POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

bürgerorientiert · professionell · rechtsstaatlich

Cybercrime
Lagebild NRW 2017

Kriminalitätsentwicklung im Überblick

> Leichter Anstieg der Fallzahlen für den Bereich der Computerkriminalität

> Rückgang der Fälle von

- Datenveränderung/Computersabotage
- Missbrauch von Telekommunikationsdiensten
- Erpressungen mit Tatmittel Internet

> Anstieg der Betrugsdelikte

> Höchste Aufklärungsquote der letzten 10 Jahre

> Anstieg der Schadenssumme

	2016	2017	Veränderung in %
Computerkriminalität	22 708	22 913	+ 0,9
Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei der Datenverarbeitung	1 879	2 153	+ 14,6
Datenveränderung/Computersabotage	1 764	1 408	- 20,2
Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen	3 215	2 893	- 10,0
Computerbetrug	15 799	16 321	+ 3,3
Straftaten mit Tatmittel Internet	57 241	60 064	+ 4,9
Betrug mit Tatmittel Internet	40 905	43 817	+ 7,1
Erpressung mit Tatmittel Internet	557	389	- 30,2
Anzahl der aufgeklärten Fälle mit Tatmittel Internet	33 499	37 042	+ 10,8

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Lagedarstellung

1.1 Vorbemerkung

Zur Cybercrime gerechnet werden Straftaten, die sich gegen das Internet, andere Datennetze und informationstechnische Systeme oder deren Daten richten oder die mittels dieser Informationstechnik begangen werden. Die Definition steht im Einklang mit internationalen Begriffsbestimmungen wie der Convention on Cybercrime des Europarats.[1]

Cybercrime im engeren Sinne sind Straftaten, bei deren Begehung Elemente der elektronischen Datenverarbeitung in den Tatbestandsmerkmalen enthalten sind. Dazu zählen:

> Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung §§ 269, 270 StGB

> Datenveränderung, Computersabotage §§ 303a, 303b StGB

> Ausspähen, Abfangen von Daten einschließlich Vorbereitungshandlungen gemäß §§ 202a, 202b, 202c StGB

> Datenhehlerei gemäß § 202d StGB

> Verletzung des Urheberrechtsgesetzes durch Softwarepiraterie (privates Handeln und gewerbsmäßiges Handeln)

> Computerbetrug gemäß § 263a StGB:

- weitere Arten des Warenkreditbetruges
- Computerbetrug mittels rechtswidrig erlangter Zahlungskarten mit PIN
- Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten.

Das Lagebild Cybercrime stellt vornehmlich die Entwicklung der Cybercrime im engeren Sinne in Nordrhein-Westfalen (NRW) dar. Die Daten basieren auf Ermittlungsverfahren der Polizei NRW, die nach einheitlichem Standard erhoben werden. Datenquelle der im Überblick dargestellten und in Tabelle 1 näher erläuterten Daten ist die Polizeiliche Kriminalstatistik (PKS). Einzelne Delikte, die mit Hilfe des Tatmittels Internet begangen werden, sind unter Nr. 1.7 gesondert dargestellt. Klammerwerte bei Zahlenangaben beziehen sich, soweit nicht anders angegeben, auf das Vorjahr. In einzelnen Phänomenbereichen ist von einem großen Dunkelfeld auszugehen, da der Polizei viele Straftaten nicht bekannt bzw. nicht zur Anzeige gebracht werden.

Der Kriminalpolizeiliche Sondermeldedienst Cybercrime ermöglicht eine differenziertere Auswertung zu einzelnen Delikten. Um neue Tatbegehungsformen der Cybercrime zeitnah zu erkennen, bietet der Sondermeldedienst den sachbearbeitenden Dienststellen auch die Möglichkeit, Straftaten über den Katalog hinaus zu melden, wenn

> zur Tatbegehung spezielles informationstechnisches Fachwissen auf Täterseite erforderlich ist

> Täter besondere Techniken zur konspirativen Kommunikation (z. B. Kryptografie[2] oder Steganografie[3]) nutzen

> eine bundesweite oder internationale Bedeutung bestehen könnte

> ein überdurchschnittlich hoher Schaden vorliegt

> ein neuer oder abweichender Modus Operandi festgestellt wird.

[1] Übereinkommen des Europarats über Computerkriminalität vom 23. November 2001 in Budapest
[2] Verschlüsselung von Daten
[3] Verborgene Speicherung oder Übermittlung von Informationen in einem Trägermedium (Container, z. Bsp. in Fotos).

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

Jahr	Erfasste Fälle	Zu-/Abnahme	aufgeklärte Fälle	Aufklärungsquote
2006	15 068	- 10,3 %	6 331	42,0 %
2007	15 467	+ 2,7 %	6 151	39,8 %
2008	13 604	- 12,0 %	4 717	34,7 %
2009	15 541	+ 14,2 %	4 989	32,1 %
2010	19 775	+ 27,2 %	5 710	28,9 %
2011	20 036	+ 1,3 %	4 877	24,3 %
2012	22 228	+ 10,9 %	4 704	21,2 %
2013	27 016	+ 21,5 %	4 518	16,7 %
2014	20 715	- 23,3 %	4 302	20,8 %
2015	16 645	- 19,6 %	4 393	26,4 %
2016	22 708	+ 36,4 %	7 297	32,1 %
2017	22 913	+ 0,9 %	8 210	35,8 %

Tabelle 2
Fallzahlen in einzelnen Deliktsfeldern der Cybercrime im engeren Sinne

Delikt	2016	2017	Zu-/Abnahme	Prozent
Betrügerisches Erlangen von Kfz § 263a StGB	26	5	- 21	- 80,77 %
Weitere Arten des Warenkreditbetruges § 263a StGB	4 062	6 169	+ 2 107	+ 51,87 %
Computerbetrug mittels rechtswidrig erlangter Zahlungskarten mit PIN § 263a StGB	3 827	2 771	- 1 056	- 27,59 %
Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten § 263a StGB	1 894	1 806	- 88	- 4,65 %
Computerbetrug mittels rechtswidrig erlangter sonstiger unbarer Zahlungsmittel § 263a StGB	432	504	+ 72	+ 16,67 %
Leistungskreditbetrug § 263a StGB	1 046	1 274	+ 228	+ 21,80 %
Computerbetrug (sonstiger) § 263a StGB (soweit nicht unter den Schlüsseln 511120, 511212, 516300, 516520, 516920, 517720, 517900, 518112 bzw. 518302 zu erfassen)	3 780	3 552	- 228	- 6,03 %
Computerbetrug (sonstiger) § 263a Abs. 1 und 2 StGB	3 714	3 459	- 255	- 6,87 %
Vorbereitung des Computerbetrugs § 263a Abs. 3 StGB	66	93	+ 27	+ 40,91 %
Missbräuchliche Nutzung von Telekommunikationsdiensten § 263a StGB	154	67	- 87	- 56,49 %

Delikt	2016	2017	Zu-/Abnahme	Prozent
Abrechnungsbetrug im Gesundheitswesen § 263a StGB	3	0	- 3	- 100,00 %
Überweisungsbetrug § 263a StGB	575	173	- 402	- 69,91 %
Computerbetrug insgesamt § 263a StGB	15 799	16 321	+ 522	+ 3,30 %
Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung §§ 269, 270 StGB	1 879	2 153	+ 274	+ 14,58 %
Fälschung beweiserheblicher Daten § 269 StGB	1 788	2 063	+ 275	+ 15,38 %
Täuschung im Rechtsverkehr bei Datenverarbeitung § 270 StGB	91	90	- 1	- 1,10 %
Datenveränderung, Computersabotage §§ 303a, 303b StGB	1 764	1 408	- 356	- 20,18 %
Datenveränderung	1 348	1 037	- 311	- 23,07 %
Computersabotage	416	371	- 45	- 10,82 %
Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen gem. §§ 202a, 202b, 202c StGB	3 215	2 893	- 322	- 10,02 %
Ausspähen von Daten gem. § 202a StGB	2 829	2 467	- 362	- 12,80 %
Abfangen von Daten gem. § 202b StGB	17	17	0	0 %
Vorbereiten des Ausspähens und Abfangens von Daten gem. § 202c StGB	369	355	- 14	- 3,79 %
Datenhehlerei gem. § 202d StGB[4]	-	54	+ 54	-
Softwarepiraterie (private Anwendung z. B. Computerspiele)	31	20	- 11	- 35,48 %
Softwarepiraterie in Form gewerbsmäßigen Handelns	20	118	+ 98	+ 490,00 %
Computerkriminalität insgesamt	22 708	22 913	+ 205	+ 0,9 %

[4] Die Datenhehlerei gem. 202d StGB wurde erstmalig in 2017 statistisch erfasst.

1.2 Verfahrensdaten

2017 wurden 22 913 Cybercrime-Fälle erfasst (22 708). Dies entspricht einer Steigerung von 0,9 Prozent gegenüber dem Vorjahr. Die Anzahl der ermittelten Tatverdächtigen verringerte sich auf 5 565 (5 790). Die am häufigsten vertretenen Delikte waren das Ausspähen von Daten gemäß § 202a StGB, die Fälschung beweiserheblicher Daten gemäß § 269 StGB und die unterschiedlichen Arten des Computerbetrugs gemäß § 263a StGB. Dabei entfielen auf die Fälle des Computerbetrugs in seinen verschiedenen Ausprägungen 71,2 Prozent aller unter Cybercrime erfassten Delikte.

.

1.3 Aufklärungsquote

Von den im Jahr 2017 erfassten Straftaten wurden 8 210 aufgeklärt. Die Aufklärungsquote lag bei 35,8 Prozent und erhöhte sich gegenüber 2016 um 3,7 Prozentpunkte. Damit wurde 2017 die höchste Aufklärungsquote der letzten zehn Jahre erreicht. Auf den Computerbetrug gemäß § 263a StGB entfielen 81,8 Prozent aller aufgeklärten Fälle der Cybercrime.

Abbildung 1
Vergleich Fallzahlen und Aufklärungsquoten

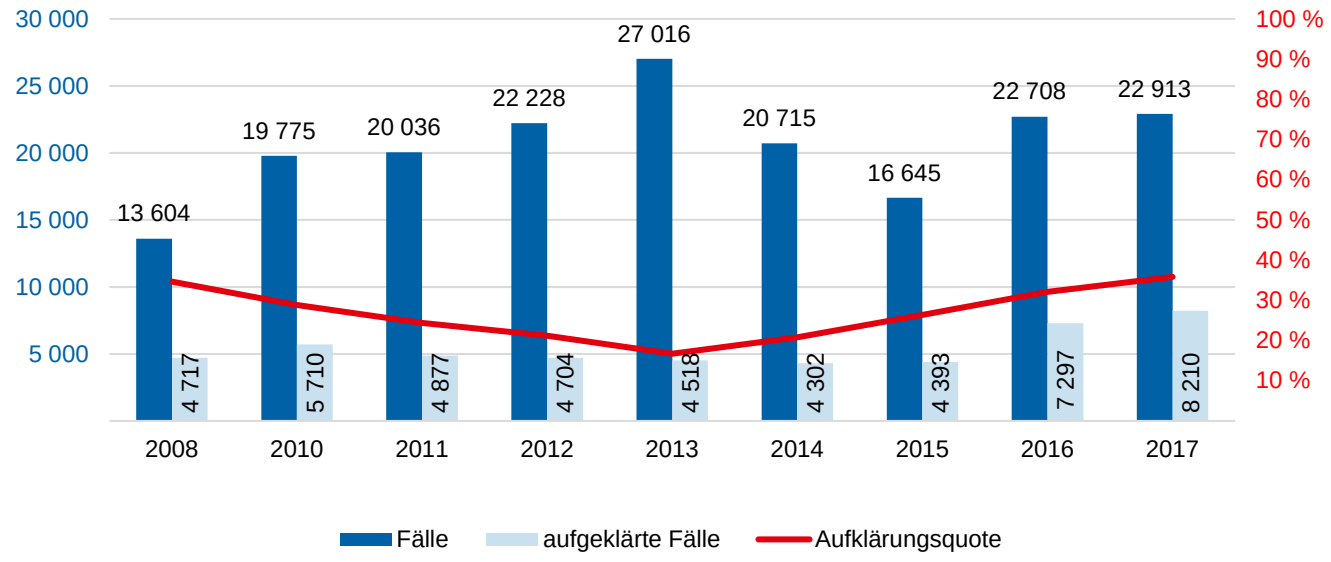


Tabelle 3
Aufklärungsquoten

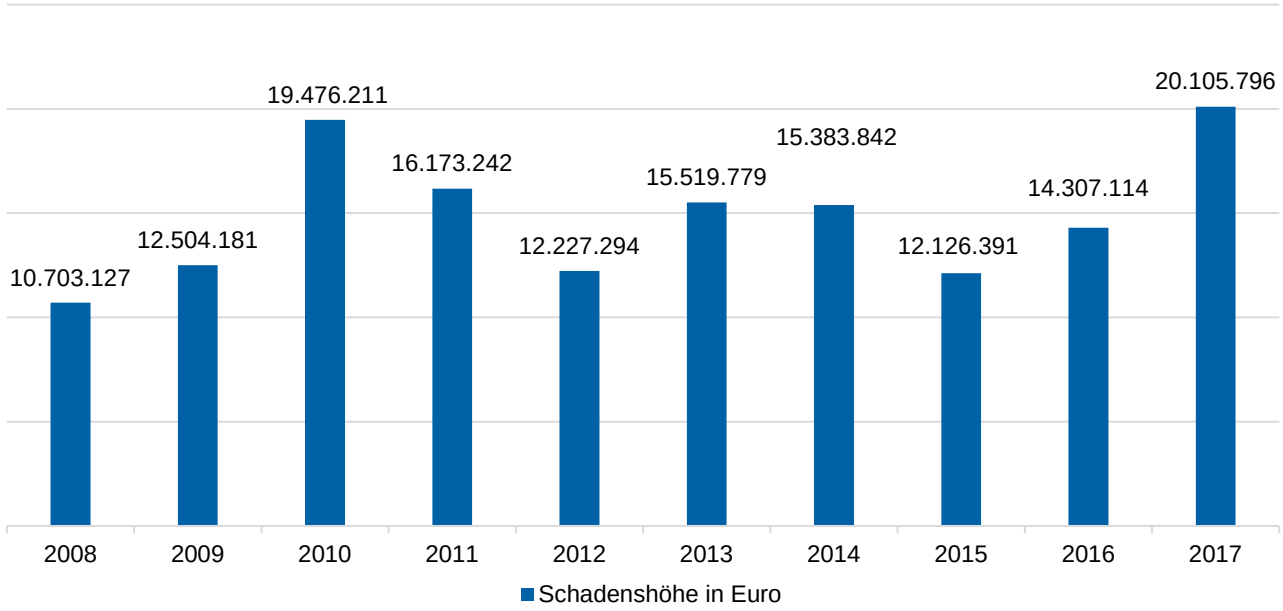
Delikt	Aufgeklärte Fälle		Aufklärungsquote		Zu-/Abnahme
	2016	2017	2016	2017	%-Punkte
Betrügerisches Erlangen von Kfz § 263a StGB	22	3	84,62 %	60,00 %	- 24,62
Weitere Arten des Warenkreditbetruges § 263a StGB	2 168	3 679	53,37 %	59,64 %	+ 6,27
Computerbetrug mittels rechtswidrig erlangter Zahlungskarten mit PIN § 263a StGB	1 205	921	31,49 %	33,24 %	+ 1,75
Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten § 263a StGB	777	558	41,02 %	30,90 %	- 10,12
Computerbetrug mittels rechtswidrig erlangter sonstiger unbarer Zahlungsmittel § 263a StGB	123	142	24,47 %	27,17 %	- 0,30
Leistungskreditbetrug § 263a StGB	331	332	31,64 %	26,06 %	- 5,58
Computerbetrug (sonstiger) § 263a StGB (soweit nicht unter den Schlüsseln 511120, 511212, 516300, 516520, 516920, 517720, 517900, 518112 bzw. 518302 zu erfassen)	1 190	1 000	31,48 %	28,15 %	- 3,33
Computerbetrug (sonstiger) § 263a Abs. 1 und 2 StGB	1 186	999	31,39 %	28,88 %	- 3,05
Vorbereitung des Computerbetrugs § 263a Abs. 3 StGB	4	1	6,06 %	1,08 %	- 4,98
Missbräuchliche Nutzung von Telekommunikationsdiensten § 263a StGB	33	9	21,43 %	13,43 %	- 8,00
Abrechnungsbetrug im Gesundheitswesen § 263a StGB	3	0	100,00 %	0	- 100,00
Überweisungsbetrug § 263a StGB	120	77	20,87 %	44,51 %	+ 23,64
Computerbetrug insgesamt § 263a StGB	5 972	6 721	37,80 %	41,18 %	+ 3,38
Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung §§ 269, 270 StGB	612	740	32,57 %	34,37 %	+ 1,8
Datenveränderung, Computersabotage §§ 303a, 303b StGB	198	241	11,22 %	17,12 %	+ 5,9
Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen gem. §§ 202a, 202b, 202c StGB	471	445	14,56 %	15,38 %	+ 0,82
Datenhehlerei gem. § 202d StGB[5]	-	13	-	24,07 %	+ 24,07
Softwarepiraterie (private Anwendung z. B. Computerspiele)	26	18	83,87 %	90,00 %	+ 6,13
Softwarepiraterie in Form gewerbsmäßigen Handelns	18	45	90,00 %	38,14 %	- 51,86

[5] Die Datenhehlerei gem. 202d StGB wurde 2017 erstmalig statistisch erfasst.

1.4 Schadensentwicklung

Schäden von Cybercrime werden in der PKS ausschließlich für Computerbetrug und die Softwarepiraterie abgebildet. Im Jahr 2017 erhöhte sich die Schadenssumme um 5.798.682 Euro auf 20.105.796 Euro. Sie stieg damit um 40,5 Prozent und erreicht nach 2010 einen erneuten Höchststand. Der Schaden beim Computerbetrug ist auf 17.070.328 Euro zu beziffern. Durch Softwarepiraterie entstand ein Schaden von 3.035.468 Euro. Bei einem einzigen Fall der Softwarepiraterie in Form gewerbsmäßigen Handels enstand ein Schaden von 2.400.000 Euro.

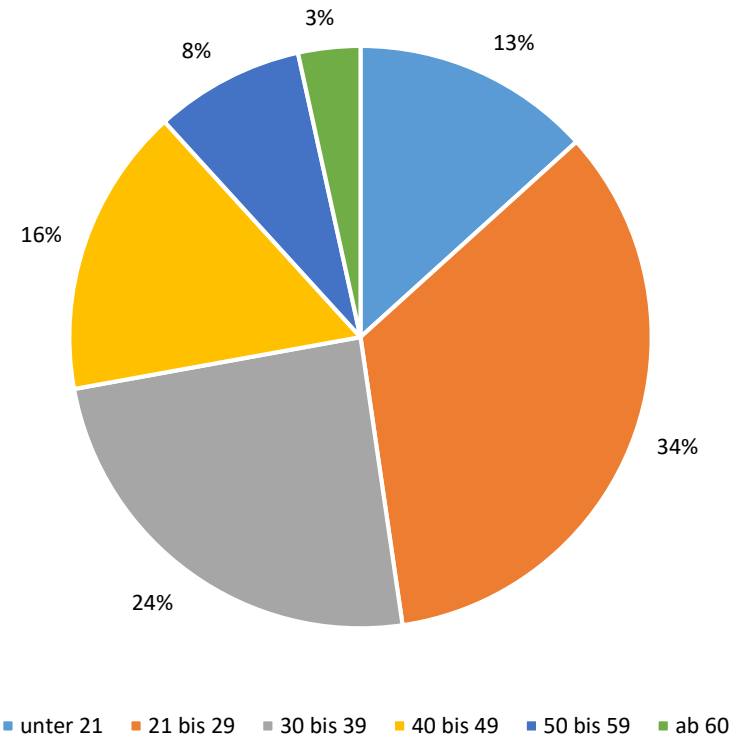
Abbildung 2
Schadensentwicklung



1.5 Tatverdächtige

Im Jahr 2017 konnten 5 565 (5 790) Tatverdächtige ermittelt werden. Den größten Anteil nahmen mit 23 Prozent die männlichen Tatverdächtigen im Alter von 21 bis 29 Jahre ein. Der Anteil tatverdächtiger Frauen betrug 34 Prozent.[6]

Abbildung 3
Tatverdächtige (Männer und Frauen gesamt)/Altersverteilung



[6] Weitere Informationen zu Tatverdächtigen können dem PKS-Jahrbuch 2017, Nr. 9.4 entnommen werden.

Tabelle 4
Entwicklung der Altersverteilung nach Tatverdächtigen

	Tatverdächtige								
	Unter 14		14 bis <18		18 bis <21		Ab 21		
Jahr	Anzahl	in %	Anzahl	in %	Anzahl	in %	Anzahl	in %	insgesamt
2006	46	1,3	396	11,5	420	12,2	2 589	75,0	3 451
2007	68	1,7	453	11,4	485	12,2	2 985	74,8	3 991
2008	61	1,6	383	10,2	457	12,1	2 849	76,0	3 750
2009	65	1,4	412	9,1	544	12,0	3 499	77,4	4 520
2010	87	1,8	472	9,7	636	13,1	3 671	75,4	4 866
2011	50	1,2	379	9,0	447	10,6	3 326	79,2	4 202
2012	64	1,7	298	7,9	410	10,9	2 981	79,4	3 753
2013	49	1,4	262	7,5	380	10,9	2 801	80,2	3 492
2014	40	1,2	201	5,8	341	9,8	2 880	83,2	3 462
2015	27	0,8	218	6,2	332	9,4	2 942	83,6	3 519
2016	23	0,4	263	4,5	557	9,6	4 947	85,4	5 790
2017	35	0,6	252	4,5	453	8,1	4 825	86,7	5 565

Tabelle 4
Entwicklung der Altersverteilung nach Tatverdächtigen - Fortsetzung

	Tatverdächtige												
	Unter 21		21 bis <30		30 bis <40		40 bis <50		50 bis <60		Ab 60		
Jahr	Anzahl	in %	Anzahl	in %	Anzahl	in %	Anzahl	in %	Anzahl	in %	Anzahl	in %	Insg.
2006	862	25,0	927	26,9	793	23,0	563	16,3	234	6,8	72	2,1	3 451
2007	1 006	25,2	1 020	25,6	820	20,5	714	17,9	337	8,4	94	2,4	3 991
2008	901	24,0	1 042	27,8	859	22,9	618	16,5	246	6,6	84	2,2	3 750
2009	1 021	22,6	1 264	28,0	979	21,7	798	17,7	336	7,4	122	2,7	4 520
2010	1 195	24,6	1 433	29,4	1 054	21,7	736	15,1	338	6,9	110	2,3	4 866
2011	876	20,8	1 348	32,1	925	22,0	666	15,8	291	6,9	96	2,3	4 202
2012	772	20,6	1 116	29,7	813	21,7	647	17,2	301	8,0	104	2,8	3 753
2013	691	19,8	1 018	29,2	779	22,3	607	17,4	276	7,9	121	3,5	3 492
2014	582	16,8	1 105	31,9	806	23,3	574	16,6	294	8,5	101	2,9	3 462
2015	577	16,4	1 116	31,7	855	24,3	525	14,9	334	9,5	112	3,2	3 519
2016	843	14,6	1 919	33,1	1 439	24,9	923	15,9	483	8,3	183	3,2	5 790
2017	740	13,3	1 914	34,4	1 361	24,5	896	16,1	462	8,3	192	3,5	5 565

1.6 Einzelne Deliktsfelder

Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei der Datenverarbeitung

Die Fallzahlen sind im Jahr 2017 (2 153) im Vergleich zum Vorjahr (1 879) um 14,58 Prozent angestiegen. Die Aufklärungsquote im Jahr 2017 betrug 34,37 Prozent. Im Vergleich zum Vorjahr (32,57 Prozent) ist dies eine Steigerung um 1,8 Prozentpunkte. Bei einem fünfjährigen Vergleichszeitraum sind die Fallzahlen um 31 Prozent gesunken. Die Aufklärungsquote ist im gleichen Zeitraum um 13,77 Prozentpunkte gestiegen. Sehr häufig wurden E-Mails verschickt, die täuschend echt real existierenden Banken, Zahlungsdienstleistern oder Online-Shops nachempfunden waren. Die ahnungslosen Opfer „klickten“ gutgläubig auf den darin enthaltenen Link und gelangten so auf fingierte Webseiten. Dort gaben sie ihre Zugangsdaten ein, die so in den Besitz der Täter gelangten.

Datenveränderung, Computersabotage

Die Fallzahlen sind im Jahr 2017 (1 408) im Vergleich zum Vorjahr (1 764) um 20,18 Prozent gesunken. Die Aufklärungsquote im Jahr 2017 betrug 17,12 Prozent. Im Vergleich zum Vorjahr (11,22 Prozent) ist dies eine Steigerung um 5,9 Prozentpunkte. Bei einem fünfjährigen Vergleichszeitraum sind die Fallzahlen um 79,03 Prozent gesunken. Die Aufklärungsquote ist im gleichen Zeitraum um 12,02 Prozentpunkte gestiegen.

Ausspähen, Abfangen von Daten einschließlich Vorbereitungshandlungen und Datenhehlerei

Die Fallzahlen sind im Jahr 2017 (2 893) im Vergleich zum Vorjahr (3 215) um 10,02 Prozent gesunken. Die Aufklärungsquote im Jahr 2017 betrug 15,38 Prozent. Im Vergleich zum Vorjahr (14,65 Prozent) ist dies eine Steigerung um 0,73 Prozentpunkte. Bei einem fünfjährigen Vergleichszeitraum sind die Fallzahlen um 47,27 Prozent gesunken. Die Aufklärungsquote ist im gleichen Zeitraum um 6,48 Prozentpunkte gestiegen. Die dominierenden Erscheinungsformen waren hier verschiedene Account[7]-Ausspähungen (z. B. digitale Identitäten, Benutzerkennungen, Kreditkarten- oder Kontodaten).

Computerbetrug

Die Fallzahlen sind im Jahr 2017 (16 321) im Vergleich zum Vorjahr (15 799) um 3,3 Prozent angestiegen. Die Aufklärungsquote im Jahr 2017 betrug 41,18 Prozent. Im Vergleich zum Vorjahr (37,80 Prozent) ist dies eine Steigerung um 3,38 Prozentpunkte. Bei einem fünfjährigen Vergleichszeitraum sind die Fallzahlen um 140,94 Prozent gestiegen. Die Aufklärungsquote ist im gleichen Zeitraum um 19,78 Prozentpunkte gestiegen. Damit stellte der Computerbetrug gemäß § 263a StGB in all seinen Facetten einen Anteil von 71,2 Prozent an der Computerkriminalität im engeren Sinne.

Weitere Arten des Warenkreditbetruges

Die Fallzahlen sind im Jahr 2017 (6 169) im Vergleich zum Vorjahr (4 062) um 51,87 Prozent angestiegen. Die Aufklärungsquote im Jahr 2017 betrug 59,64 Prozent. Im Vergleich zum Vorjahr (53,37 Prozent) ist dies eine Steigerung um 6,27 Prozentpunkte. Der starke Anstieg des Warenkreditbetrugs gemäß § 263a StGB dürfte insbesondere darauf zurückzuführen sein, dass Delikte, die in den letzten Jahren noch als „normaler“ Betrug gemäß § 263 StGB erfasst wurden, wegen der differenzierten Erfassungsmöglichkeiten nunmehr als Computerbetrug erfasst wurden. Für eine Verschiebung innerhalb der Erfassungsmöglichkeiten spricht auch der Rückgang um 2 702 Fälle beim Warenkreditbetrug gemäß § 263 StGB.

Computerbetrug mittels rechtwidrig erlangter Zahlungskarten mit PIN

Die Fallzahlen sind im Jahr 2017 (2 771) im Vergleich zum Vorjahr (3 827) um 27,59 Prozent gesunken. Die Aufklärungsquote im Jahr 2017 betrug 33,24 Prozent. Im Vergleich zum Vorjahr (31,49 Prozent) ist dies eine Steigerung um 1,75 Prozentpunkte. Bei einem fünfjährigen Vergleichszeitraum sind die Fallzahlen um 86,98 Prozent gestiegen. Die Aufklärungsquote ist im gleichen Zeitraum um 0,64 Prozentpunkte gestiegen. Grund für den Rückgang der Fallzahlen im Jahr 2017 dürfte sein, dass der Umgang mit Zahlungskarten und der Aufbewahrung der dazugehörigen PIN zunehmend verantwortungsbewusst erfolgt.

[7] Ein Benutzerkonto (englisch user account) ist eine Zugangsberechtigung zu einem zugangsbeschränkten IT-System. Üblicherweise muss ein Benutzer sich beim Einloggen mit Benutzernamen und Kennwort authentifizieren. (Quelle: https://de.wikipedia.org/wiki/Benutzerkonto, Stand: 10.04.2017)

Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten

Die Fallzahlen sind im Jahr 2017 (1 806) im Vergleich zum Vorjahr (1 894) um 4,67 Prozent gesunken. Die Aufklärungsquote im Jahr 2017 betrug 30,90 Prozent. Im Vergleich zum Vorjahr (41,02 Prozent) ist dies ein Rückgang um 10,12 Prozentpunkte. Zahlungskartendaten, die durch Phishing oder Skimming rechtswidrig erlangt wurden, wurden zum Teil im Internet eingesetzt, um Waren zu erhalten. Auch wurden die Daten genutzt, Karten aus Rohlingen herzustellen, um an Geldautomaten im außereuropäischen Ausland Geldverfügungen zu tätigen. Die Geschädigten erfuhren erst zeitversetzt bei Belastung ihrer Konten von dem Abfangen und dem Missbrauch ihrer Daten.

Computerbetrug mittels rechtswidrig erlangter sonstiger unbarer Zahlungsmittel

Die Fallzahlen sind im Jahr 2017 (504) im Vergleich zum Vorjahr (432) um 16,67 Prozent gestiegen. Die Aufklärungsquote im Jahr 2017 betrug 28,17 Prozent. Im Vergleich zum Vorjahr (28,47 Prozent) ist dies ein Rückgang um 0,30 Prozentpunkte. Unbare Zahlungsmittel sind u. a. PayPal-Konten, Guthabenkarten, Schecks oder Bonuskarten. In den meisten Fällen wurden Waren im Online-Handel bestellt und über ein zuvor gehacktes oder ausgespähtes PayPal-Konto bezahlt. Gerade durch die Beliebtheit in der Bevölkerung, PayPal als unbares Zahlungsmittel im Onlinehandel zu nutzen[8], ist hier eine stetige Steigerung zu beobachten.

Leistungskreditbetrug

Die Fallzahlen sind im Jahr 2017 (1 274) im Vergleich zum Vorjahr (1 046) um 21,80 Prozent gestiegen. Die Aufklärungsquote im Jahr 2017 betrug 26,06 Prozent. Im Vergleich zum Vorjahr (31,64 Prozent) ist dies ein Rückgang um 5,58 Prozentpunkte. Beim Leistungskreditbetrug erbringt der Verkäufer eine Leistung im Voraus. Der Täter bestellt diese Leistung über das Internet, z. B. beauftragt er das Erstellen einer Webseite. Mit dem Täter wird eine spätere Zahlung vereinbart. Der Täter hat jedoch von Anfang an nicht die Absicht zu zahlen. Oft werden frei erfundene Personalien oder die existierender Personen missbräuchlich genutzt.

Sonstiger Computerbetrug

Die Fallzahlen sind im Jahr 2017 (3 552) im Vergleich zum Vorjahr (3 780) um 6,03 Prozent gesunken. Die Aufklärungsquote im Jahr 2017 betrug 28,15 Prozent. Im Vergleich zum Vorjahr (31,48 Prozent) ist dies ein Rückgang um 3,33 Prozentpunkte.

Missbräuchliche Nutzung von Telekommunikationsdiensten

Die Fallzahlen sind im Jahr 2017 (67) im Vergleich zum Vorjahr (154) um 56,49 Prozent gesunken. Die Aufklärungsquote im Jahr 2017 betrug 13,43 Prozent. Im Vergleich zum Vorjahr (21,43 Prozent) ist dies ein Rückgang um 8 Prozentpunkte. Bei einem fünfjährigen Vergleichszeitraum sind die Fallzahlen um 3,08 Prozent gestiegen. Die Aufklärungsquote ist im gleichen Zeitraum um 6,97 Prozentpunkte gesunken. Immer noch steht die Manipulation von Telekommunikationsanlagen im Vordergrund. Durch die Ausnutzung von Sicherheitslücken oder unzureichender Zugangssicherungen können die Täter auf Router von Firmen oder Privatleuten zugreifen und so teure Verbindungen in das Ausland oder zu Mehrwertdiensten herstellen. Analog zur Reduzierung der Fallzahlen, sank die Schadenssumme auf 24.138 Euro (278.246 Euro).

Überweisungsbetrug

Die Fallzahlen sind im Jahr 2017 (173) im Vergleich zum Vorjahr (575) um 69,91 Prozent gesunken. Die Aufklärungsquote im Jahr 2017 betrug 44,51 Prozent. Im Vergleich zum Vorjahr (20,87 Prozent) ist dies eine Steigerung um 23,64 Prozentpunkte. Durch Einreichen einer ge- oder verfälschten Überweisung bzw. Zahlungsaufforderung wird dem kontoführenden Institut vorgetäuscht, der Kontoinhaber habe die Überweisung auf das Konto des Täters beauftragt. Erfolgt dieser Prozess automatisiert, erfüllt dies den Tatbestand des § 263a StGB. Die zunehmende Nutzung des Online-Bankings dürfte insbesondere zum deutlichen Rückgang der Fallzahlen beitragen.

[8] Gemäß eines Berichts der Wissenschaftlichen Dienste des Bundestages, welcher sich auf eine EHI-Studie „Online Payment 2016“ des EHI Retail Institute bezieht, lag der Anteil im Markt für physische Güter (inkl. E-Books) im Jahr 2015 bei 19,6 Prozent. Bei dieser Datengrundlage ist zu berücksichtigen, dass der Onlinehändler Amazon ebenfalls einen Bezahldienst anbietet. Bei Nichtberücksichtigung dieses Bezahldienstes käme Paypal auf einen Marktanteil von 24,5 Prozent.
https://www.bundestag.de/blob/434296/5dbc531d88cd738eccbe2e9b8079f1d1/wd-4-059-16-pdf-data.pdf

1.7 Tatmittel Internet

Straftaten, bei denen das Internet als Tatmittel wird, werden in der PKS mit der Sonderkennung „Tatmittel Internet“ erfasst. Es kommen sowohl Straftaten in Betracht, deren Tatbestände durch das bloße Einstellen von Informationen in das Internet bereits erfüllt werden (so genannte Äußerungs- bzw. Verbreitungsdelikte), als auch solche, bei denen das Internet zur Tatbestandsverwirklichung genutzt wird.

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.

2017 wurden 60 064 Fälle mit dem Tatmittel Internet erfasst, 2 823 mehr als 2016. Mit einer Aufklärungsquote von 61,7 Prozent wurden 37 042 Fälle aufgeklärt. Trotz eines Anstiegs der Aufklärungsquote ging die Anzahl der ermittelten Tatverdächtigen auf 21 689 (22 436) zurück. Den größten Anteil nahmen Betrugsdelikte mit 73 Prozent ein.

Abbildung 4
Tatmittel Internet

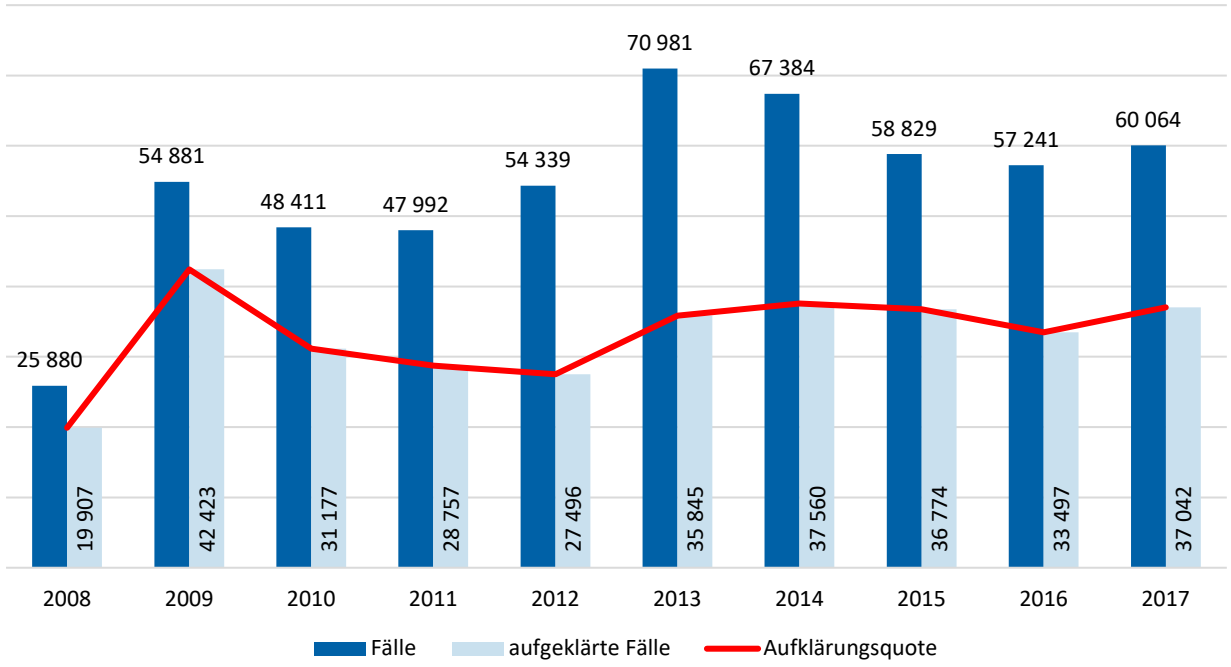


Tabelle 5
Tatmittel Internet

Straftaten	Gesamt-kriminalität 2017	darunter Tatmittel Internet Fälle	darunter Tatmittel Internet Anteil in %
Insgesamt	1 373 390	60 064	3,9
gegen die sexuelle Selbstbestimmung	12 886	1 796	13,9
Verbreitung pornografischer Schriften	2 011	1 501	74,6
Besitz/Verschaffen von Kinderpornografie	1 250	984	78,7
Verbreitung von Kinderpornografie	628	521	83,0
Betrug	228 491	43 817	19,2
Waren- und Warenkreditbetrug	78 618	32 534	41,4
Sonstiger Computerbetrug	3 552	2 542	71,6
Betrügerisches Erlangen von Kfz § 263a StGB	26	2	7,7
Weitere Arten des Warenkreditbetruges § 263a StGB	6 169	4 405	71,4
Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten § 263a StGB	1 806	1 211	67,1
Computerbetrug mittels rechtswidrig erlangter sonstiger unbarer Zahlungsmittel § 263a StGB	504	247	49,0
Leistungskreditbetrug § 263a StGB	1 274	848	66,6
Überweisungsbetrug § 263a StGB	575	42	7,3
Missbräuchliche Nutzung von Telekommunikations-diensten	67	17	25,4
Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung	2 153	1 400	65,0
Datenveränderung, Computersabotage	1 408	1 136	80,7
Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen	2 893	2 076	71,8
Erpressung	1 767	389	16,4
Überweisungsbetrug § 263a StGB	173	67	38,7

1.8 Kinderpornografie

Im Jahr 2017 wurden für den Deliktsbereich „Verbreitung, Erwerb und Besitz kinderpornografischer Schriften“ gemäß § 184b StGB 1 250 (1 025) Fälle erfasst. Dies entspricht einer Zunahme von 22 Prozent. In diesem Deliktsbereich besitzt das Internet eine herausragende Rolle. Bei 984 Fällen (78,7 Prozent) war das Internet Tatmittel. Hiervon konnten 85,3 Prozent aller Taten aufgeklärt werden.

Im Berichtszeitraum wurden allein von der halbstaatlichen US-amerikanischen Organisation „National Center for Missing and Exploited Children“ (NCMEC) 32 500 Verdachtsfälle an das BKA gemeldet. Der NCMEC gegenüber sind mehr als 700 US-amerikanische Provider per Bundesgesetz verpflichtet, strafrechtlich relevante Sachverhalte mitzuteilen. Nach Prüfung der strafrechtlichen Relevanz und erfolgversprechender Ermittlungsansätze wurden davon ca. 1 750 Fälle nach Nordrhein-Westfalen übermittelt und Ermittlungen aufgenommen.

Die übermittelten Daten beinhalteten in der Regel eine gute Beweislage, so dass aus den Verdachtsfällen ca. 770 Ermittlungsverfahren (300) resultierten.

Nach Schätzungen des Bundesministeriums der Justiz und für Verbraucherschutz liegt der Anteil der polizeilich nicht bekannten Straftaten im Bereich des sexuellen Missbrauchs von Kindern und Jugendlichen um ein achtfaches über den justizbekannten Taten. Bei Delikten der Kinderpornografie geht man ebenfalls von einem hohen Dunkelfeld aus.[9]

[9] Bundesministerium des Innern, Opferhilfe und Gewaltprävention, Themenbeitrag Präventionsnetzwerk „Kein Täter werden“, http://www.bmjv.de/DE/Themen/OpferschutzUndGewaltpraevention/KeinTaeterWerden/KeinTaeterWerden_node.html

2 Ausgewählte Phänomene

2.1 Identitätsdiebstahl

Name, Geburtsdatum, Adresse oder Bilder von Gesichtern sind Identitätsattribute, die den Einzelnen von anderen Individuen abgrenzen. Mit einem offiziellen Dokument kann jeder Mensch seine Identität nachweisen. Dies schafft Rechtssicherheit und Vertrauen auf allen Seiten.

Auch im digitalen Raum existieren Identitäten, die einer bestimmten Person zugeordnet werden können. Die Mehrheit der Menschen macht keinen Unterschied zwischen ihrer analogen und digitalen Identität. Genau das macht die digitale Identität zu einem begehrten „Diebesgut“ im Internet.

Onlinebanking und Online-Shops, Internetforen und soziale Netzwerke, selbst das Versenden und Empfangen einer E- Mail erfordern die Identifizierung des Nutzers. Meist geschieht dies durch die Kombination von Benutzername und Passwort. Der „Diebstahl“ und der Missbrauch persönlicher Daten sind ein lohnendes Geschäft für Cyber-Kriminelle. Digitalen Daten werden entweder selber zur Begehung von Straftaten benutzt oder über Plattformen der Underground Economy zum Verkauf angeboten.

Das Vorgehen der Täter zur Erlangung persönlicher Daten ist mannigfaltig. Gängige Methoden sind u.a. Phishing, Hacking, manipulierte Internetseiten oder das Versenden von schadhaften E-Mail Anhängen. Das Interesse gilt insbesondere Bankdaten und E-Mail-Konten aber auch Zugangsdaten zu Kommunikationsdiensten, Verkaufsplatt-formen, Sozialen Netzwerken oder Online-Spielen.

Regelmäßig starten Internet-Betrüger neue Phishing-Wellen. So werden Betroffene vom vermeintlichen Kundenservice ihrer Bank zum Ausfüllen eines neuen Formulars aufgefordert oder ein Online-Shop bittet um Aktualisierung der Kundendaten aufgrund eines neuen EU-Beschlusses.. Das Vorgehen der Betrüger ähnelt sich in vielen Fällen. Die Zeitpunkte der Angriffswellen liegen oft vor Feiertagen, zur Ferienzeit oder vor besonders verkaufstarken Tagen wie Ostern oder Weihnachten. In den E-Mails wird oftmals mit Sperrung des Benutzerkontos oder mit einer erhöhten Bearbeitungsgebühr gedroht, wenn Daten nicht bis zu einem bestimmten Termin versandt werden.

2.2 DDoS-Angriff

Bei DDoS[10]-Angriffen werden durch eine Vielzahl von Computern zielgerichtet Anfragen und Datenpakete auf Zielrechner bzw. -server gesendet. Dies führt zu einer Ressourcenerschöpfung des betroffenen Systems, das daraufhin nicht mehr erreichbar ist. Diese Angriffe stellen Unternehmen vor große Probleme, da sie bei einem erfolgreichen Angriff durch Einnahmenausfälle zum Teil erhebliche Verluste erfahren bzw. ihre Reputation als sicherer Handelspartner leidet.

[10]Distributed Denial of Service

Oftmals verüben Tätergruppierungen zunächst einen nur kurzzeitigen „Testangriff“. Im Anschluss wird ein Erpresserschreiben per E-Mail versendet. Darin wird angekündigt, von einem DDoS-Angriff abzusehen, falls ein vorgegebener Betrag in einer digitalen Währung gezahlt wird. In anderen Fällen wird auf ein Erpresserschreiben verzichtet und lediglich ein DDoS-Angriff verübt, um die Dienste des Betroffenen zu stören.

2.3 Malware

Unter Malware versteht man ein Computerprogramm, welches entwickelt wurde, um unerwünschte oder schädigende Funktionen auszuführen. Diese laufen häufig unbemerkt vom Benutzer im Hintergrund.

Ziel der Malware ist nicht selten das Ausspähen persönlicher Daten oder Kennwörter. Während in der Vergangenheit Malware oftmals mittels eines Anhangs einer E-Mail verbreitet wurde, besteht heutzutage die Gefahr, diese per Drive-by-Download herunterzuladen. Hierbei lädt der Nutzer unbewusst durch das bloße Aufrufen der Internetseite die Schadsoftware herunter. Diese wird dann ohne Wissen des Nutzers ausgeführt, befällt das jeweilige System und führt den Schadcode aus. Bei den Tätern steht oftmals eine wirtschaftliche Motivation im Vordergrund. Eine verbreitete Variante von Malware ist die Keylogger-Software. Diese zeichnet Tastatureingaben des Gerätebenutzers auf. Das Protokoll wird über das Internet an einen anderen Rechner geschickt. Ziel der Cyberkirminellen ist das Ausspähen von z. B. Benutzername, Passwörter oder Bankdaten.

2.4 Ransomware

Ransomware ist eine spezielle Malware, die Daten oder ganze Systeme verschlüsselt und den Zugriff darauf verhindert. Zur Freigabe wird die Zahlung eines Lösegeldes (engl.: ransom) gefordert.

Ransomware wird über Schadsoftware verbreitet, die in Anhängen von E-Mails verborgen ist. Die Verbreitung ist auch durch den schlichten Aufruf entsprechend programmierter Internetseiten möglich, dem sogenannten Drive-by-Exploit.

Die Fallzahlen der Datenveränderung und Computersabatogae sind im Vergleich zum Vorjahr rückgängig (2016: 1764 Fälle / 2017: 1408 Fälle).

3 Prävention

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

Bei der polizeilichen Präventionsarbeit stehen verhaltensorientierte Ansätze im Vordergrund. Diese werden durch Workshops, Vorträge oder Projekte verfolgt.

Bei der Prävention von Cybercrime wird zwischen Cybercrime im weiteren Sinn und Cybercrime im engeren Sinn getrennt. Während die Prävention von Cybercrime im weiteren Sinn (Tatmittel Internet) vollständig in der Hand der KPB liegt, deckt das LKA NRW mit dem Cybercrime-Kompetenzzentrum den Bereich der Cybercrime Prävention im engeren Sinn mit der Schwerpunktausrichtung Wirtschaftsunternehmen ab, aber auch Behörden und vergleichbare Institutionen sind Zielgruppe der Maßnahmen. Hierbei wird ein bewährtes Netzwerk unterschiedlichster Kooperationspartner wie dem Bitkom[11], dem Voice - Bundesverband der IT-Anwender und der Sicherheitspartnerschaft mit dem ASW NRW[12] bedient. Am 29.09.2017 unterzeichnete das LKA NRW gleichgelagerte Kooperationsvereinbarungen mit dem eco - Verband der Internetwirtschaft e.V. und dem networker NRW e.V. und fürte erste gemeinsame Veranstaltungen durch.

Durch die enge Zusammenarbeit werden unterschiedlichste Akteure als Multiplikatoren innerhalb der Wirtschaft mit den Präventionsbotschaften erreicht und für die Prävention von Cybercrime sensibilisiert. Hierbei werden unterschiedliche Formate wie Informationsstände, Vorträge, Teilnahme an Kongressen und Messen genutzt. Durch die Beteiligung an „Round Tables“ und die Zusammenarbeit in Regionalgruppen werden Berührungsängste zwischen Wirtschaft und Polizei abgebaut, so dass die Anzeigebereitschaft und das Bewusstsein für die durch Cybercrime bestehenden Gefahren (Awareness) gesteigert werden. Die Informations- und Wissensvermittlung umfasst neben den Möglichkeiten zum Schutz vor Angriffen auch die Sensibilisierung zur Notwendigkeit der Vorbereitung auf den „Ernstfall“. Potentiell Betroffene, die sich mit geplanten Reaktionsmustern und Notfallplänen wappnen, können erfolgreiche Angriffe deutlich besser abwehren, so dass geringere finanzielle Schäden entstehen oder ganz vermieden werden können.

Das LKA NRW sensibilisierte im Jahr 2017 durch Vorträge bei verschiedenen Veranstaltungen von Behörden und in der Wirtschaft zu den Gefahren durch Cybercrime. Mit Voice veranstaltete das LKA NRW einen gemeinsamen IT-Sicherheitstag, ebenso wie mit dem Bitkom und weiteren Landeskriminalämtern eine Fachtagung zur „Sicherheitskooperation Cybercrime“ gemeinsam ausgerichtet wurde. Durch die Kooperationen mit Bitkom und Voice konnten Präventionsbotschaften effizient einem großen Spektrum von Personen und Firmen zugänglich gemacht werden.

Der Besuch von Großveranstaltungen wie der CeBIT 2017, dem Deutschen Präventionstag 2017 und der protekt[13] in Leipzig wurde genutzt, um mit Vorträgen und Informationsständen die breite Öffentlichkeit zu erreichen.

Die Schnelllebigkeit und Komplexität des Deliktsbereichs erfordern, dass die Polizei auch künftig andere Akteure in die Bewältigung dieser Aufgabe einbinden muss.

[11] Bitkom - Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
[12] ASW Nordrhein-Westfalen - Allianz für Sicherheit in der Wirtschaft Nordrhein-Westfalen e.V.
[13] protekt - Konferenz und Fachausstellung für den Schutz Kritischer Infrastrukturen

Herausgeber

Landeskriminalamt Nordrhein-Westfalen
Völklinger Straße 49
40221 Düsseldorf

Abteilung 4
Cybercrime-Kompetenzzentrum
Dezernat 41

Redaktion: KR Dennis Boß
Telefon: +49 211 939-4100
Fax: +49 211 939-194100

Dez41.LKA@polizei.nrw.de
https://lka.polizei.nrw

Bildnachweis: Titelbild – santiago silver/fotolia.com