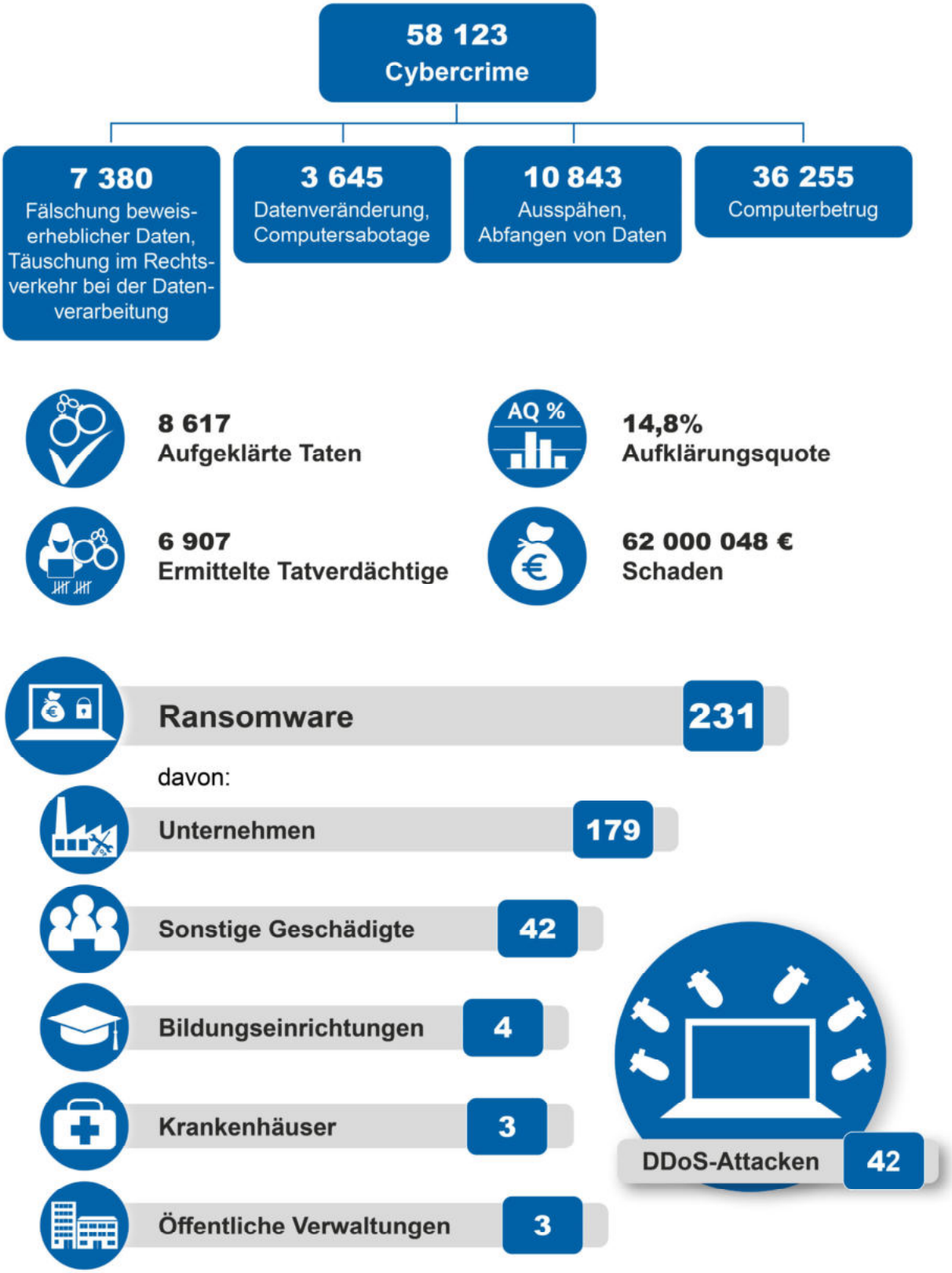
POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

bürgerorientiert · professionell · rechtsstaatlich

Cybercrime

Lagebild LKA NRW 2024

Cybercrime 2024 in Zahlen



Inhaltsverzeichnis

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

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 §§ 202a, 202b, 202c StGB
- Computerbetrug § 263a StGB:
  - Computerbetrug mittels rechtswidrig erlangter Zahlungskarten mit PIN
  - Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten
  - weitere Arten des Warenkreditbetruges

Cybercrime im weiteren Sinne

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 Handel mit Betäubungsmitteln oder Betrugsdelikte gemäß § 263 StGB.

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. 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 der PKS NRW werden ausschließlich Straftaten erfasst, bei denen der Handlungsort nachweislich in Deutschland liegt. Durch die globale Vernetzung kann der Ort an dem der Täter handelte von dem Ort abweichen, an dem der Schaden eingetreten 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.

Vor 20 Jahren betrug der Anteil der Internetnutzer in Deutschland ca. 53 %. Seitdem ist der Anteil stetig gestiegen[2], sodass im Jahr 2024 lediglich 4 % der Deutschen noch nie das Internet genutzt haben.[3] Im Jahr 2023 besaßen bereits 92 % (ca. 33 Millionen) der privaten Haushalte

[1] Übereinkommen des Europarats über Computerkriminalität vom 23. November 2001 in Budapest
[2] Vgl. Statista: *Anteil der Internetnutzer in Deutschland in den Jahren 2001 bis 2023*. 10.03.2025. https://de.statista.com/statistik/daten/studie/13070/umfrage/entwicklung-der-internetnutzung-in-deutschland-seit-2001/, zuletzt besucht:23.04.2025.
[3] Vgl. Statista: *Anteil der Deutschen, die noch nie das Internet genutzt haben in den Jahren 2005 bis 2024*. 18.12.2024. https://de.statista.com/statistik/daten/studie/158813/umfrage/anteil-der-nicht-nutzer-des-internets-in-deutschland/, zuletzt besucht: 23.04.2025.

in Deutschland einen Internetzugang.[4] Das Internet wird heutzutage auf vielfältige Weise genutzt, für Terminbuchungen, zum Einkaufen, zur Informationsbeschaffung, zum Musik- und Videostreaming sowie um mit Freunden über Social Media in Kontakt zu bleiben. 86 % der in Deutschland Lebenden nutzten 2024 das Internet, um E-Mails zu versenden und zu empfangen[5] und 84 % für das Online-Banking.[6] Die Digitalisierung und die zunehmende Internetnutzung bereichern sowohl das Privat- als auch das Geschäftsleben mit zahlreichen Vorteilen und sind aus dem modernen Alltag nicht mehr wegzudenken. Gleichzeitig eröffnen sie jedoch Kriminellen vielfältige neue Wege, Straftaten zu begehen. 80 % der Unternehmen in Deutschland geben an, dass Cyberangriffe in den letzten 12 Monaten zugenommen haben und die stattgefundenen Angriffe einen Schaden von 178,6 Millarden Euro verursachten.[7]

Im Bereich der Cybercrime ist unter anderem eine Zunahme der Auslandsstraftaten 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. Auslandsstraftaten 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.

In einzelnen Deliktsbereichen ist von einem großen Dunkelfeld auszugehen, da der Polizei viele Straftaten nicht bekannt sind, beziehungsweise nicht zur Anzeige gebracht werden. Davon ist auch bei den Delikten der Cybercrime auszugehen. Die Polizei NRW empfiehlt bei jedem Cyberangriff Anzeige zu erstatten. Dadurch werden die Strafverfolgungsbehörden in die Lage versetzt, wirkungsvolle Maßnahmen zur Störung der Täterinfrastruktur und zur Verfolgung der Täter sowie zum Abschöpfen kriminell erlangter Gewinne zu treffen.

Die Bekämpfung von Cybercrime ist in NRW seit 2011 Schwerpunkt. Die Bearbeitung von Cybercrimedelikten findet in allen 47 Kreispolizeibehörden (KPB) und dem Landeskriminalamt NRW (LKA NRW) statt. Hier ist seit 2011 auch das Cybercrime-Kompetenzzentrum der Polizei NRW angesiedelt. Die Schwerpunktsetzung zur Bekämpfung von Cybercrime wurde im Jahr 2024 noch einmal deutlich verstärkt:

Zum 15.07.2024 wurden in den sechs Polizeipräsidien Bielefeld, Dortmund, Düsseldorf, Essen, Köln und Münster eigene Kriminalinspektionen Cybercrime mit einem Interventionsteam Digitale Tatorte eingerichtet. Die Spezialisten der Interventionsteams arbeiten behördenübergreifend als ein Team zusammen. Sie und ihre Kompetenzen sind landesweit einsetzbar, selbst bei einer Störung öffentlicher Kommunikationseinrichtungen.

Für Unternehmen und Behörden hält das LKA NRW eine zentrale 24/7-Erreichbarkeit über einen Single Point of Contact (SPoC) bereit. Dieser ist über die Telefonnummer 0211-939-4040 oder die E-Mail-Adresse: cybercrime.lka@polizei.nrw.de erreichbar. Insbesondere in Fällen aktueller Angriffe auf Unternehmen und Einrichtungen wird so eine zeitnahe Reaktion der Polizei NRW sichergestellt.

---

[4] Vgl. Behrends, S., Geisler, S. Kott, K., Ziebach, M. 06.11.2024. *Internetnutzung, Sozialbericht 2024.* https://www.bpb.de/kurz-knapp/zahlen-und-fakten/sozialbericht-2024/553201/internetnutzung/, zuletzt besucht: 23.04.2025.

[5] Vgl. Statista: *Anteil der Bevölkerung in Deutschland, die das Internet für das Versenden und Empfangen von E-Mails nutzen in den Jahren 2002 bis 2024.* 18.12.2024. https://de.statista.com/statistik/daten/studie/204272/umfrage/nutzung-des-internets-fuer-versenden-empfangen-von-e-mails-in-deutschland/, zuletzt besucht: 23.04.2025.

[6] Vgl. Statista: *Anteil der Nutzer von Online- bzw. Mobile Banking in Deutschland in den Jahren von 1998 bis 2024.* 11.09.2024. https://de.statista.com/statistik/daten/studie/3942/umfrage/anteil-der-nutzer-von-online-banking-in-deutschland-seit-1998/, zuletzt besucht: 23.04.2025.

[7] Vgl. Wintergerst, Dr. R. 28.08.2024. *Wirtschaftsschutz 2024*. Bitkom Research 2024.

1 Cybercrime im engeren Sinne

1.1 Entwicklung der Fallzahlen

1.1.1 Fallzahlen Cybercrime im engeren Sinne

Im Jahr 2024 wurden 22 842 (21 181) inländische Fälle von Cybercrime im engeren Sinne erfasst. Die Anzahl der Auslandsstraftaten sank im gleichen Zeitraum von 36 792 im Jahr 2023 auf 35 281 Fällen im Jahr 2024. Insgesamt stieg die Gesamtzahl der in Nordrhein-Westfalen erfassten Fälle von Cybercrime im engeren Sinne von 57 973 im Jahr 2023 auf 58 123 im Jahr 2024. Die häufigsten Delikte waren der Computerbetrug gemäß § 263a StGB, das Ausspähen von Daten gemäß § 202a StGB und die Fälschung beweiserheblicher Daten gemäß § 269 StGB. Den größten Anstieg der Fallzahlen gab es im Bereich des Computerbetruges mittels rechtswidrig erlangter Daten von Zahlungskarten gemäß § 263a StGB um 1 592 auf 11 397 (9 805) im Jahr 2024.

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
2024	58 123	0,3	8 617	14,8

Abbildung 1:
Vergleich Fallzahlen Cybercrime im engeren Sinne

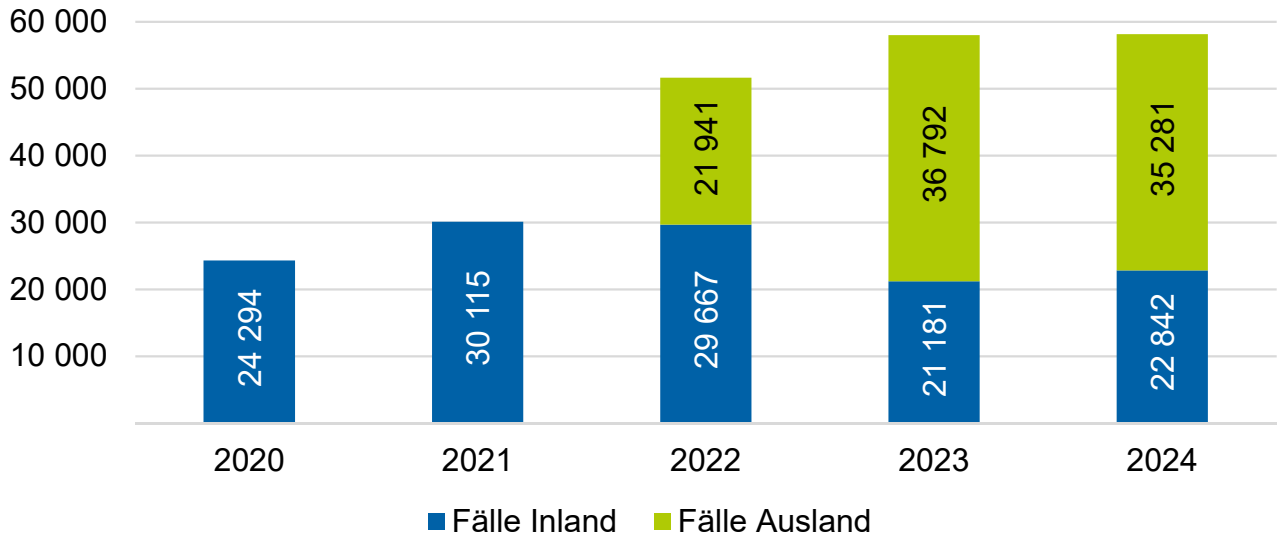


Tabelle 2:
Fallzahlen in einzelnen Deliktsfeldern der Cybercrime im engeren Sinne (Inland)

Delikt	2023	2024	Zu-/ Abnahme	Veränderung in %
Computerkriminalität (Cybercrime im engeren Sinne)	21 181	22 842	1 661	7,8
Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei der Datenverarbeitung §§ 269, 270 StGB	2 300	2 934	634	27,6
Datenveränderung, Computersabotage §§ 303a, 303b StGB	390	561	171	43,8
Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen und Datenhehlerei §§ 202a, 202b, 202c, 202d StGB	1 976	2 622	646	32,7
Computerbetrug § 263a StGB	16 515	16 725	210	1,3
Betrügerisches Erlangen von Kfz § 263a StGB	12	20	8	66,7
Weitere Arten des Warenkreditbetruges § 263a StGB	3 644	3 432	- 212	- 5,8
Computerbetrug mittels rechtswidrig erlangter Zahlungskarten mit PIN § 263a StGB	4 171	3 918	- 253	- 6,1
Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten § 263a StGB	3 308	3 504	196	5,9
Computerbetrug mittels rechtswidrig erlangter sonstiger unbarer Zahlungsmittel § 263a StGB	1 533	1 782	249	16,2
Leistungskreditbetrug § 263a StGB	452	460	8	1,8
Computerbetrug (sonstiger) § 263a StGB	3 097	3 403	306	9,9
Missbräuchliche Nutzung von Telekommunikationsdiensten § 263a StGB	48	10	- 38	- 79,2
Abrechnungsbetrug im Gesundheitswesen § 263a StGB	6	3	- 3	- 50,0
Überweisungsbetrug § 263a StGB	244	193	- 51	- 20,9

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

Delikt	2023	2024	Zu-/ Abnahme	Veränderung in %
Computerkriminalität (Cybercrime im engeren Sinne)	36 792	35 281	- 1 511	- 4,1
Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei der Datenverarbeitung §§ 269, 270 StGB	5 947	4 446	- 1 501	- 25,2
Datenveränderung, Computersabotage §§ 303a, 303b StGB	3 070	3 084	14	0,5
Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen und Datenhehlerei §§ 202a, 202b, 202c, 202d StGB	8 187	8 221	34	0,4
Computerbetrug § 263a StGB	19 588	19 530	- 58	- 0,3
Betrügerisches Erlangen von Kfz § 263a StGB	0	1	1	100,0
Weitere Arten des Warenkreditbetruges § 263a StGB	3 752	3 208	- 544	- 14,5
Computerbetrug mittels rechtswidrig erlangter Zahlungskarten mit PIN § 263a StGB	295	146	- 149	- 50,5
Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten § 263a StGB	6 497	7 893	1 396	21,5
Computerbetrug mittels rechtswidrig erlangter sonstiger unbarer Zahlungsmittel § 263a StGB	1 596	1 598	2	0,1
Leistungskreditbetrug § 263a StGB	714	788	74	10,4
Computerbetrug (sonstiger) § 263a StGB	6 306	5 631	- 675	- 10,7
Missbräuchliche Nutzung von Telekommunikationsdiensten § 263a StGB	16	12	- 4	- 25,0
Überweisungsbetrug § 263a StGB	412	253	- 159	- 38,6

1.1.2 Aufklärungsquote (AQ) (In- und Ausland)

Von den im Jahr 2024 erfassten Straftaten der Cybercrime im engeren Sinne wurden 8 617 (9 496) aufgeklärt. Die Aufklärungsquote liegt mit 14,8 % (16,4 %) unter dem Vorjahresniveau. Im Bereich des Computerbetrugs wurden 6 291 (6 646) Fälle aufgeklärt. Dies entspricht einer Aufklärungsquote von 17,4 % (18,4 %).

Tabelle 4:
Aufklärungsquote (AQ) Inland und Ausland

Delikt	Aufgeklärte Fälle		Aufklärungs-quote		Zu-/Abnahme (AQ) %-Punkte[8]
	2023	2024	2023	2024	
Computerkriminalität (Cybercrime im engeren Sinne)	9 496	8 617	16,4	14,8	- 1,6
Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei der Datenverarbeitung §§ 269, 270 StGB	1 587	1 242	19,2	16,8	- 2,4
Datenveränderung, Computersabotage §§ 303a, 303b StGB	271	197	7,8	5,4	- 2,4
Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen und Datenhehlerei §§ 202a, 202b, 202c, 202d StGB	992	887	9,8	8,2	- 1,6
Computerbetrug § 263a StGB	6 646	6 291	18,4	17,4	- 1,1
Betrügerisches Erlangen von Kfz § 263a StGB	11	16	91,7	76,2	- 15,5
Weitere Arten des Warenkreditbetruges § 263a StGB	2 308	1 711	31,2	25,8	- 5,4
Computerbetrug mittels rechtswidrig erlangter Zahlungskarten mit PIN § 263a StGB	853	1 122	19,1	27,6	8,5
Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten § 263a StGB	793	894	8,1	7,8	- 0,2

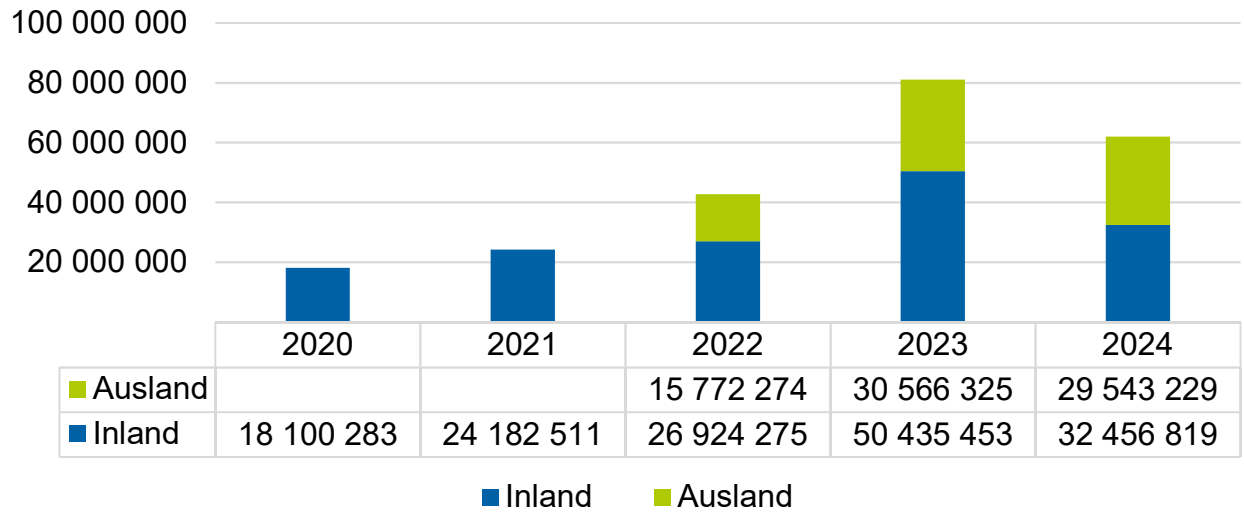
[8] Zur Darstellung von Entwicklungen in Prozentzahlen oder Prozentpunkten werden die exakten Werte zugrunde gelegt. Bei der Berechnung der gerundeten Werte kann es im Einzelfall zu Differenzen kommen

Computerbetrug mittels rechtswidrig erlangter sonstiger unbarer Zahlungsmittel § 263a StGB	498	535	15,9	15,8	- 0,1
Leistungskreditbetrug § 263a StGB	275	240	23,6	19,2	- 4,4
Computerbetrug (sonstiger) § 263a StGB	1 695	1 607	18,0	17,8	- 0,2
Missbräuchliche Nutzung von Telekommunikationsdiensten § 263a StGB	39	6	60,9	27,3	- 33,7
Überweisungsbetrug § 263a StGB	168	158	25,6	35,4	9,8

1.1.3 Schadenshöhe (In- und Ausland)

In der PKS NRW werden im Bereich Cybercrime ausschließlich für das Delikt Computerbetrug Schäden erfasst und abgebildet. Im Bereich der Erpressungsdelikte ist eine Differenzierung nach Erpressungen im Kontext mit Cybercrimedelikten nicht möglich. Der deutliche Anstieg der Schadenshöhe im Jahr 2023 ist auf einen Fall mit einer Schadenshöhe von 24 001 664 Euro zurückzuführen. Daher ist ein Vergleich zwischen den Jahren 2023 und 2024 nur eingeschränkt aussagekräftig. Ohne diesen herausragenden Schadensfall aus dem Jahr 2023 beträgt der Anstieg der Schadenshöhe auf 62 000 048 Euro für das Jahr 2024 8,8 %.

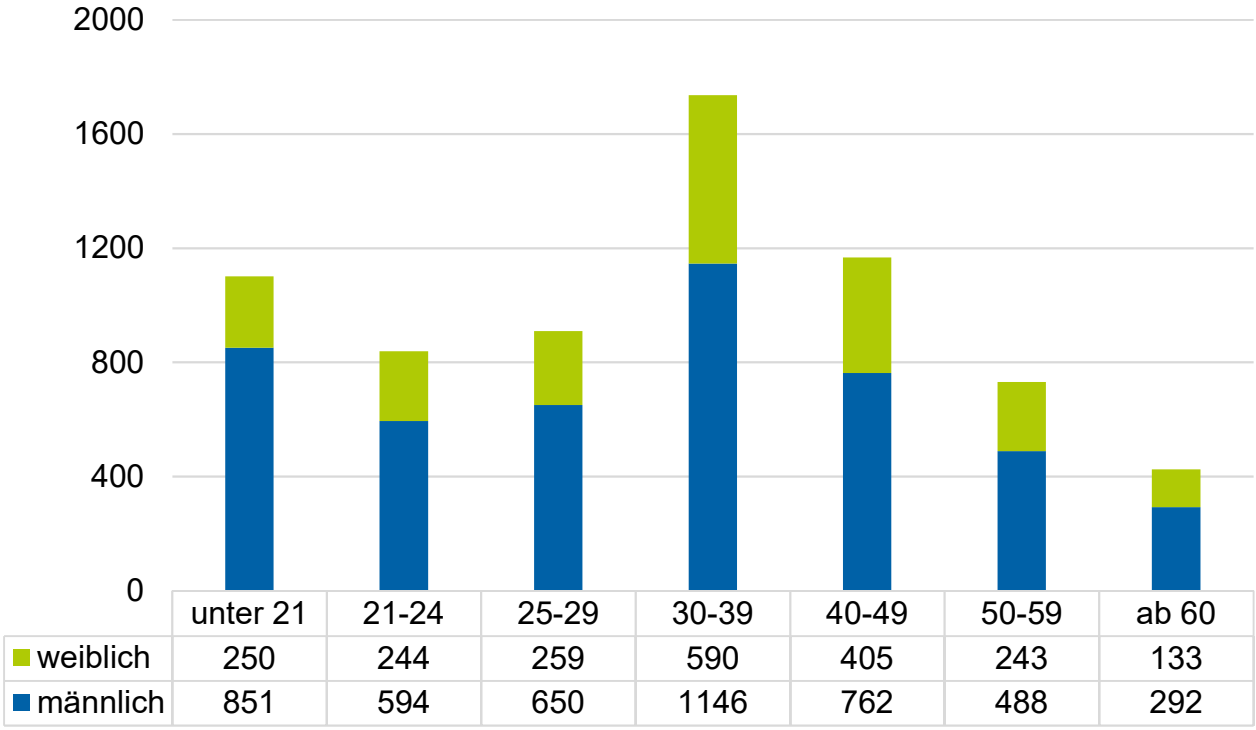
Abbildung 2:
Vergleich Schadensentwicklung Cybercrime in Euro (Inland und Ausland)



1.1.4 Tatverdächtige (Inland)

Im Jahr 2024 wurden 6 907 (7 062) Tatverdächtige ermittelt. Die männlichen Tatverdächtigen sind mit 4 783 oder 69,2 % (4 726) gegenüber den weiblichen Tatverdächtigen mit 2 124 (2 336) überrepräsentiert. Den größten Anteil mit 1 736 (1 840) macht die Gruppe der Erwachsenen im Alter von 30 bis 39 Jahren aus.

Abbildung 3:
Tatverdächtige Cybercrime nach Alter und Geschlecht (Inland)



	unter 21	21-24	25-29	30-39	40-49	50-59	ab 60
weiblich	250	244	259	590	405	243	133
männlich	851	594	650	1146	762	488	292

1.2 Darstellung ausgewählter Phänome

Grundlage für die Lagedarstellung sind die Daten der PKS NRW. Kriminalitätsphänomene und Modi Operandi können aus den PKS-Schlüsseln jedoch nicht abgeleitet werden, da sie nicht einem spezifischen PKS-Schlüssel entsprechen. So werden Phänomene begründeterweise mit verschiedenen PKS-Schlüsseln erfasst, weil unterschiedliche Tatbestände verwirklicht wurden. Zum Beispiel können bei einem Ransomware-Angriff, je nach Sachverhalt, die PKS-Schlüssel Datenveränderung (§ 303a StGB), Computersabotage (§ 303b StGB), Abfangen von Daten (§ 202b StGB) oder Erpressung (§ 253 StGB) zutreffend sein. In diesem Lagebild können erstmals Fallzahlen auch zu Kriminalitätsphänomenen dargestellt werden. Dies wurde durch eine Sonderauswertung mit der Unterstützung Künstlicher Intelligenz (KI) ermöglicht.

Ransomware

Ransomware-Angriffe stellen auch im Jahr 2024 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 Entschlüsselung 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 beziehungsweise 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. Bei Ransomware-Angriffen auf die IT-Infrastruktur von Krankenhäusern ist beispielsweise der komplette Krankenhausbetrieb gefährdet inklusive eines Risikos für Leib und Leben der Bevölkerung. 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 beziffern.

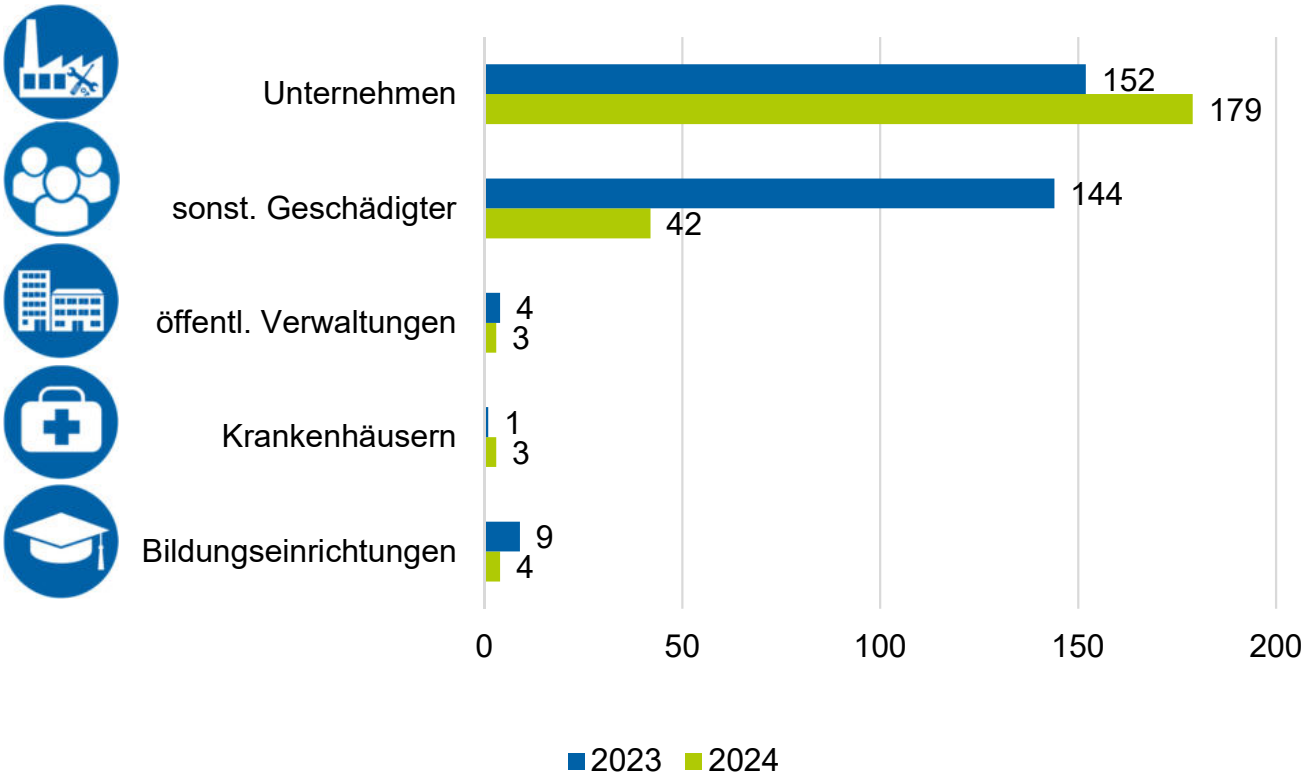
Bei einem Ransomware-Angriff dringen die Angreifer zunächst in das IT-Netzwerk ihrer Opfer ein, um in der Folge die Daten auf dem System zu verschlüsseln. In vielen Fällen geschieht der Ransomware Angriff als „Double Extortion“. Dazu werden im Vorfeld der Verschlüsselung Unternehmensdaten aus dem angegriffenen 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.

Im Falle einer „Triple Extortion“ wird zusätzlich zur „Double Extortion“ mit einem DDoS-Angriff (Distributed Denial of Service) gedroht, so dass die Internetpräsenz des betroffenen Unternehmens nicht mehr erreichbar ist. Mit der Drohung beabsichtigen die Täter das Unternehmen arbeitsunfähig zu machen und die Bereitschaft für eine größere Lösegeldforderung oder Zahlungsbereitschaft zu erwirken. Eine weitere Variante der „Triple Extortion“ ist die Erpressung Dritter, die mit dem betroffenen Unternehmen Geschäftsverbindungen pflegen und deren Daten die Täter erlangt haben. Dazu gehören Kunden, Interessengruppen oder Partner des betroffenen Unternehmens.

Die Täter gehören häufig Ransomware-Gruppierungen an, nutzen deren Support oder bieten ihre Software als Dienstleistung an (Cybercrime-as-a-Service). Im Jahr 2024 konnten durch Ermittlungen beim Phänomen Ransomware insgesamt 37 verschiedene Tatmittel (Schadsoftware) beziehungsweise Gruppierungen konkreten Fällen zugeordnet werden. Die Trennung zwischen der eingesetzten Schadsoftware und einer Gruppierung ist nicht immer gegeben. Ein eindeutiger Rückschluss auf eine Tätergruppierung ist trotz ermittelter Ransomware nicht immer möglich.

Abbildung 4:
TOP 6 der ermittelten Softwarevarianten/Gruppierungen

Abbildung 5:
Fallzahlen von Ransomware auf bestimmte Zielgruppen



(Distributed-) Denial-of-Service (DDoS-Angriff)

42
DDoS-Attacken

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 geplante 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 auch 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 kann nahezu jeder DDoS-Angriffe gegen Bezahlung in Auftrag geben, auch ohne tiefergehende Kenntnisse oder die IT-Infrastruktur selbst zu besitzen. Wird ein Angriff frühzeitig erkannt, können Gegenmaßnahmen eingeleitet werden, wie das Blockieren ausländischer IP-Adressen.

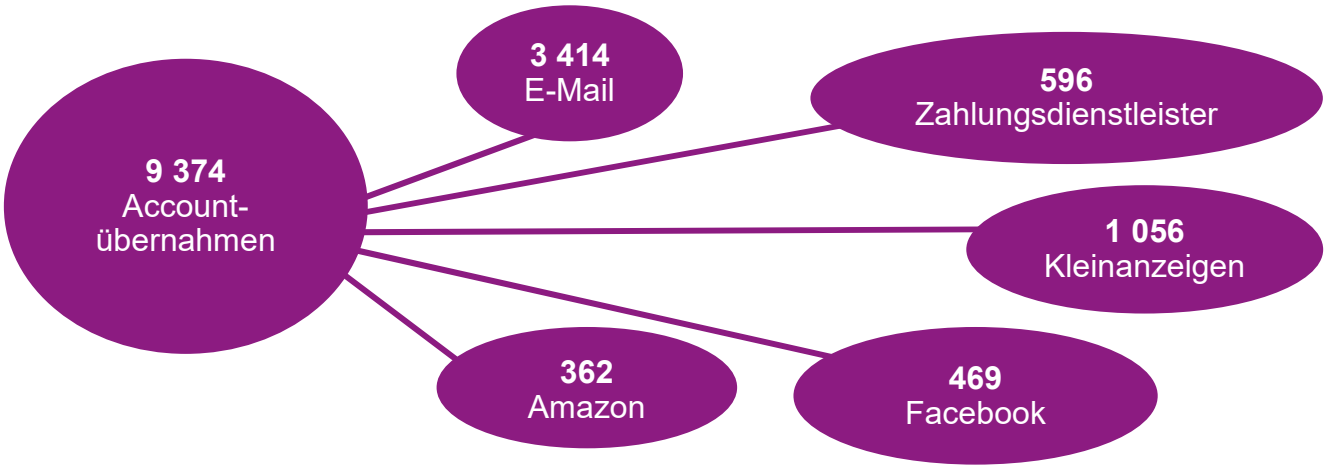
Der pro-russischen Hacktivistengruppe[9] NoName057 werden im Berichtszeitraum mehrere DDoS-Angriffe zugeordnet, darunter auch auf die Domain der Stadt Dortmund. Ziel des Angriffs war die Störung der Funktionen kommunaler Online-Dienste der Stadt. Die Bevölkerung war durch diesen Angriff direkt betroffen.

Weiteres Ziel der Gruppierung war das regionale Bahnunternehmen National Express. Durch DDoS-Angriffe war die Fahrplanauskunft und der Online-Ticketverkauf gestört.

Die Rheinmetall IT Solution GmbH war ebenfalls von Angriffen der Gruppierung im Berichtszeitraum betroffen, wodurch Störungen der IT-Systeme und Einschränkungen im Betriebsablauf erzeugt werden sollten.

Accountübernahme

In 9 374 Fällen wurden im Berichtszeitraum Accounts von Nutzern unbefugt übernommen. Oft wurden dabei von den Tätern die Zugangsdaten geändert, sodass die Geschädigten keinen Zugriff mehr auf ihren Account hatten. Die Zugangsdaten zu den Accounts können durch Phishing, Malware oder Datenkauf im Darknet erlangt worden sein, oft ist der Weg der Erlangung unbekannt. Übernommene Accounts werden benutzt, um Waren zu (ver)kaufen, Inhalte zu posten, E-Mails zu versenden oder Zahlungen zu tätigen/zu legitimieren.



Unter den TOP 5 der übernommenen Accounttypen stehen E-Mail Accounts an erster Stelle. In vielen Fällen werden mehrere Accounts bei einer Tat übernommen, weil Opfer dasselbe Passwort für mehrere Accounts verwenden. Die übrigen der 3 477 übernommenen Accounts betreffen Zahlungsdienstleister, andere soziale Netzwerke, Online-Shops, Gaming- und Streamingdienste.

Quishing

112 Fälle
Quishing

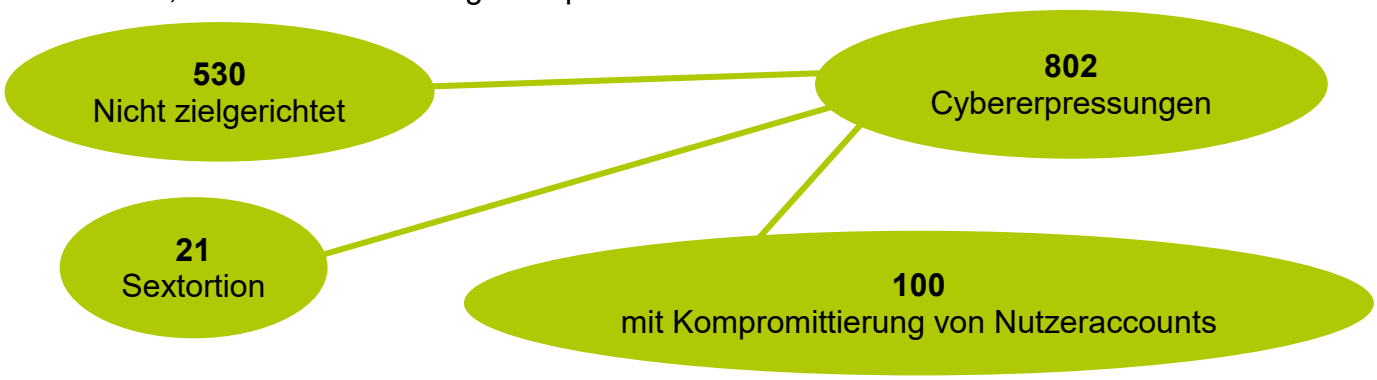
Quishing ist Phishing mit einem QR-Code. Der technische Ablauf ist ähnlich. Die Opfer scannen mit ihrem Smartphone den QR-Code und folgen einem dahinter befindlichen Link. Je nach Gerät und Browser ist auf den ersten Blick nicht erkennbar, dass die Opfer auf eine Fake-Seite geleitet werden und dort ihre persönlichen oder Zugangsdaten preisgeben. Ebenso kann beim Scannen Schadsoftware heruntergeladen werden. Die Täter nutzen die inzwischen weite Verbreitung von QR-Codes aus

[9] Hacktivismus vereint Konzepte des Hackings und des Aktivismus und beschreibt ideologisch, sozial und/oder politisch motivierte Aktionen unter Nutzung von Hackingtools.

und setzen sie unter anderem auf gefälschten Plakaten im öffentlichen Raum, auf täuschend echt wirkender Beklebung an Parkscheinautomaten oder E-Ladesäulen ein. Es erfordert höchste Aufmerksamkeit, die Manipulation zu erkennen.

Cybererpressung

In 802 Fällen wurden Nutzer Opfer von Cybererpressungen. Zu nicht zielgerichteten Erpressungen, in denen die Nutzer per E-Mail mit Standardtexten zu einer Geldzahlung aufgefordert werden und mit der Veröffentlichung privater/persönlicher Daten, Bilder oder Videos gedroht wird, kam es in 530 Fällen. In 21 Fällen kam es zu Sextortion-Erpressungen, bei denen ebenfalls mit der Veröffentlichung privater Bilder oder Videos gedroht wird. Allerdings bestand hier tatsächlich ein Kontakt zwischen den Geschädigten und dem Erpresser bei dem (intimes) Bild-/Videomaterial ausgetauscht wurde. Mit KI-basierten Verfahren ist es den Tätern möglich, unverfängliche Bilder, Bildfragmente oder wenig bewegte Bilder zu kompromittierendem Material zu verändern. In 100 Fällen fand vor der Erpressung eine Kompromittierung von Nutzeraccounts statt, womit die Geschädigten erpresst werden.



In 151 Fällen kam es zu sonstigen Erpressungen per E-Mail, die keiner der oben genannten Kategorien entsprechen.

Microsoft -Support

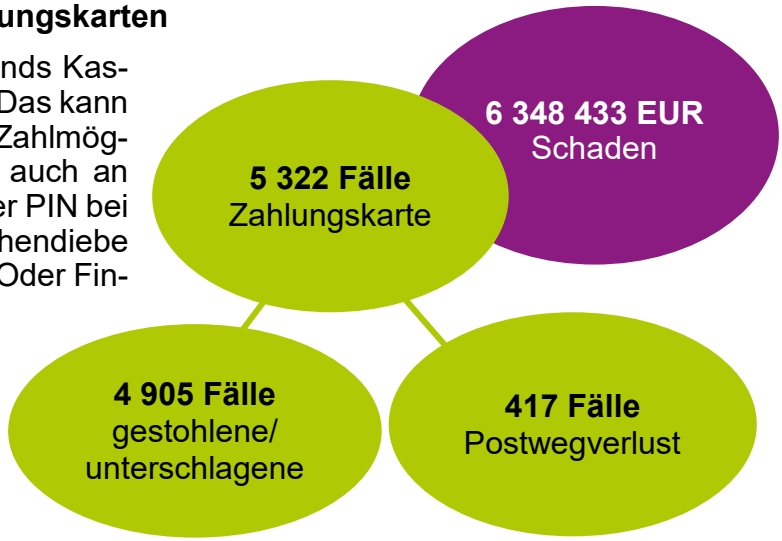
„Microsoft-Sicherheitsalarm, Fehler Nr. VD 0036! Ihr Computer hat uns alarmiert, dass er mit schädlichen Trojanern infiziert wurde. Diese Viren schicken ihre Kreditkartendaten, Facebook-LogIns sowie persönliche und private Daten über Remote-IP Adressen an Hacker weiter. Bitte rufen sie uns sofort unter der angegebenen kostenlosen Nummer an, damit unsere Microsoft-Support Ingenieure sie per Telefon durch den Lösungsvorgang führen können. Wenn sie diese Seite schließen, bevor sie uns anrufen, müssen wir ihren Computer deaktivieren, damit weitere Schäden an unserem Netzwerk verhindert werden. Außerdem werden wir eine Kopie dieses Berichts an die Netzsicherheit schicken, um weitere Schritte einzuleiten.“

Während der normalen Nutzung des Computers ertönt plötzlich eine Computerstimme und es erscheint ein Sperrbildschirm oder ein Pop-Up Fenster auf dem Bildschirm. Durch den Sperrbildschirm können die Opfer nichts anklicken, schließen oder den Computer auf herkömmlichen Weg herunterfahren. Den Opfern wird suggeriert, ihr Computer sei mit einem Computer-Virus infiziert worden und sie müssten schnell handeln, weil ihre Kredit- und Online-Banking Daten und damit ihr Geld in Gefahr seien und Hacker Zugriff auf ihren Computer hätten. Auf den Sperrbildschirmen wird zur Problembehebung eine deutsche Telefonnummer einer Ser-

vice-Hotline, eines Microsoft- oder Windows-Supports angegeben, die die Opfer anrufen sollen. Viele Opfer geraten in Panik darüber, dass der eigene Computer und das gesparte Geld nicht mehr sicher seien und blenden kritische Fragen nach der Echtheit des Hilfsangebots aus.

Ein angeblicher Service-Mitarbeiter leitet die Opfer am Telefon mit geschickter Gesprächsführung zum Herunterladen einer Fernwartungs-Software an. Über diese Fernwartungssoftware haben die Täter Fernzugriff auf den Computer der Opfer und können im Hintergrund sensible Daten einsehen, manipulieren und nutzen. Wenn ein Sperrbildschirm sich nicht wegklicken lässt und das herkömmliche Herunterfahren des Computers verhindert, hilft es in der Regel den Computer vom Internet zu trennen, den Router auszuschalten oder den Power-Button des Computers gedrückt zu halten und so das Herunterfahren zu erzwingen.

Gestohlene und unterschlagene Zahlungskarten



„Mit Karte, bitte!“ heißt es an Deutschlands Kassen mittlerweile häufiger als „Bar, bitte“. Das kann an der kontaktlosen und komfortablen Zahlmöglichkeit mittels NFC-Chips liegen, aber auch an der nicht mehr erforderlichen Eingabe der PIN bei kleineren Beträgen. Das nutzen Taschendiebe aus, indem sie Zahlungskarten stehlen. Oder Finder unterschlagen die verlorenen Karten und bezahlen damit im Einzelhandel oder an Automaten. Trotz zahlreicher Präventionskampagnen tragen noch immer viele die notierte PIN in der Nähe der Zahlungskarte bei sich, sodass die Täter mit der zusätzlich erlangten PIN erhebliche Summen im Geschäftsverkehr zahlen oder an Geldautomaten abheben können. Üblicherweise haften die Opfer in solch einem Fall selbst. Sobald der Verlust der Karte bemerkt wird, sollte die Zahlungskarte unverzüglich unter der folgenden Rufnummer gesperrt werden!

Sperr-Notruf: 116 116

Ein weiterer Modus Operandi, bei dem das Opfer aber zunächst keinerlei Kenntnis von dem Verlust und der missbräuchlichen Nutzung der Zahlungskarten erhält, ist der Diebstahl des Bankbriefs auf dem Postweg. Die Kriminellen kennen die Versandprozedur der Banken und versuchen den anschließend in einem ähnlichen Brief versendeten PIN ebenfalls abzufangen. Das Opfer erfährt häufig erst durch die Kontoumsätze von dem Diebstahl.

2 Cybercrime im weiteren Sinne

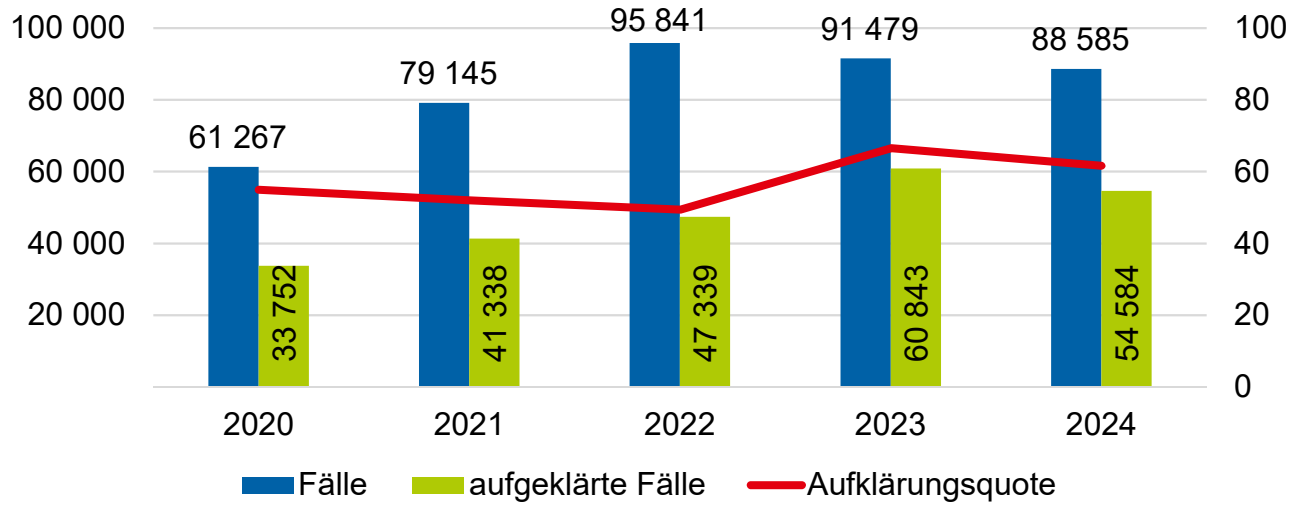
Cybercrime im weiteren Sinne umfasst alle Straftaten, die über das Internet erfolgen beziehungsweise die mithilfe digitaler Endgeräte begangen werden können und der Mensch unmittelbares Ziel des Angriffs ist. Es handelt sich um Straftaten, die auch in der analogen Welt begangen werden können, wie beispielsweise Beleidigung, Bedrohung, Enkeltrick inklusive deren Abwandlungen oder Waren- und Warenkreditbetrug. Im Jahr 2024 wurden 88 585 (91 479) Fälle Cybercrime im weiteren Sinne erfasst, 2 894 weniger als 2023. Den größten Anteil nahmen hierbei Betrugsdelikte mit 53 340 (53 441) Fällen ein. Die Aufklärungsquote sank auf 61,6 % (66,5 %). Es wurden 54 584 (60 843) Straftaten aufgeklärt.

Tabelle 5:
Entwicklung der Fallzahlen und Aufklärungsquoten der Cybercrime im weiteren Sinne

	2023	2024	Zu-/ Abnahme	Veränderung in %	AQ 2024 in %
Cybercrime im weiteren Sinne	**91 479**	**88 585**	**- 2 894**	- 3,2	61,6
Straftaten gegen die sexuelle Selbstbestimmung	13 796	8 750	- 5 046	- 36,6	81,3
Verbreitung pornografischer Inhalte (Erzeugnisse) gem. §§ 184ff. StGB	12 395	7 375	- 5 020	- 40,5	81,3
Verbreitung, Erwerb, Besitz und Herstellung kinderpornographphischer Inhalte gemäß § 184b StGB	9 519	5 630	- 3 889	- 40,9	80,6
Verbreitung von Kinderpornographie gemäß § 184b Abs. 1 Nr. 1 StGB	4 567	2 269	- 2 298	- 50,3	68,7
Bedrohung § 241 StGB	2 643	3 035	392	14,8	83,8
Nachstellung (Stalking) § 238 StGB	845	1 028	183	21,7	87,7
Waren- und Warenkreditbetrug	29 011	26 330	- 2 681	- 9,2	62,4
Kapitalanlage- und Anlagebetrug	309	652	343	111,0	25,3
Kontoeröffnungsbetrug	159	233	74	46,5	57,1
Sonstige weitere Betrugsarten	13 131	14 985	1 854	14,1	50,1
Erpressung § 253 StGB	1 029	1 773	744	72,3	49,6

Betreiben krimineller Handelsplattformen im Internet § 127 StGB	5	46	41	820,0	13,0
Beleidigung §§ 185-187, 189 StGB	5 069	5 458	389	7,7	76,1

Abbildung 6:
Vergleich Fallzahlen Cybercrime im weiteren Sinne



Erlangung von Bankdaten bei Online-Verkäufen

1 060 Fälle
Erlangung Bankdaten bei Online-Verkäufen

Auf Verkaufsplattformen wie eBay, Kleinanzeigen oder Vinted täuschen Täter Kaufabsichten vor, oft auch mit Hilfe übernommener Accounts von Dritten. Um das Geld für den vermeintlichen Kauf zu erhalten, sollen die Geschädigten ihre Bankverbindung angeben und werden dazu auf gefälschte, täuschend echt aussehende Webseiten geführt. Nach der Eingabe sensibler Zugangsdaten, Debit- oder Kreditkarteninformationen, werden sie von den Tätern für Bestellungen oder Zahlungen im Internet genutzt.

Missbrauch der Paypal-Bezahloption „Zahlen ohne Paypal-Konto“

Ein besonderer Modus Operandi der Warenkreditbetrugsdelikte ist das Phänomen „Zahlen ohne Paypal-Konto“. Dabei wählen die Kriminellen zunächst einen Onlineshop aus, der sowohl die Zahlungsart Paypal akzeptiert als auch die sogenannte „Gastzahlung“ anbietet. Bei Letzterer reicht die manuelle Eingabe einer IBAN – hier die unberechtigt genutzte IBAN der Opfer – sowie eines Namens, einer Anschrift und einer E-Mail-Adresse für den Bestellvorgang aus. Die dazu widerrechtlich benutzten Daten können von den Tätern im Vorfeld durch Phishing oder Datenkauf im Darknet erlangt worden sein. Ohne Überprüfung der angegebenen Daten zieht Paypal den Betrag per Lastschriftverfahren vom angegebenen Bankkonto ein.

3 Kinderpornografie

Im Jahr 2024 wurden für den Deliktsbereich „Verbreitung, Erwerb, Besitz und Herstellung kinderpornographischer Inhalte“ gemäß § 184b StGB 9 013 (10 728) Fälle erfasst. Dies entspricht einem Rückgang um 16,0 %, somit ergeben sich zum zweiten Mal in Folge sinkende Fallzahlen. Dennoch bleiben die Fallzahlen, wie im Vorjahr, auf einem hohen Niveau. Die Aufklärungsquote lag im Jahr 2024 mit 7 367 aufgeklärten Fällen bei 81,7 % (84,8 %).

Mit einer Anzahl von 5 630 Fällen und damit ein Anteil von 62,5 % nimmt das Internet als Tatmittel für den Deliktsbereich der Kinderpornografie weiterhin eine große Bedeutung ein, wenngleich der prozentuale Anteil im Vergleich zum Vorjahr (88,7 %) um 26,3 Prozentpunkte sank. Von den erfassten Fällen konnten 4 539 Taten und somit 80,6 % aufgeklärt werden, was einem Rückgang um 4,0 Prozentpunkte im Vergleich zum Vorjahr (84,6 %) entspricht.

Ein Großteil der Ermittlungsverfahren ist auf das Hinweisaufkommen durch die teilstaatliche US-amerikanische Organisation „National Center for Missing and Exploited Children“ (NCMEC) zurückzuführen. Nach Prüfung der strafrechtlichen Relevanz und erfolgversprechender Ermittlungsansätze durch das BKA, wurden dem LKA NRW im Jahr 2024 insgesamt 14 326 (12 169) Verdachtsfälle übermittelt. Damit erhöhte sich die Anzahl der in NRW eingegangenen Hinweise im Vergleich zum Vorjahr um 17,7 %. Der Anteil NRWs an der Gesamtzahl der NCMEC-Hinweise liegt weiterhin konstant bei 23,9 %. Die Hinweise werden nach Erstbearbeitung durch das LKA NRW über die Zentral- und Ansprechstelle Cybercrime der Staatsanwaltschaft Köln den örtlich zuständigen KPB NRW zu weiteren Ermittlungen zugeleitet.

Erstmals wurden den Ländern im Jahr 2024 vom BKA zusätzlich Hinweise übermittelt, die dort im Rahmen der Meldeverpflichtungen für Hostingdiensteanbieter nach dem Digital Services Act (DSA10) eingingen. Der DSA gilt für alle Diensteanbieter in der EU seit dem 17.02.2024. In NRW gingen seitdem 144 Meldungen ein.

Bei 51,0 % (41,8 %) aller bekannten Tatverdächtigen im Jahr 2024 handelt es sich um Kinder und Jugendliche.

Das bereits im letzten Jahr dargestellte Phänomen des massenhaften Hackings von Facebook-Accounts und anschließendem Hochladen von kinderpornografischen Dateien ist weiterhin feststellbar. Inzwischen sind auch Instagram-Accounts davon betroffen. Weitere Hacking-Phänomene betreffen im Jahr 2024 die Plattformen Reddit und X (ehemals Twitter). Hier wurden kompromittierte Internetanschlüsse unbeteiligter Dritter durch unbekannte Tätergruppierungen aus dem Ausland heraus zur Verbreitung von Missbrauchsabbildungen beziehungsweise zur „Werbung“ für Bildsammlungen mit inkriminierten Inhalten benutzt. Zu den Hintergründen der Hacking-Angriffe besteht weiterhin Unklarheit. Erkenntnisse zu diesen Phänomenen werden fortwährend gesammelt und ausgewertet.

[10] Der DSA als Teil der „Digitalstrategie für Europa“ zielt auf die „Schaffung eines sicheren, vorhersehbaren und vertrauenswürdigen Online-Umfelds […] ab. Rechtsgrundlage in Deutschland bildet hierfür das Digitale Daten Gesetzt (DDG). Mit dem DDG wurden neue Regeln für Online-Dienste geschaffen und Meldeverpflichtungen für Hostingdiensteanbieter festgeschrieben. Im Sinne des Art. 18 DSA fallen in Deutschland darunter z. B. DNS-Dienste, Netzwerkbetreiber, Cloud- und Webhosting-Dienste, Online-Plattformen (Soziale Medien, Marktplätze u. a.) sowie Online-Suchmaschinen [Quelle: BKA].

Seit dem 01.08.2024 wird landeszentral im LKA NRW die Recherchemöglichkeit der staatlichen us-amerikanischen Initiative „Internet Crimes Against Children (ICAC) Task Force Program“ genutzt. Die über die Homepage[11] zur Verfügung gestellten Informationen zu IP-Adressen wurden im Zusammenhang mit dem Download inkriminierter Dateien in Peer-to-Peer-Netzwerke identifiziert. Auf dieser Grundlage wurden im Jahr 2024 377 Strafanzeigen gefertigt und an die ZAC NRW übergeben.

4 Politisch motivierte Kriminalität begangen im Internet

4.1 Kriminalpolizeilicher Meldedienst - Politisch motivierte Kriminalität mit Tatmittel Internet

Im Jahr 2024 wurden 2 450 politisch motivierte Straftaten erfasst, die mit dem Tatmittel Internet begangen wurden. Das sind 22,7 % der gesamten Politisch motivierten Kriminalität und ist eine Steigerung um 31,8 % im Vergleich zum Vorjahr. In allen Phänomenbereichen der PMK ist ein deutlicher Anstieg der Fallzahlen im Vergleich zum Vorjahr zu verzeichnen.

Abbildung 7:
PMK mit Tatmittel Internet

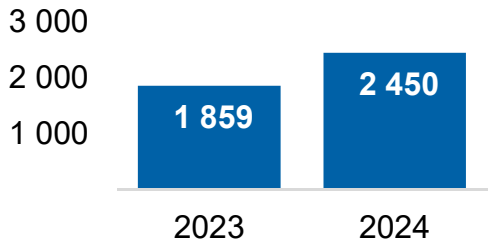
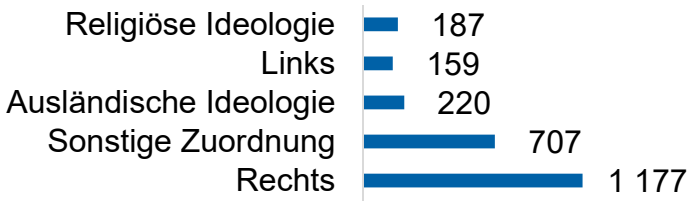


Abbildung 8:
Phänomenbereiche der PMK mit Tatmittel Internet 2024

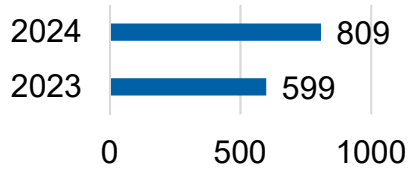


[11] https://www.icaccops.com

Hasskriminalität:

Hasskriminalität im Internet charakterisiert sich durch die Einschüchterung Andersdenkender sowie die Verbreitung und Förderung extremistischer Ideologien und führt zur deutlich wahrnehmbaren Verrohung der Kommunikation im digitalen Raum, bei der die Grenze zur Meinungsfreiheit überschritten und Rechte anderer verletzt werden. Social-Media-Anwendungen bieten weiträumige und schnelle Verbreitungswege für „Hasspostings“. Urheber von Hasspostings fühlen sich in ihrer scheinbaren Anonymität bestärkt, verbotene Inhalte, wie verbotene Kennzeichen, Volksverhetzungen, Beleidigungen, Bedrohungen oder sogar Mordaufrufe zu posten. Amts- und Mandatsträger sind seit der Corona-Pandemie vermehrt Anfeindungen und Angriffen im virtuellen Raum ausgesetzt. Betroffen sind Bundestags- und Landtagsabgeordnete, sowie Lokalpolitiker und Personen, die sich zivilgesellschaftlich engagieren.

Abbildung 9:
Hasskriminalität mit Tatmittel Internet



Hasskriminalität

Der Hasskriminalität werden Straftaten zugeordnet, wenn in Würdigung der Umstände der Tat und/oder der Einstellung des Täters Anhaltspunkte dafür vorliegen, dass sie gegen eine Person wegen ihrer Nationalität, ethnischen Zugehörigkeit, Hautfarbe, Religionszugehörigkeit, des sozialen Status, physischer und/oder psychischer Behinderung oder Beeinträchtigung, ihres Geschlechts/ geschlechtlichen Identität, der sexuellen Orientierung oder aufgrund ihres äußerlichen Erscheinungsbildes gerichtet sind.

Hasskriminalität im Internet wird durch die Polizei NRW konsequent strafrechtlich verfolgt.

Das Internet stellt keinen rechtsfreien Raum dar.

4.2 Cyberspionage, Cybersabotage, Desinformation, Hacktivismus

Durch die globalen Auswirkungen des russischen Angriffskrieges gegen die Ukraine und der Eskalation des Nahostkonflikts ist Cybercrime verstärkt im Kontext des polizeilichen Staatsschutzes festzustellen. Dabei können entsprechende Gruppierungen ausländischen Nachrichtendiensten direkt angegliedert oder unterstellt sein oder von diesen für ihre Zwecke genutzt und finanziert werden. Cyberangriffe zur politischen, wirtschaftlichen, wissenschaftlichen und militärischen Spionage dienen der klassischen Informationsgewinnung, wie die auf deutsche Parteien vor der Europawahl 2024.

Zu Sabotagezwecken wird versucht, technische Abläufe von Unternehmen und Behörden der Kritischen Infrastruktur zu stören. Erfolgreiche Sabotageangriffe, beispielsweise auf Wasser- oder Stromversorger, haben große Wirkung auf das Sicherheitsempfinden der Bevölkerung und beanspruchen Ressourcen der Ermittlungsbehörden. Professionelles Vorgehen der Täter und Verschleiern digitaler Spuren erschweren die Ermittlungen. Für die Gerichtsverwertbarkeit müssen Nachweise für eine staatliche Steuerung erbracht werden, ein Kernelement polizeilicher Ermittlungen. Auf Grund der geopolitischen Lage ist weiterhin von einem Anstieg politisch motivierter Cybercrime auszugehen.

4.3 Kooperationen

Die Themen „Hasskriminalität“ und „Extremismus/Terrorismus im digitalen Raum“ wurden in den letzten Jahren durch Gesetzesinitiativen auf EU-Ebene vorangetrieben. Bei der Zentralen Meldestelle für strafbare Inhalte im Internet beim BKA, die seit dem 01.02.2022 in Betrieb ist, wurden Meldestrukturen der Bundesländer zentral zusammengeführt. Unter Einbindung von Kooperationspartnern wird so bundesweit konsequent gegen Hass und Hetze im Netz vorgegangen. Die Kooperation wirkt der zunehmenden Verrohung der Kommunikation in sozialen Netzwerken entgegen und verfolgt effektiv die dort begangenen Straftaten.

Seit 2017 wirkt die Staatsschutzabteilung des LKA NRW im Projekt „Verfolgen statt nur Löschen“ mit. Weitere Projektpartner sind die Zentral- und Ansprechstelle Cybercrime NRW der Justiz, die „Landesanstalt für Medien NRW“ sowie diverse Medienhäuser.

Das LKA NRW beteiligt sich seit 2016 außerdem an den mit großem Erfolg jährlich stattfindenden, bundesweiten „Aktionstagen zur Bekämpfung von Hasspostings im Internet“.

5 Prävention

5.1 Cybercrime im engeren Sinne

Die Cybersicherheitslage im Jahr 2024 ist sowohl für Unternehmen als auch für öffentliche Institutionen und Behörden weiterhin angespannt. Die zunehmende Digitalisierung und Vernetzung von Dienstleistungen und Verwaltungsvorgängen eröffnen neue Möglichkeiten. Gleichzeitig werden informationstechnische Systeme zu attraktiven Zielen von Cyberkriminellen und staatlich gelenkten Akteuren.

Die rasante Entwicklung im Bereich der KI bringt sowohl Chancen als auch Risiken mit sich. Während KI-gestützte Sicherheitslösungen dabei helfen, Cyberangriffe besser zu erkennen und abzuwehren, nutzen Angreifer zunehmend dieselbe Technologie für Cyberangriffe – beispielsweise durch automatisierte Phishingkampagnen, Deepfakes oder mit Hilfe von Künstlicher Intelligenz erstellter Schadsoftware. Cyberkriminalität bleibt ein lukratives Geschäft und wird von professionell agierenden Tätergruppierungen oder staatlich instruierten Akteuren gleichermaßen betrieben oder über das Darknet in Form von „Cybercrime-as-a-Service“ als Dienstleistung angeboten.

Im Zuge dessen steigen die Anforderungen an die Cybersicherheit und die Herausforderungen für die Polizei NRW im Bereich der Prävention in diesem Deliktsbereich sukzessive. Um diese Herausforderungen professionell bewältigen zu können, wurden umfassende Organisationsänderungen der Polizei NRW im Ermittlungsbereich Cybercrime vorgenommen und die Prävention von Cybercrime durch den Ausbau bestehender Kooperationsnetzwerke und den Fokus auf regionale kleine und mittelständische Unternehmen weiter akzentuiert.

5.1.1 Zuständigkeiten und Geltungsbereich

Auch bei der Prävention von Cybercrime unterscheidet die Polizei NRW zwischen Cybercrime im weiteren Sinne und Cybercrime im engeren Sinne. Die Prävention von Cybercrime im wei-

teren Sinne wird überwiegend durch die KPB NRW wahrgenommen und ist vor dem Hintergrund der vielfältigen Delikts- und Phänomenbereiche durch intensive Kooperationen geprägt. Das LKA NRW unterstützt diese insbesondere durch die Koordinierung überregionaler Präventionsmaßnahmen und durch die Entwicklung von Medien und Standards, die den KPB zur Verfügung gestellt werden.

Die Prävention im Bereich Cybercrime im engeren Sinne wird vor allem durch die Abteilung 4 des LKA NRW wahrgenommen. Das LKA NRW unterstützt im Rahmen von Sicherheitspartnerschaften überregional Unternehmen, kommunale Verbände, öffentliche Bildungseinrichtungen und steht allen Behörden für Fragen der Prävention im Bereich Cybercrime im engeren Sinne zur Verfügung.

5.1.2 Präventionsmaßnahmen im Jahr 2024

Die Prävention im Bereich Cybercrime wurde im Jahr 2024 maßgeblich durch den fortlaufenden Ausbau von Sicherheitspartnerschaften, gemeinsame Veranstaltungen, (Online-) Vorträge zur Awareness[12] und weiterer Aktivitäten im Rahmen der Sicherheitspartnerschaften zur Schärfung des Bewusstseins für Cybersicherheit geprägt. Die Präventionskampagne www.mach-dein-passwort-stark.de wurde auch im Jahr 2024 weiter fortgeschrieben.

Im Bereich Cybercrime im engeren Sinne arbeitet das LKA NRW weiterhin eng und vertrauensvoll in einem etablierten Kooperationsnetzwerk mit dem Bitkom und dem Voice – Bundesverband der IT-Anwender e. V. Seit 2017 bestehen gleichgelagerte Kooperationsvereinbarungen mit dem eco - Verband der Internetwirtschaft e. V. und dem Networker Nordrhein-Westfalen e. V. Seit Ende 2024 wird dieses Netzwerk durch eine verstärkte Zusammenarbeit mit der Allianz für Sicherheit in der Wirtschaft West e. V. erweitert, um insbesondere kleine und mittelständische Unternehmen in Nordrhein-Westfalen bei der Bewältigung eines Cyberangriffs zu unterstützen. Durch eine fortlaufende Erweiterung und Vertiefung der Zusammenarbeit mit den Kooperationspartnern trägt das LKA NRW nachhaltig zur Steigerung der Awareness und damit zur Erhöhung der Cyber-Resilienz von Unternehmen, öffentlichen Institutionen und Behörden bei.

Zahlreiche öffentlichkeitswirksame Veranstaltungen, in denen das LKA NRW über die Gefahren durch Cyberangriffe und Interventionsmaßnahmen und Hilfestellungen seitens der Polizei NRW aufklärt, waren auch im Jahr 2024 der Schwerpunkt im Bereich der Prävention. Gleichzeitig wurde die Zentrale Ansprechstelle Cybercrime für die Wirtschaft in Form einer Beratungs – und Koordinationsstelle für die Anliegen rund um Cybercrime für die nordrhein-westfälischen Unternehmen in die Präventionsarbeit mit aufgenommen und weitergeführt.

Anfang März 2024 wurde das Digitale Beratungs- und Präventionszentrum der Polizei NRW in Köln eröffnet, um den aktuellen Erfordernissen der polizeilichen Kriminalprävention gerecht zu werden. Auf einer Fläche von 160 Quadratmetern befindet sich ein umfassendes und modernes Beratungs- und Hilfsangebot zu verschiedenen Themen. Dieses hochmoderne Präventionszentrum bietet nicht nur Bürgerinnen und Bürgern die Möglichkeit, sich zur Prävention unterschiedlichster Deliktsbereiche beraten zu lassen, sondern auch Veranstaltungen zu Themen der Cybercrimeprävention durchzuführen und zu streamen. Im selben Jahr begann das

[12] Der Begriff Awareness heißt übersetzt Bewusstsein und Achtsamkeit.

LKA NRW damit, dort gemeinsam mit Kooperationspartnern, Veranstaltungen zu zentralen Themen der Cybersicherheit und Prävention durchzuführen.

Im September 2024 richtete das LKA NRW gemeinsam mit dem Kooperationspartner VOICE e.V. einen Sicherheitstag aus. Im Rahmen dieses Sicherheitstags konnten sich ca. 170 Gäste aus der Wirtschaft und Behörden in den Räumlichkeiten des LKA NRW zu aktuellen Entwicklungen im Bereich von Cyberangriffen, Cybersicherheit und Künstlicher Intelligenz informieren und durch die Netzwerkarbeit vor Ort die vertrauensvolle Zusammenarbeit in der Zukunft stärken. Darüber hinaus nimmt das LKA NRW regelmäßig an Fachmessen teil und war auch 2024 wiederholt Aussteller bei einem der wichtigsten Events in Deutschland im Bereich der Cybersicherheit, der Internet Security Messe it-sa in Nürnberg. Die Teilnahme erfolgt in der Partnerschaft mit fünf weiteren Landeskriminalämtern, welche an der Sicherheitskooperation Cybercrime mit dem Bitkom e.V. teilnehmen.

5.2 Cybercrime im weiteren Sinne

Online-Betrug und Identitätsdiebstahl sind aktuell verbreitete Kriminalitätsphänomene. Das zeigt die jährliche Bürgerbefragung[13] zur Cyber-Sicherheit „Cybersicherheitsmonitor“, die im Auftrag des Bundesamtes für Sicherheit in der Informationstechnik ~~(BSI)~~ und des Programms Polizeiliche Kriminalprävention der Länder und des Bundes durchgeführt wurde.

Zur Fußball-Europameisterschaft 2024 wurde mit dem Artikel „Rote Karte: Vorsicht vor Fakeshops“ auf der Internetseite des LKA NRW www.mach-dein-passwort-stark.de vor betrügerischen Internetseiten im Zusammenhang mit dem Verkauf von Tickets und EM-Artikeln gewarnt. In Zusammenarbeit mit dem BSI erfolgte zum Thema Identitätsdiebstahl die Beteiligung an dem Podcast „Update verfügbar“[14] (#49 – Alarmstufe Rot für private Daten – Schutz vor Identitätsdiebstahl). Der Podcast gibt Internetnutzerinnen und -nutzern regelmäßig Tipps zur Cybersicherheit im digitalen Alltag.

[13] Vgl. Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK): *Cybersicherheitsmonitor 2024*. https://www.polizei-beratung.de/themen-und-tipps/gefahren-im-internet/cymon/. Zuletzt besucht: 23.04.2025.

[14] Vgl. Bundesamt für Sicherheit in der Informationstechnik: *Podcast ‘Update verfügbar‘: #49-Alarmstufe Rot für private Daten-Schutz vor Identitätsdiebstahl*. https://www.bsi.bund.de/SharedDocs/Audio/DE/BSI/Update_verfuegbar_Folge49_2024_12_04.html. Zuletzt besucht: 23.04.2025.

Herausgegeben von:

Landeskriminalamt Nordrhein-Westfalen
Völklinger Straße 49
40221 Düsseldorf

Abteilung 4
Cybercrime Kompetenzzentrum

Dezernat 41

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

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

Titelfoto: Adobe Stock Polizei NRW
Stand: September 2025