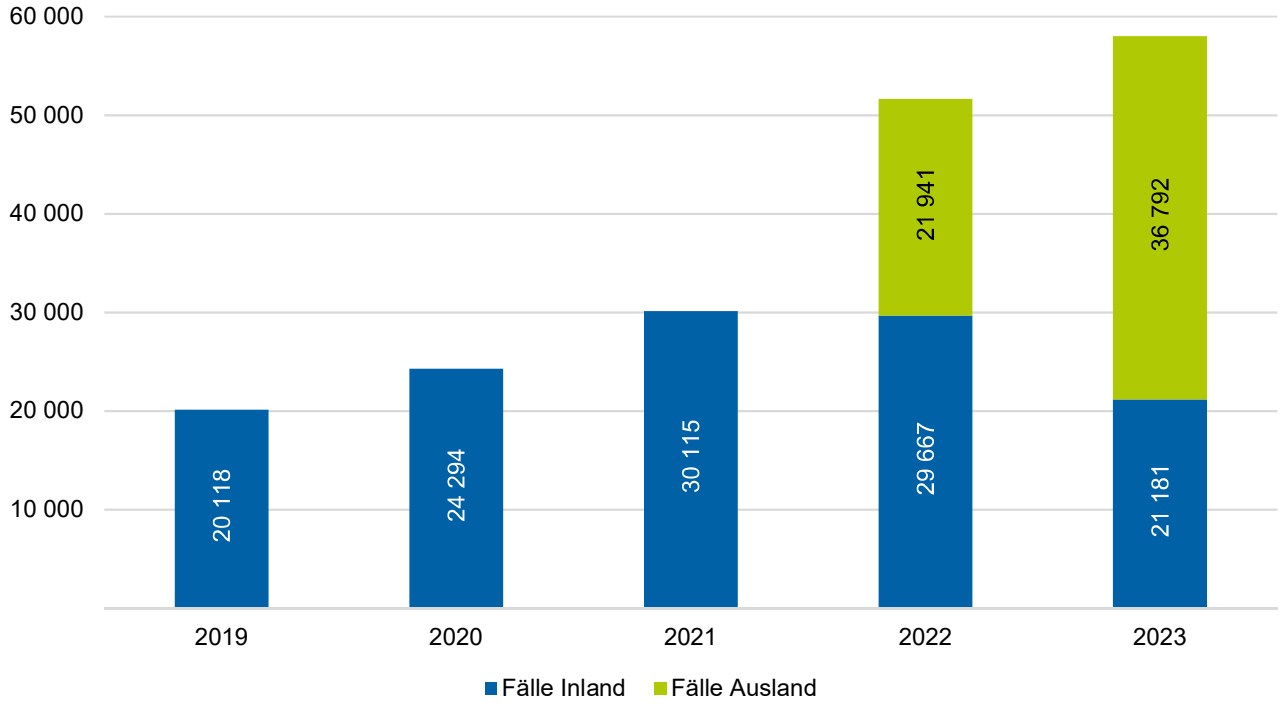
Tabelle 1
Entwicklung der Fallzahlen und Aufklärungsquoten der Cybercrime im engeren Sinne

Jahr	erfasste Fälle	Veränderung in %	aufgeklärte Fälle	Aufklärungsquote in %
2022	51 608		8 560	16,6
2023	57 973	12,3	9 496	16,4

Quelle: PKS NRW und Auslandsstatistik 2022 und 2023 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.

Abbildung 1
Vergleich Fallzahlen Cybercrime im engeren Sinne



Quelle: PKS NRW und Auslandsstatistik NRW

Tabelle 2
Fallzahlen in einzelnen Deliktsfeldern der Cybercrime im engeren Sinne (Inland)

Delikt	2022	2023	Zu-/Abnahme	Veränderung in %
Computerkriminalität (Cybercrime im engeren Sinne)	**29 667**	**21 181**	**- 8 486**	**- 28,6**
Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei der Datenverarbeitung §§ 269, 270 StGB	4 129	2 300	- 1 829	- 44,3
Datenveränderung, Computersabotage §§ 303a, 303b StGB	1 194	390	- 804	- 67,3
Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen und Datenhehlerei §§ 202a, 202b, 202c, 202d StGB	4 153	1 976	- 2 177	- 52,4
Computerbetrug § 263a StGB	20 191	16 515	- 3 676	- 18,2
Betrügerisches Erlangen von Kfz § 263a StGB	13	12	- 1	- 7,7
Weitere Arten des Warenkreditbetruges § 263a StGB	5 999	3 644	- 2 355	- 39,3
Computerbetrug mittels rechtswidrig erlangter Zahlungskarten mit PIN § 263a StGB	4 161	4 171	10	0,2
Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten § 263a StGB	2 916	3 308	392	13,4
Computerbetrug mittels rechtswidrig erlangter sonstiger unbarer Zahlungsmittel § 263a StGB	1 831	1 533	- 298	- 16,3
Leistungskreditbetrug § 263a StGB	964	452	- 512	- 53,1
Computerbetrug (sonstiger) § 263a StGB	3 856	3 097	- 759	- 19,7
Missbräuchliche Nutzung von Telekommunikationsdiensten § 263a StGB	71	48	- 23	- 32,4
Abrechnungsbetrug im Gesundheitswesen § 263a StGB	11	6	- 5	- 45,5
Überweisungsbetrug § 263a StGB	369	244	- 125	- 33,9

Quelle: PKS NRW

Tabelle 3
Fallzahlen in einzelnen Deliktsfeldern der Cybercrime im engeren Sinne (Ausland)

Delikt	2022	2023	Zu-/Abnahme	Veränderung in %
Computerkriminalität (Cybercrime im engeren Sinne)	**21 941**	**36 792**	**14 851**	**67,7**
Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei der Datenverarbeitung §§ 269, 270 StGB	3 905	5 947	2 042	52,3
Datenveränderung, Computersabotage §§ 303a, 303b StGB	2 206	3 070	864	39,2
Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen und Datenhehlerei §§ 202a, 202b, 202c, 202d StGB	6 226	8 187	1 961	31,5
Computerbetrug § 263a StGB	9 604	19 588	9 984	104,0
Betrügerisches Erlangen von Kfz § 263a StGB	1	0	- 1	- 100,0
Weitere Arten des Warenkreditbetruges § 263a StGB	2 414	3 752	1 338	55,4
Computerbetrug mittels rechtswidrig erlangter Zahlungskarten mit PIN § 263a StGB	78	295	217	278,2
Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten § 263a StGB	2 430	6 497	4 067	167,4
Computerbetrug mittels rechtswidrig erlangter sonstiger unbarer Zahlungsmittel § 263a StGB	912	1 596	684	75,0
Leistungskreditbetrug § 263a StGB	387	714	327	84,5
Computerbetrug (sonstiger) § 263a StGB	3 054	6 306	3 252	106,5
Missbräuchliche Nutzung von Telekommunikationsdiensten § 263a StGB	67	16	- 51	- 76,1
Überweisungsbetrug § 263a StGB	261	412	151	57,9

Quelle: Auslandsstatistik NRW

Die Zunahme von 67,7 Prozent der Fallzahlen von Cybercrime im engeren Sinne im Vergleich zu den Zahlen des Jahres 2022 belegt, dass Cyberkriminalität nicht an örtliche Grenzen gebunden ist. Die Täter agieren zunehmend aus dem Ausland oder nicht ermittelbaren Orten.

Die Auslandstaten stellen die Polizei in NRW vor große Herausforderungen bei der Ermittlung und Festnahme von Tatverdächtigen. Dies ist auf juristische Hürden und mangelnde Bereitschaft einiger Staaten im Bereich der internationalen Strafverfolgung zurückzuführen.

1.1.3 Aufklärungsquote

Von den im Jahr 2023 erfassten Straftaten der Cybercrime im engeren Sinne wurden 9 496 aufgeklärt. Die Aufklärungsquote liegt mit 16,38 Prozent (16,59 %) auf Vorjahresniveau. Im Bereich des Computerbetrugs wurden 6 646 Fälle aufgeklärt. Dies entspricht einer Aufklärungsquote von 18,41 Prozent (20,08 %).

Tabelle 4
Aufklärungsquote (AQ)

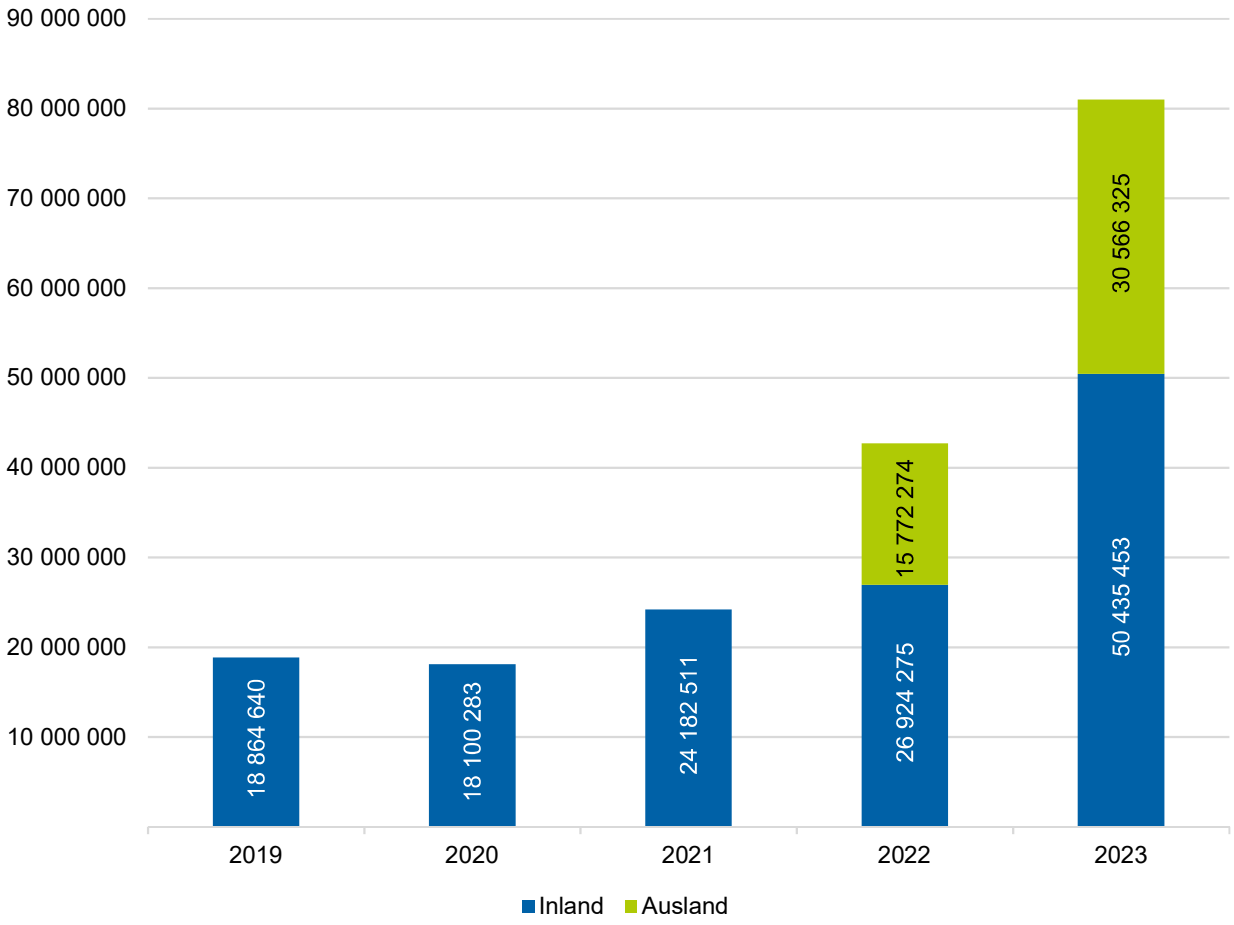
Delikt	Aufgeklärte Fälle		Aufklärungsquote		Zu-/Abnahme (AQ) %-Punkte
	2022	2023	2022	2023	
Computerkriminalität (Cybercrime im engeren Sinne)	**8 560**	**9 496**	**16,6**	**16,4**	**- 0,2**
Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei der Datenverarbeitung §§ 269, 270 StGB	1 422	1 587	17,7	19,2	1,5
Datenveränderung, Computersabotage §§ 303a, 303b StGB	238	271	7,0	7,8	0,8
Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen und Datenhehlerei §§ 202a, 202b, 202c, 202d StGB	917	992	8,8	9,8	0,9
Computerbetrug § 263a StGB	5 983	6 646	20,1	18,4	- 1,7
Betrügerisches Erlangen von Kfz § 263a StGB	7	11	50,0	91,7	41,7
Weitere Arten des Warenkreditbetruges § 263a StGB	2 099	2 308	24,6	31,2	6,6
Computerbetrug mittels rechtswidrig erlangter Zahlungskarten mit PIN § 263a StGB	816	853	19,3	19,1	- 0,2
Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten § 263a StGB	480	793	9,0	8,1	-0,9
Computerbetrug mittels rechtswidrig erlangter sonstiger unbarer Zahlungsmittel § 263a StGB	618	498	22,5	15,9	-6,6
Leistungskreditbetrug § 263a StGB	374	275	27,7	23,6	- 4,1
Computerbetrug (sonstiger) § 263a StGB	1 378	1 695	19,9	18,0	-1,9
Missbräuchliche Nutzung von Telekommunikationsdiensten § 263a StGB	13	39	9,4	60,9	51,5
Abrechnungsbetrug im Gesundheitswesen § 263a StGB	5	6	45,5	100,0	54,5
Überweisungsbetrug § 263a StGB	193	168	30,6	25,6	-5,0

Quelle: PKS NRW und Auslandsstatistik NRW

1.1.4 Schadensentwicklung

In der PKS NRW werden im Bereich Cybercrime ausschließlich für das Delikt Computerbetrug Schäden abgebildet. Im Bereich der Erpressungsdelikte ist eine Differenzierung nach Erpressungen im Kontext mit Cybercrimedelikten nicht möglich. Im Jahr 2023 erhöhte sich der Gesamtschaden der Computerkriminalität um 38 305 229 Euro auf 81 001 778 (42 696 549) Euro und erreicht somit einen neuen Höchstwert innerhalb der vergangenen fünf Jahre.[2]

Abbildung 2
Vergleich Schadensentwicklung Cybercrime Inland und Ausland in Euro



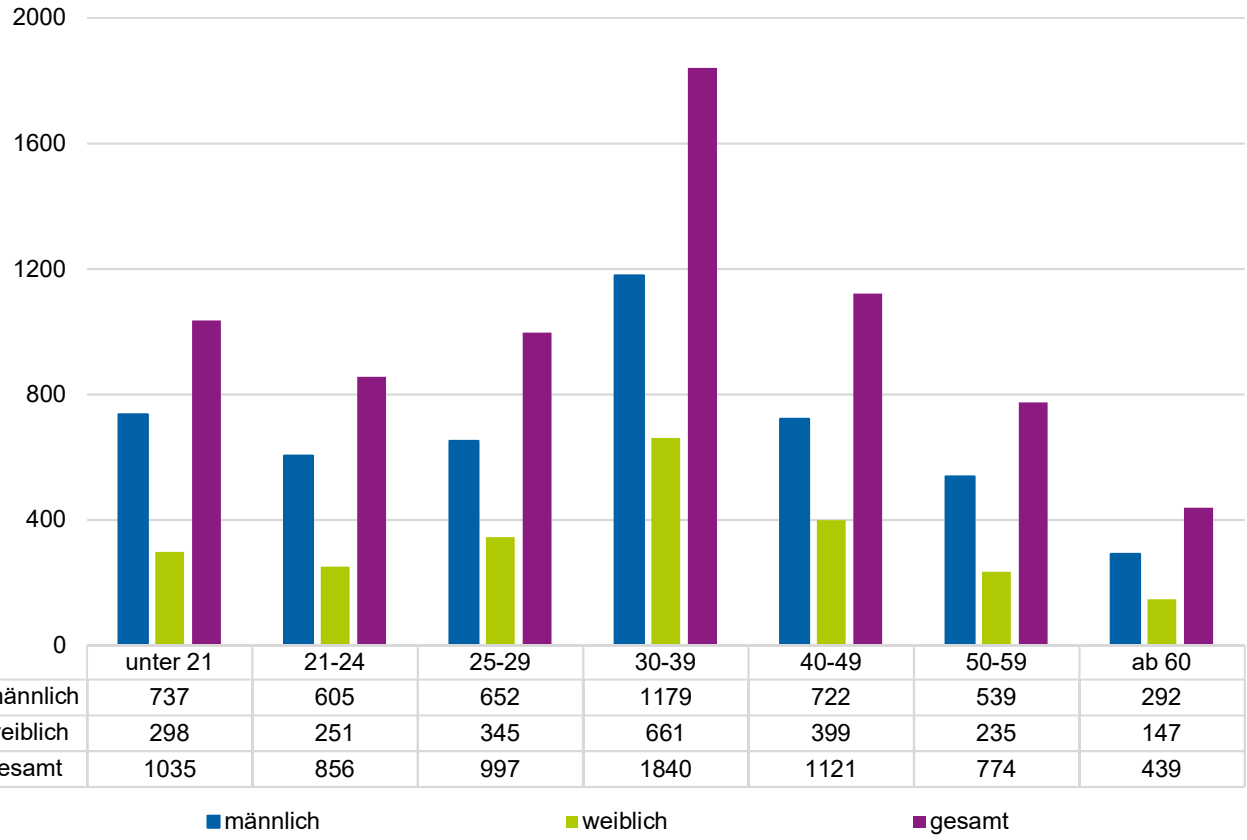
Quelle: PKS NRW Inland und Ausland und Auslandsstatistik NRW

[2] Der signifikante Anstieg im Bereich der Schadenssumme (Inland) ist zurückzuführen auf ein Verfahren mit einer Schadenshöhe von 24 001 664 Euro. Der Anstieg der Schadenssumme (Ausland) ergibt sich aus dem Anstieg der Fallzahlen im Bereich der Auslandsstraftaten.

1.1.5 Tatverdächtige

Im Jahr 2023 wurden 7 062 (6 623) Tatverdächtige ermittelt. Die männlichen Tatverdächtigen sind mit 4 726 gegenüber den weiblichen Tatverdächtigen mit 2 336 überrepräsentiert. Den größten Anteil nahm mit 1 840 ermittelten Tatverdächtigen die Gruppe der Erwachsenen im Alter von 30 bis 39 Jahren ein.

Abbildung 3
Tatverdächtige Computerkriminalität nach Alter und Geschlecht (Inland)



	unter 21	21-24	25-29	30-39	40-49	50-59	ab 60
männlich	737	605	652	1179	722	539	292
weiblich	298	251	345	661	399	235	147
gesamt	1035	856	997	1840	1121	774	439

Quelle: PKS NRW und Auslandsstatistik NRW

1.2 Darstellung ausgewählter Phänomenbereiche

Datenveränderung, Computersabotage

Bei der Begehung bestimmter Straftaten erfüllen die Täter mehrere Straftatbestände, sodass die Darstellung der Kriminalitätsentwicklung in diesem Deliktsbereich auf Grundlage der Deliktsschlüssel unzureichend aussagekräftig ist. Aus diesem Grund werden bei diesen Begehungsweisen die einzelnen Deliktschlüssel zu Phänomenen zusammengefasst. Sie werden unabhängig von der deliktischen Erfassung ausgewertet, um so Entwicklungen genauer darstellen zu können. Beispielsweise werden durch die Verwirklichung von Straftaten in dem Phänomenbereich Ransomware, abhängig von der Tatbegehungsweise, üblicherweise die Straftatbestände Computersabotage (§303b StGB), Abfangen von Daten (§202b StGB), Erpressung (§253 StGB) oder Datenveränderung (§303a StGB) erfüllt.

Die Fallzahlen im Deliktsbereich Datenveränderung, Computersabotage §§ 303a, 303b StGB sind im Jahr 2023 auf insgesamt 3 460 um 1,76 Prozent gestiegen. Davon waren 3 070 Fälle Auslands- und 390 Fälle Inlandstaten. Die Aufklärungsquote im Jahr 2023 stieg leicht auf 7,83 Prozent (7,00 %).

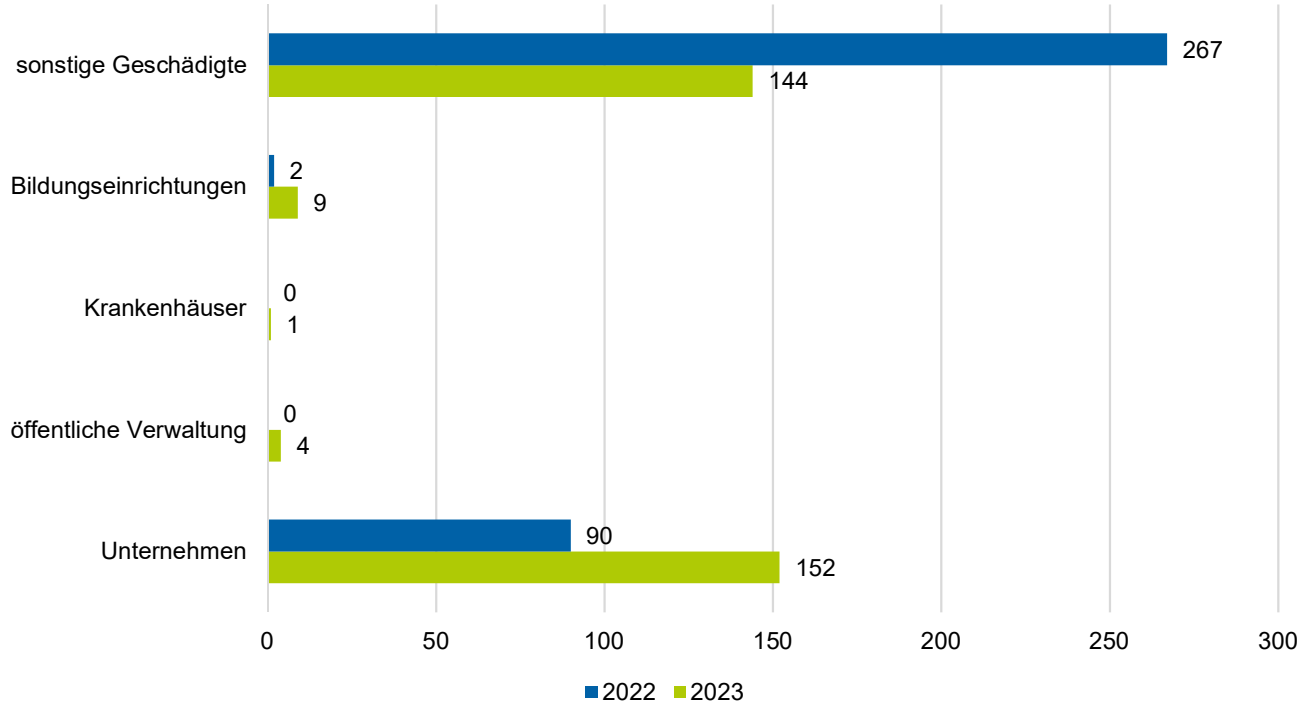
Ransomware

Ransomware-Angriffe stellen auch im Jahr 2023 eine der größten Bedrohungen im Bereich der IT-Sicherheit dar. Dabei handelt es sich um eine Begehungsweise, bei der unter Nutzung von Schadsoftware die Daten auf infizierten Systemen verschlüsselt werden. Die Täter fordern Lösegeld von den Opfern, um eine Wiederherstellung der Daten möglich zu machen. Die betroffenen Firmen bzw. Organisationen sind in den meisten Fällen nicht mehr oder nur eingeschränkt arbeitsfähig. Die angegriffene IT-Infrastruktur bleibt beschädigt und erfordert in der Regel eine Neuinstallation. Zwar sind die Fallzahlen von Ransomware-Angriffen im Verhältnis zu anderen Phänomenen bzw. Delikten gering, aber der daraus entstehende betriebs- und volkswirtschaftliche Schaden ist oftmals immens. Wird beispielsweise ein Zulieferbetrieb eines oder mehrerer Automobilhersteller verschlüsselt, so kann es sein, dass die Produktion des Zulieferbetriebs stillsteht und durch eine mögliche Exklusivität der Produkte die gesamte Lieferkette über Monate beeinträchtigt wird. Der betriebs- und volkswirtschaftliche Schaden, der durch Ransomware-Angriffe auf die IT-Infrastrukturen von Krankenhäusern, Bildungseinrichtungen oder kommunalen Verwaltungen entsteht, lässt sich oftmals monetär nicht ermessen.

Das allgemeine Vorgehen bei einem Ransomware-Angriff besteht darin, dass die Angreifer zunächst in das IT-Netzwerk ihrer Opfer eindringen und im Weiteren die Daten auf dem System verschlüsseln. In vielen Fällen geschieht der Angriff als „Double Extortion Ransomware“. Dazu werden im Vorfeld der Verschlüsselung Unternehmensdaten aus dem angegriffenen IT-System exfiltriert. Um der finanziellen Forderung Nachdruck zu verleihen, wird anschließend durch die Täter-Gruppierungen mit der Veröffentlichung der exfiltrierten Daten (englisch: leaken) oder dem Verkauf zum Zwecke einer Imageschädigung gedroht.

Die Täter gehören häufig Ransomware-Gruppierungen an bzw. nutzen deren Support (Cybercrime-as-a-Service). Im Jahr 2023 hatte die Gruppierung Akira einen bedeutenden Anteil an den Ransomware-Angriffen in NRW und gilt derzeit als eine der am schnellsten wachsenden Ransomware-Gruppierungen. Akira verfolgt vor allem monetäre Ziele. Mit Ransomware-Angriffen versuchen sie hohe Lösegeldsummen von ihren Opfern zu erpressen. So erfolgte beispielsweise im Oktober 2023 durch Akira ein Cyberangriff auf die Süd-Westfalen IT (SIT), der eine Verschlüsselung der informationstechnischen Systeme zur Folge hatte. Das Unternehmen verlor jeglichen Zugriff auf diese Systeme. Die Angreifer nutzten eine Schwachstelle in der IT-Sicherheitsarchitektur, um auf die Systeme zuzugreifen. Bei der SIT handelt es sich um einen kommunalen Zweckverband, der die informationstechnische Infrastruktur von 72 Kreisen und Gemeinden betreibt und betreut. Als Folge des erfolgreichen Cyberangriffs kam es zu einem Ausfall aller Bürgerdienste in den betroffenen Stadtverwaltungen dieser Gemeinden. Die Verwaltungen sind seither nicht oder beschränkt arbeitsfähig.

Abbildung 4
Fallzahlen von Ransomware auf bestimmte Zielgruppen



Quelle: PKS NRW und Auslandsstatistik NRW

(Distributed-) Denial-of-Service

Seit Beginn des russischen Angriffskriegs gegen die Ukraine im Februar des Jahres 2022 hat sich die Bedrohungslage im Cyberraum verschärft. Besonders DDoS-Angriffe aus politisch motivierten Gründen, initiiert von russischen Gruppierungen wie NoName057 bzw. Killnet, stellen eine ernsthafte Gefahr dar. Diese Cyberangriffe zielen darauf ab, durch die gezielte Störung von Servern Verunsicherung zu verbreiten, Geschäftsprozesse zu stören sowie Aufmerksamkeit zu erregen und die öffentliche Meinung zu beeinflussen. DDoS-Angriffe richten sich nicht nur gegen Ziele in der Ukraine, sondern verstärkt auch gegen Ziele in Deutschland, darunter NRW.

Die direkten Auswirkungen der DDoS-Angriffe auf die IT-Infrastruktur sind in der Regel begrenzt, können jedoch zu vorübergehenden Ausfällen von Webseiten und Online-Services führen. Durch DDoS-as-a-Service ist es nahezu jedermann möglich DDoS-Angriffe, gegen Bezahlung in Auftrag zu geben, durchzuführen.

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

Im Berichtsjahr 2023, insbesondere im zweiten Halbjahr, wurde eine verstärkte Häufung von Fallzahlen im Bereich des Computerbetrugs gemäß §263a StGB festgestellt, bei denen Täter über Kleinanzeigenplattformen aktiv wurden. Die Täter gaben vor, oft auch mit Hilfe übernommener Accounts von Dritten, Artikel zu kaufen oder zu verkaufen. Der An- und Verkauf soll dabei mittels der plattfominternen Bezahlmethode erfolgen. Im weiteren Verlauf wurden die Geschädigten durch geschickte Gesprächsführung, Phishing-E-Mails oder QR-Codes auf gefälschte, täuschend echt aussehende Webseiten geführt. Dort wird die Eingabe sensibler Zugangsdaten oder Kreditkarteninformationen gefordert, um die Transaktion abschließen zu können. Die so erlangten Daten wurden von den Tätern insbesondere dazu genutzt, die Kreditkarteninformationen für Bestellungen oder Zahlungen im Internet zu nutzen oder digitale Zahlungskarten auf mobilen Endgeräten der Täter einzurichten, mit denen Verfügungen am Geldautomaten oder im Einzelhandel durchgeführt werden.

Fälschung beweiserheblicher Daten – Business-E-Mail-Compromise (BEC)

Das BEC hat sich als eine raffinierte Form des Internetbetrugs etabliert, die Unternehmen weltweit bedroht. Insbesondere im Jahr 2023 setzte sich dieser Trend mit großer Geschwindigkeit fort, wobei die Nutzung von Künstlicher Intelligenz (KI) die Effektivität dieser Angriffe deutlich steigerte. BEC ist eine Betrugsmethode, bei der Kriminelle – oftmals mit Erfolg – versuchen, sensible Daten abzugreifen oder finanzielle Transaktionen auszulösen. Die Täter beabsichtigen Angestellte von Unternehmen oder Institutionen per E-Mail zu manipulieren. Die häufigsten Ziele sind die Veranlassung von Überweisungen hoher Geldsummen auf die Bankkonten der Betrüger, aber auch das Ausspionieren sensibler Daten für zukünftige Straftaten.

Der Einsatz von KI in BEC-Angriffen erhöht deutlich die Gefahr, die von diesen Angriffen ausgeht. Durch maschinelles Lernen können Angreifer nun ohne großen Aufwand personalisierte und überzeugende E-Mails erstellen, die schwer von legitimen Nachrichten zu unterscheiden sind. KI-gestützte Angriffe ermöglichen es, Sprachstile von Geschäftsführern oder Lieferanten zu imitieren, um Mitarbeiter zur Preisgabe von Informationen oder zur Autorisierung von Zahlungen zu verleiten. Diese Entwicklung erhöht die Gefahr von BEC-Angriffen erheblich und erschwert die Abwehr durch herkömmliche Sicherheitsmaßnahmen.

Die strafrechtliche Bewertung von BEC-Angriffen bleibt bestehen und umfasst weiterhin typische Straftatbestände wie Betrug, Fälschung beweiserheblicher Daten und Computerbetrug. Allerdings erfordert der Einsatz von KI in diesen Angriffen möglicherweise auch eine Überarbeitung der bestehenden Gesetze, um den sich verändernden Bedrohungen angemessen zu begegnen. Auch bei diesem Kriminalitätsphänomen wird die internationale Kooperation zur Strafverfolgung zunehmend wichtiger.

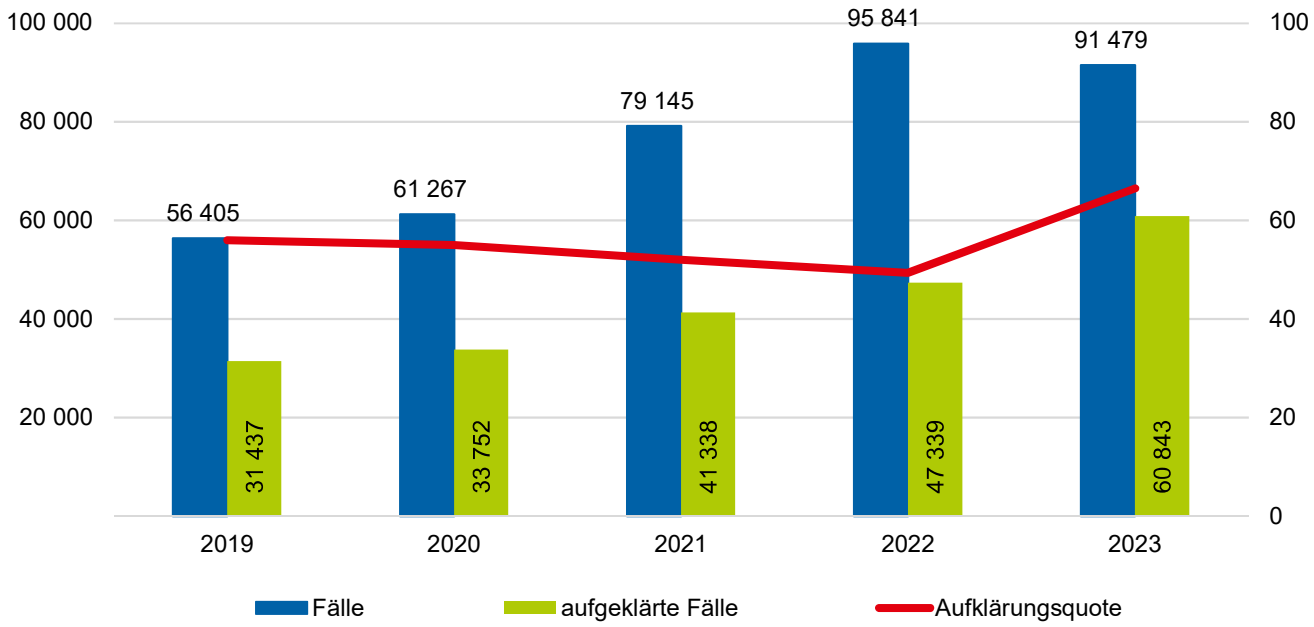
2 Lagedarstellung Straftaten mit Tatmittel Internet

Straftaten aus den Bereichen Cybercrime im engeren und weiteren Sinne, bei denen das Internet als Tatmittel verwendet wird, werden in der PKS NRW mit der Sonderkennung „Tatmittel Internet“ erfasst. Hierunter werden auch Straftaten erfasst, die nicht ausschließlich über klassische Webbrowser am Computer, sondern ebenso durch die Nutzung von Messengerdiensten oder Applikationen auf mobilen Endgeräten wie Smartphones oder Tablets begangen werden. Der größte Anteil an Straftaten mit Tatmittel Internet liegt im Bereich Cybercrime im weiteren Sinne.

Der Unterschied zur Cybercrime im engeren Sinne in Verbindung mit dem Tatmittel Internet wird insbesondere beim Betrug deutlich: Erfolgt die Täuschungshandlung gegenüber einem informationstechnischen System, handelt es sich um einen Computerbetrug gemäß § 263a StGB und damit um Cybercrime im engeren Sinne. Erfolgt die Täuschung unter Nutzung eines Computers gegenüber einem Menschen, liegt ein Betrug mit Tatmittel Internet gemäß § 263 StGB vor, also 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. Im Jahr 2023 wurden 91 479 Fälle mit dem Tatmittel Internet erfasst, 4 362 weniger als 2022. Den größten Anteil nahmen hierbei Betrugsdelikte mit 53 441 Fällen ein. Bei einer Aufklärungsquote von 66,51 Prozent wurden 60 843 Straftaten mit „Tatmittel Internet“ aufgeklärt. Dies bedeutet eine Steigerung der Aufklärungsquote um 17,12 Prozentpunkte im Vergleich zum Jahr 2022 (49,39 %).

Abbildung 5
Straftaten mit Tatmittel Internet[3]



Quelle: PKS NRW Inland

[3] Für Straftaten mit Tatmittel Internet werden keine statistischen Daten zu Auslandsstraftaten erfasst.

Tabelle 5
Straftaten mit Tatmittel Internet

	Gesamt	davon mit Tatmittel Internet	
	Fälle	Fälle	Anteil in %
Alle Straftaten	**1 412 807**	**91 479**	**6,5**
Straftaten gegen die sexuelle Selbstbestimmung	32 463	13 796	42,5
Verbreitung pornografischer Schriften (Erzeugnisse) gem. §§ 184, 184a, 184b, 184c, 184d, 184e StGB	14 172	12 395	87,5
Verbreitung, Erwerb, Besitz und Herstellung kinderpornographischer Inhalte gemäß § 184b StGB	10 728	9 519	88,7
Verbreitung von Kinderpornographie gemäß § 184b Abs. 1 Nr. 1	4 968	4 567	91,9
Betrug §§ 263, 263a, 264, 264a, 265, 265a, 265b StGB	181 245	53 441	29,5
Waren- und Warenkreditbetrug	64 411	29 011	45,0
Computerbetrug (sonstiger) §263a StGB	3 097	2 173	70,2
Betrügerisches Erlangen von Kfz § 263a StGB	12	7	58,3
Weitere Arten des Warenkreditbetruges § 263a StGB	3 644	3 017	82,8
Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten § 263a StGB	3 308	2 101	63,5
Computerbetrug mittels rechtswidrig erlangter sonstiger unbarer Zahlungsmittel § 263a StGB	1 533	824	53,8
Leistungskreditbetrug § 263a StGB	452	324	71,7
Überweisungsbetrug § 263a StGB	244	140	57,4
Missbräuchliche Nutzung von Telekommunikationsdiensten § 263a StGB	48	46	95,8
Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung §§ 269, 270 StGB	2 300	1 681	73,1
Datenveränderung, Computersabotage §§ 303a, 303b StGB	390	314	80,5
Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen und Datenhehlerei §§ 202a, 202b, 202c, 202d StGB	1 976	1 451	73,4
Erpressung § 253 StGB	2 707	1 029	38,0

Quelle: PKS NRW

Tabelle 6
Entwicklungen der Straftaten mit Tatmittel Internet

	2022	2023	Zu-/Abnahme	Veränderung in %
Straftaten mit Tatmittel Internet	**95 841**	**91 479**	**- 4 362**	**- 4,6**
Straftaten gegen die sexuelle Selbstbestimmung	15 098	13 796	- 1 302	- 8,6
Verbreitung pornografischer Inhalte (Erzeugnisse) gem. §§ 184, 184a, 184b, 184c, 184d, 184e StGB	14 142	12 395	- 1 747	- 12,4
Verbreitung, Erwerb, Besitz und Herstellung kinderpornographischer Schriften gemäß § 184b StGB	10 977	9 519	- 1 458	- 13,3
Verbreitung von Kinderpornographie gemäß § 184b Abs. 1 Nr. 1	5 059	4 567	- 492	- 9,7
Betrug §§ 263, 263a, 264, 264a, 265, 265a, 265b StGB	60 577	53 441	- 7 136	- 11,8
Waren- und Warenkreditbetrug	34 262	29 011	- 5 251	- 15,3
Computerbetrug (sonstiger) §263a StGB	2 673	2 173	- 500	- 18,7
Betrügerisches Erlangen von Kfz § 263a StGB	4	7	3	75,0
Weitere Arten des Warenkreditbetruges § 263a StGB	4 604	3 017	- 1 587	- 34,5
Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten § 263a StGB	1 534	2 101	567	37,0
Computerbetrug mittels rechtswidrig erlangter sonstiger unbarer Zahlungsmittel § 263a StGB	1 038	824	- 214	- 20,6
Leistungskreditbetrug § 263a StGB	660	324	- 336	- 50,9
Überweisungsbetrug § 263a StGB	206	140	- 66	- 32,0
Missbräuchliche Nutzung von Telekommunikationsdiensten § 263a StGB	44	46	2	4,6
Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung §§ 269, 270 StGB	2 901	1 681	- 1 220	- 42,1
Datenveränderung, Computersabotage §§ 303a, 303b StGB	1 003	314	- 689	- 68,7
Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen und Datenhehlerei §§ 202a, 202b, 202c, 202d StGB	4 078	1 451	- 2 627	- 64,4
Erpressung § 253 StGB	1 690	1 029	- 661	- 39,1

Quelle: PKS NRW

2.1 Darstellung ausgewählter Phänomenbereiche

2.1.1 Immobilienbetrug

Über Online-Portale werden Wohnungssuchende seitens der Täter mit dem Angebot einer freistehenden Wohnung kontaktiert. Bei Interesse an einer Wohnungsbesichtigung werden die Interessenten auf eine gefälschte Website geführt, die der einer existierenden Immobilienfirma täuschend ähnlichsieht.

Nach Buchung einer eigenständigen und kontaktlosen Wohnungsbesichtigung können die Interessenten den Wohnungsschlüssel in einem mit Code zugänglichen Schlüsselkasten in Wohnungsnähe abholen. Nach erfolgter Besichtigung werden die Interessenten durch die Täter zwecks Interessenabfrage kontaktiert. Bei Interesse der Opfer wird ihnen nach einer Wartezeit der Zuschlag erteilt und der Mietvertrag zugesandt. In diesem Schritt werden die Opfer aufgefordert den Mietvertrag zu unterzeichnen und einen Kautionsbetrag, die erste Monatsmiete im Voraus sowie ggf. eine Abschlagszahlung für Möbel zu überweisen.
Den Opfern wird suggeriert, man werde sich dann zu Mietbeginn am Objekt treffen und eine persönliche Übergabe durchführen. Zum vereinbarten Termin stellen die Opfer am Mietobjekt fest, dass die Wohnung zwar unbewohnt ist, jedoch anstatt des Vermieters zahlreiche weitere Opfer mit dem gleichen Mietvertrag für dieselbe Immobilie vor Ort erschienen sind.

2.1.2 Fake-Shops

Anhand von Fake-Shops wird deutlich, dass die Täter fortlaufend etablierte Tatbegehungen im Rahmen ihrer kriminellen Möglichkeiten anpassen, um die Wahrscheinlichkeit eines Taterfolgs zu erhöhen. Ein in jüngerer Vergangenheit vielfach aufgetretener Modus Operandi betrifft Flugreisende. Die Täter erstellen Webseiten, welche die Urheberschaft von Fluggesellschaften, unter anderem anhand des Firmenlogos, vorspiegeln und enthalten Rufnummern zu einem durch die Täter bereitgestellten Kundenservice. Bei Anruf dieser Rufnummer meldet sich der vermeintliche Kundenservice. Die Täter zielen darauf ab, im Rahmen einer „individuellen Beratung“ das Opfer zu veranlassen, eine Überweisung vorzunehmen und sensible Daten mitzuteilen. Die Täter profitieren davon, dass viele Flugreisende besonders bemüht sind preiswerte Flugreisen zu finden. Zudem müssen sich Reisende grundsätzlich, oft auch kurzfristig, mit einer Vielfalt von Fragen im Rahmen ihrer Reiseplanung auseinandersetzen, wodurch der kritische Blick im Einzelfall getrübt sein kann. Diese Umstände nutzen die gut vorbereiteten Täter aus, die Opfer vor dem Hintergrund eines vermeintlich attraktiven Angebots und im Telefonat mit einer angeblichen Mitarbeiterin/eines Mitarbeiters der Fluggesellschaft dazu zu bringen, den Anweisungen zu folgen.

2.2 Kinderpornographie

Im Jahr 2023 wurden in dem Deliktsbereich „Verbreitung, Erwerb, Besitz und Herstellung kinderpornographischer Inhalte“ gemäß § 184b StGB 10 728 (11 183) Fälle erfasst. Dies entspricht einem Rückgang von 4,07 Prozent. Die Aufklärungsquote lag im Jahr 2023 mit 9 101 aufgeklärten Fällen bei 84,83 Prozent und erhöhte sich damit im Vergleich zum Vorjahr (84,36 %) um 0,47 Prozentpunkte.

Mit einer Anzahl von 9 519 Fällen (88,73 %) nimmt das Internet als Tatmittel für den Deliktsbereich der Kinderpornographie weiterhin eine herausragende Bedeutung ein, wenngleich der prozentuale Anteil im Vergleich zum Vorjahr (98,16 %) um 9,43 Prozentpunkte sank. Von den erfassten Fällen konnten 8 050 Taten und somit 84,57 Prozent aufgeklärt werden, was einer Steigerung um 0,59 Prozentpunkten im Vergleich zum Vorjahr (83,98 %) entspricht.

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 eingegangenen Hinweise ging im Jahr 2023 im Vergleich zum Vorjahr um 18 Prozent zurück. Nach Prüfung der strafrechtlichen Relevanz und erfolgversprechender Ermittlungsansätze durch das BKA wurden dem Landeskriminalamt Nordrhein-Westfalen (LKA NRW) im Jahr 2023 insgesamt 12 169 (14 857) Verdachtsfälle bekannt. Diese werden nach Erstbearbeitung durch das LKA NRW über die Zentral- und Ansprechstelle Cybercrime der Staatsanwaltschaft Köln (ZAC NRW) den nordrhein-westfälischen Kreispolizeibehörden (KPB) zu weiteren Ermittlungen zugeleitet.

Die Zahl der Tatverdächtigen aus Nordrhein-Westfalen in bundesweiten Umfangsverfahren sank von 591 im Jahr 2022 auf 204 im Jahr 2023.

Die Zahl der Tatverdächtigen unter 14 Jahren lag mit 1 524 (1 546) in etwa auf dem Niveau des Vorjahres. 2 189 Tatverdächtige waren zwischen 14 und 18 Jahren alt (2 718). Somit ist die Zahl der jugendlichen Tatverdächtigen um 19,46 Prozent gesunken. Bei 41,80 Prozent (54,60 %) aller bekannten Tatverdächtigen handelt es sich im Jahr 2023 demnach um Kinder und Jugendliche.

Das seit Sommer 2021 bekannte Phänomen im In- und Ausland, bei denen Facebook-Accounts gehackt und anschließend inkriminierte Bilder oder Videos hochgeladen wurden, hat sich inzwischen ebenfalls auf Instagram-Accounts ausgeweitet. Hintergründe und Absichten dieser Hacking Angriffe sind bisher nicht bekannt. Erkenntnisse zu diesem Phänomen werden weiterhin gesammelt und ausgewertet.

3 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

[4] Schwind, Hans-Dieter: Kriminologie, 2011, 38.

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 2023 des Bitkom e.V. 80 Prozent in den letzten zwölf Monaten von Diebstahl, Industriespionage oder Sabotage betroffen. 82 Prozent der Unternehmen gaben an, dass die Anzahl der Cyberattacken in diesem Zeitraum eher oder stark zugenommen hat und erstmals fühlte sich mit 52 Prozent die Mehrheit der Unternehmen durch Cyberangriffe in ihrer Existenz bedroht.

Die Arten von Cyberangriffen waren bei 29 Prozent der befragten Unternehmen Angriffe auf Passwörter, bei 31 Prozent Phishing und bei 28 Prozent der Unternehmen die Infizierung mit Schadsoftware beziehungsweise Malware. Schäden durch DDoS-Angriffe wurden bei 12 Prozent der Unternehmen festgestellt und Schäden durch Ransomware bei 23 Prozent, was einem Anstieg von 11 Prozentpunkten im Vergleich zum Vorjahr entspricht.[6]

4 Interventionsteams Digitale Tatorte

Die zunehmende Professionalisierung der Straftäter bei der Begehung von Cybercrime sowie die kontinuierliche Erweiterung des Angebotsportfolios inkriminierter IT-Dienstleistungen führen zur Steigerung des Bedrohungspotentials. Der Aufnahme digitaler Tatorte/Spuren und der Auswertung digitaler Daten kommt dabei einerseits besondere Bedeutung zu, andererseits bedarf es hierzu spezifischer Expertise sowie modernster, technischer Ausstattung.

Um den Herausforderungen zu begegnen, werden die Interventionsteams Digitale Tatorte (IDT) die Tatortarbeit im Hinblick auf digitalen Spuren sowie die Ermittlungen bei Cyberangriffen gegen Krankenhäuser, Behörden und Wirtschaftsunternehmen weiter professionalisieren.

Die Polizei NRW stellt hierzu 94 IT-Spezialisten und KI-Experten ein. Sie richtet damit die IDT in den sechs KPB Bielefeld, Dortmund, Düsseldorf, Essen, Köln und Münster sowie dem LKA NRW ein und stattet diese mit mordernster Spezial-Hard- und -Software aus. Mit diesem Personal und modernster Ausstattung werden Cyberermittlungen, KI-Entwicklung und IT-Forensik in allen Kriminalitätsbereichen deutlich gestärkt. Begleitet wird dies durch die Bereitstellung zentraler IT-Systeme und moderner Kollaborationstechnik.

Mit dem Aufbau der IDT stellt sich die Polizei NRW auch organisatorisch für den Bereich Cybercrime neu auf. In den sechs Standortbehörden entstehen vor dem obigen Hintergrund die Kriminalinspektionen Cybercrime, in denen das Fachpersonal/die Fachdienststellen für den Bereich Cybercrime gebündelt werden. Im LKA NRW wird das Cybercrime-Kompetenzzentrum umstrukturiert, bündelt Kompetenzen, integriert ein IDT und koordiniert die Maßnahmen aller IDTs der Polizei NRW.

[5] Vgl. Dreißigacker, Arne/von Skarczinski, Bennet/Wollinger, Gina Rosa: Forschungsbericht Nr. 152, Cyberangriffe gegen Unternehmen, 2020, 150.
[6] Vgl. Mann, Streim, Lange: Wirtschaftsschutz 2023, Bitkom. URL: https://www.bitkom.org/sites/main/files/2023-09/Bitkom-Charts-Wirtschaftsschutz-Cybercrime.pdf (Abrufdatum 29. Mai 2024).

5 Prävention

Das Jahr 2023 war durch Herausforderungen, wie den Strukturwandel in der Industrie, Fachkräftemangel, den immer noch zu spürenden Auswirkungen der COVID-19-Pandemie sowie durch weltweite Spannungen in Verbindung mit den militärischen Konflikten, geprägt. In dieser Situation sah sich die Gesellschaft mit zunehmenden Bedrohungen aus dem digitalen Raum konfrontiert. Während im Jahr 2023 KI-Technologien weiterhin deutliche Fortschritte machten und in verschiedenen Bereichen eingesetzt wurden, entstanden auch neue Herausforderungen für die Cybersicherheit.

In dieser Situation ist es wichtig, der Wirtschaft Unterstützung, unter anderem in Form der polizeilichen Prävention, anzubieten. Das LKA NRW strebt an, dass mit den Präventionsmaßnahmen den kleinen und mittelständischen Unternehmen eine Hilfestellung gegeben wird, ihre eigenen Aktivitäten im Bereich Cybersicherheit einzuordnen, mögliche Handlungsbedarfe und Handlungsoptionen zu erkennen. Das LKA NRW macht auf Veranstaltungen und Messen die Unternehmen und Organisationen auf die vorhandenen Unterstützungs- und Präventionsangebote der Polizei, des Verfassungsschutzes sowie der Kooperationspartner aufmerksam. Neben Publikationen unterschiedlichster Art (Flyer, Social Media, auf der eigenen Homepage) bietet die Polizei NRW Institutionen, Behörden und Unternehmen Vorträge zu den aktuellen Gefahren des Cybercrime und der Awareness an.

5.1 Zuständigkeiten und Geltungsbereich

Die Prävention von Cybercrime obliegt grundsätzlich den KPB. Das LKA NRW unterstützt die KPB insbesondere durch das Optimieren von Standards, Entwickeln von Medien sowie durch Initiierung und Koordination 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 zu den Aufgaben der KPB gehört, deckt das LKA NRW mit dem Cybercrime-Kompetenzzentrum den Bereich der Cybercrime-Prävention im engeren Sinn ab. Adressaten sind insbesondere kleine und mittelständische Unternehmen, aber auch Behörden und vergleichbare Institutionen. Die Prävention von Cybercrime im weiteren Sinn ist vor dem Hintergrund der vielfältigen Deliktsbereiche durch intensive Kooperationen geprägt. Hier wird das LKA NRW zudem koordinierend tätig und setzt die Entwicklungen in diesem Deliktsbereich in Empfehlungen und Standards um.

5.2 Rückblick in ausgewählten Bereichen

Die Präventionsarbeit des LKA NRW umfasste auch im Jahr 2023 eine Reihe von Maßnahmen, wie Präventionskampagnen, Veranstaltungen und Vorträge zur Sensibilisierung und Awareness im Bereich Cybercrime, sowie das Networking, u. a. im Rahmen von Sicherheitspartnerschaften.

5.2.1 Landeskampagne „Mach-Dein-Passwort-stark“

Die Studie des Hasso-Plattner-Instituts zu geleakten Datensätzen aus 2023 hat gezeigt, dass das beliebteste Passwort nach wie vor die Zahlenreihe 1–9 ist.[7] Der Umgang mit Passwörtern ist weiterhin ein wichtiges Themenfeld für die kriminalpräventive Arbeit. Die Internetseite der durch das LKA NRW entwickelten Kampagne „Mach-dein-Passwort-stark“[8] wurde durch eine Medienagentur Ende 2023 überarbeitet. Mit der neuen Headline „Geht ganz einfach“ wurde die umgestaltete Internetseite zur Aktionswoche „Black Friday“ (47. KW) freigegeben. Neue Entwicklungen oder auch themenspezifische Präventionshinweise zu Aktionstagen, wie dem Safer Internet Day (6. Februar 2024) oder auch dem Weltfrauentag (8. März 2024), finden dort ebenfalls Berücksichtigung.

5.2.2 Messenger-Betrug

Unter der Beteiligung der Polizei NRW wurden die Präventionsmaßnahmen im Phänomenbereich Messenger-Betrug auf der Internetseite des Programms Polizeiliche Kriminalprävention der Länder und des Bundes intensiviert.[9] Beispielsweise wurden neben drei Status-Bildern, welche für das eigene Profil heruntergeladen werden konnten, kurze Clips/Reels für Soziale Medien erstellt und veröffentlicht. Ab dem 31.07.2023 gab es auf dieser Internetseite eine Themenwoche mit diversen Informationsmaterialien für interessierte Bürgerinnen und Bürger. Auch wurde im Zusammenhang mit der Betrugsmasche das Thema des sog. „Victim Blamings“ (Täter-Opfer-Umkehr) aufgegriffen. Unter der Überschrift „Wer ist so blöd und fällt darauf rein“ wird darauf hingewiesen, dass nicht die Opfer schuld sind, sondern die Täterinnen und Täter. Des Weiteren gehört zur erfolgreichen Bekämpfung des Phänomens die Störung der Täterinnen und Täter in ihrer Tatausführung und beim Erlangen der Beute. Dies kann dadurch erreicht werden, dass die Geldinstitute so früh wie möglich über erfolgte Geldtransaktionen informiert werden und durch frühzeitiges Agieren eine Rückholung des Geldes erfolgt. Diesbezüglich wurden Handlungsempfehlungen für die anzeigenaufnehmenden Polizeibeamtinnen und -beamten entwickelt. Diese beinhalten bündige Informationen zum Kriminalitätsphänomen sowie Checklisten in Bezug auf notwendige Informationen und Meldewege zur Informationsweitergabe an die Geldinstitute.

5.2.3 Kooperationen und Prävention im Bereich Wirtschaft und Unternehmen

Im Bereich Cybercrime im engeren Sinn wird ein bewährtes Netzwerk unterschiedlichster Kooperationspartner wie dem Bitkom e. V., dem VOICE e. V. - Bundesverband der IT-Anwender und der Sicherheitspartnerschaft mit der Allianz für Sicherheit in der Wirtschaft West NRW e. V. bedient. Seit 2017 besteht eine gleichgelagerte Kooperationsvereinbarung mit dem eco - Verband der Internetwirtschaft e. V. und dem Networker NRW e. V. Dieses Netzwerk ist eine sehr gut etablierte Kooperation zur Stärkung der Anzeigebereitschaft und dem Bewusstsein für die durch Cybercrime bestehenden Gefahren (Awareness) im Bereich der Wirtschaft. Auch weitere staatliche Behörden wie das Bundesamt für Sicherheit in der Informationstechnik und das BKA beteiligen sich an der Zusammenarbeit. Durch die enge Zusammenarbeit sensibilisiert das LKA NRW die unterschiedlichsten Akteure als Multiplikatoren innerhalb der Wirtschaft für den Bereich Prävention von Cybercrime. Der rege Austausch und die aktive Beteiligung stärken die vertrauensvolle Zusammenarbeit zwischen Wirtschaft und Polizei und steigern so die Awareness. Die Informations- und Wissensvermittlung umfasst neben den Möglichkeiten zum Schutz vor Angriffen auch die Sensibilisierung zur Notwendigkeit der Vorbereitung auf den „Ernstfall“.

Online-Veranstaltungen sind seit der Pandemiezeit ein wichtiger Kanal der Präventionsarbeit und werden weiterhin neben den Präsenz-Veranstaltungen regelmäßig genutzt. Digitale Angebote wie Streaming, Aufzeichnungen und Podcasts machen es möglich, die Teilnahme flexibel und bequem zu gestalten und so einen wesentlich breiteren Teilnehmerkreis zu erreichen.

Im Rahmen von Sicherheitskooperationen nimmt das LKA NRW regelmäßig an Fachmessen teil. Im Jahr 2023 war das LKA NRW beispielsweise erneut Aussteller bei der Internet Security Messe it-sa in Nürnberg, einem der wichtigsten Events im Bereich der Cybersicherheit. Durch die gemeinsamen Aktionen mit Kooperationspartnern des Bitkom e. V. auf Fachmessen

[7] https://hpi.de/news/jahrgaenge/2023/123456789-ist-das-beliebteste-passwort-2023-in-deutschland.html
[8] https://www.mach-dein-passwort-stark.de/
[9] https://www.polizei-beratung.de/themen-und-tipps/betrug/messenger/

weist die Polizei NRW auf aktuelle Gefahren des Cybercrime hin und zeigt auf, wie wichtig funktionierende Kooperationen bei der Bekämpfung von Cybercrime sind. Ein wesentliches Ziel ist das Verständnis für die polizeiliche Arbeit und dadurch die Kooperations- und Anzeigebereitschaft zu steigern. Das LKA NRW konkurriert als Arbeitgeber im IT-Bereich, einschließlich IT-Sicherheit, mit den anderen Unternehmen und hofft auch auf diesem Weg Fachkräfte zu gewinnen.

Das Ministerium des Innern des Landes Nordrhein-Westfalen, die Hochschule Niederrhein und die Hochschule Bonn-Rhein-Sieg sind eine Kooperation zur Entwicklung einer akademischen Qualifizierungsmaßnahmen „Cyberkriminalistik / Digitale Forensik“ zur Fortbildung von Polizeivollzugsbeamtinnen und -beamten zu Cyberkriminalistinnen und Cyberkriminalisten eingegangen. Der berufsbegleitende Bachelorstudiengang „Cyberkriminalistik/Digitale Forensik“ bereitet Ermittlerinnen und Ermittler am „Cyber Campus NRW“ in Mönchengladbach auf die Herausforderungen digitaler Kriminalität vor und vermittelt Problemlösekompetenzen für zukünftige digitale Bedrohungen. Im kommenden Wintersemester startet bereits der dritte Jahrgang in den Studiengang.

Cybercrime stellt eine Gefahr für alle Bereiche des gesellschaftlichen Lebens dar. Ob im privaten Umfeld beispielsweise durch Angriffe auf Social Media-Accounts oder die Haustechnik (Internet of Things), aber auch im Bereich von Unternehmen und Organisationen, wo durch Spionage, Ransomwareangriffe und weitere Arten des Cybercrime jährliche Schäden in Milliardenhöhe entstehen (Studie des Bitkom e. V.). Somit stellt die Bekämpfung von Cybercrime eine gesamtgesellschaftliche Aufgabe dar, zu der die polizeiliche Präventionsarbeit einen wesentlichen Beitrag leistet, indem sie auf die Gefahren hinweist, Lösungsmöglichkeiten aufzeigt und somit zu einer verbesserten Awareness beiträgt.

Herausgegeben von:

Landeskriminalamt Nordrhein-Westfalen
Völklinger Straße 49
40221 Düsseldorf

Abteilung 4
Cybercrime Kompetenzzentrum
Dezernat 41

Redaktion: Oliver Heinze, EKHK
Telefon: +49 211 939-4110
Fax: +49 211 939-194110
CNPol: 07-224-4110

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

Bildnachweis: Titelseite – Adobe Stock Polizei NRW

Stand September 2024