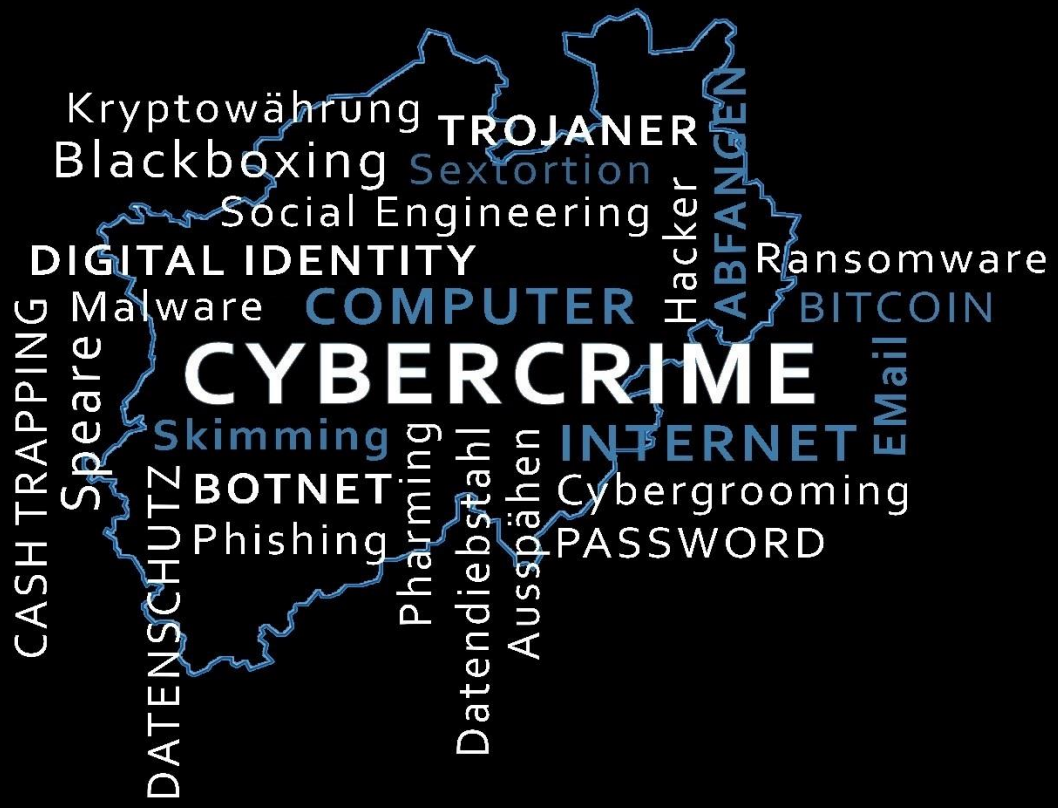
POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

bürgerorientiert · professionell · rechtsstaatlich



Cybercrime

Lagebild NRW 2021

Überblick Kriminalitätsentwicklung- Cybercrime

- Anstieg der Fallzahlen für den Bereich der Computerkriminalität (Cybercrime im engeren Sinne) um 23,96 Prozent.
- Anstieg der Fallzahlen bei Straftaten mit Tatmittel Internet (Cybercrime im weiteren Sinne) um 29,18 Prozent.
- Anstieg der Fallzahlen für den Deliktsbereich Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen und Datenhehlerei um 107,33 Prozent.
- Anstieg der Fallzahlen bei Betrug mit Tatmittel Internet um 13,80 Prozent.
- Anstieg der Fallzahlen bei Verbreitung, Erwerb, Besitz und Herstellung kinderpornografischer Schriften um 137,19 Prozent.

Inhaltsverzeichnis

1 Vorbemerkung

Cybercrime umfasst als Sammelbegriff 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 der Datenverarbeitung gemäß §§ 269, 270 StGB

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

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

> Datenhehlerei gemäß § 202d StGB

> Verletzung des Urheberrechtsgesetzes durch Softwarepiraterie[2] gemäß §§ 106 ff. UrhG (privates Handeln und gewerbsmäßiges Handeln)

> Computerbetrug gemäß § 263a StGB:

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

Cybercrime im weiteren Sinne bezeichnet Straftaten, bei denen die Informations- und Kommunikationstechnik zur Planung, Vorbereitung oder Ausführung eingesetzt wird.

[1] Übereinkommen des Europarats über Computerkriminalität vom 23. November 2001 in Budapest
[2] Die rechtswidrige Vervielfältigung und Verbreitung urheberrechtlich geschützter Software.

Die in Tabellen und Abbildungen aufgeführten Daten basieren auf der Polizeilichen Kriminalstatistik (PKS). Klammerwerte bei Zahlenangaben beziehen sich, soweit nicht anders angegeben, auf das Vorjahr.

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

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

- zur Tatbegehung spezielles informationstechnisches Fachwissen auf Täterseite erforderlich ist,
- Täter besondere Techniken zur konspirativen Kommunikation (z. B. Kryptografie[3] oder Steganografie[4]) nutzen,
- eine bundesweite oder internationale Bedeutung bestehen könnte,
- ein überdurchschnittlich hoher Schaden vorliegt,
- ein neuer oder abweichender Modus Operandi festgestellt wird.

Die Entwicklungen in diesem Kriminalitätsfeld im Jahr 2021 wurden durch die Corona-Pandemiesituation beeinflusst. Kurzarbeit, Quarantäne, die Betreuungssituation von Kindern, Homeoffice und andere pandemiebedingten Anpassungen bewirkten, dass große Teile der Bevölkerung bedeutend mehr Zeit mit der Nutzung von Onlinediensten verbrachten. Viele Geschäfte konnten ihre Waren und Dienstleistungen zeitweise nur online anbieten.

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

[3] Verschlüsselung von Daten
[4] Verborgene Speicherung oder Übermittlung von Informationen in einem Trägermedium (Container, z. B. in Fotos).

2 Lagedarstellung Cybercrime im engeren Sinne

2.1 Verfahrensdaten

2.1.1 Fallzahlen

2021 wurden 30 115 Cybercrime-Fälle erfasst. Dies entspricht einem Anstieg von 23,96 Prozent gegenüber dem Vorjahr (24 294). Die Anzahl der ermittelten Tatverdächtigen erhöhte sich um 17,23 Prozent auf 6 056. Die am häufigsten vertretenen Delikte waren der Computerbetrug gemäß § 263a StGB, die Fälschung beweiserheblicher Daten gemäß § 269 StGB und das Ausspähen von Daten gemäß § 202a StGB.

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

Jahr	Erfasste Fälle	Veränderung in %	aufgeklärte Fälle	Aufklärungsquote in %
2017	22 913	0,90	8 210	35,83
2018	19 693	-14,05	6 994	35,52
2019	20 118	2,16	5 911	29,38
2020	24 294	20,76	6 963	28,66
2021	30 115	23,96	8 020	26,63

Tabelle 2
Fallzahlen in einzelnen Deliktsfeldern der Cybercrime im engeren Sinne

Delikt	2020	2021	Zu-/Abnahme	Veränderung in %
Computerkriminalität (Cybercrime im engeren Sinne)	**24 294**	**30 115**	**5 821**	**23,96**
Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei der Datenverarbeitung §§ 269, 270 StGB	2 791	4 106	1 315	47,12
Datenveränderung, Computersabotage §§ 303a, 303b StGB	1 258	1 653	395	31,40
Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen und Datenhehlerei §§ 202a, 202b, 202c, 202d StGB	2 292	4 752	2 460	107,33
Softwarepiraterie (private Anwendung z.B. Computerspiele)	13	32	19	146,15
Softwarepiraterie in Form gewerbsmäßigen Handelns	6	7	1	16,67
Computerbetrug § 263a StGB	17 934	19 604	1 670	9,31
Betrügerisches Erlangen von Kfz § 263a StGB	10	10		0,00
Weitere Arten des Warenkreditbetruges § 263a StGB	6 257	6 888	631	10,08
Computerbetrug mittels rechtswidrig erlangter Zahlungskarten mit PIN § 263a StGB	2 583	3 356	773	29,93
Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten § 263a StGB	2 612	2 420	-192	-7,35
Computerbetrug mittels rechtswidrig erlangter sonstiger unbarer Zahlungsmittel § 263a StGB	1 098	1 376	278	25,32
Leistungskreditbetrug § 263a StGB	1 078	1 258	180	16,70
Computerbetrug (sonstiger) § 263a StGB	4 038	3 836	-202	-5,00
Missbräuchliche Nutzung von Telekommunikationsdiensten § 263a StGB	49	53	4	8,16
Abrechnungsbetrug im Gesundheitswesen § 263a StGB	1	4	3	300,00
Überweisungsbetrug § 263a StGB	208	403	195	93,75

2.1.2 Aufklärungsquote

Von den im Jahr 2021 in der PKS erfassten Straftaten wurden 8 020 aufgeklärt. Die Aufklärungsquote betrug 26,63 Prozent und verringerte sich gegenüber 2020 um 2,03 Prozentpunkte. Im Bereich des Computerbetrugs wurden 5 847 Fälle aufgeklärt. Dies entspricht einer Aufklärungsquote von 29,83 Prozent (29,95 Prozent).

Abbildung 1
Vergleich Fallzahlen und Aufklärungsquote Cybercrime im engeren Sinne

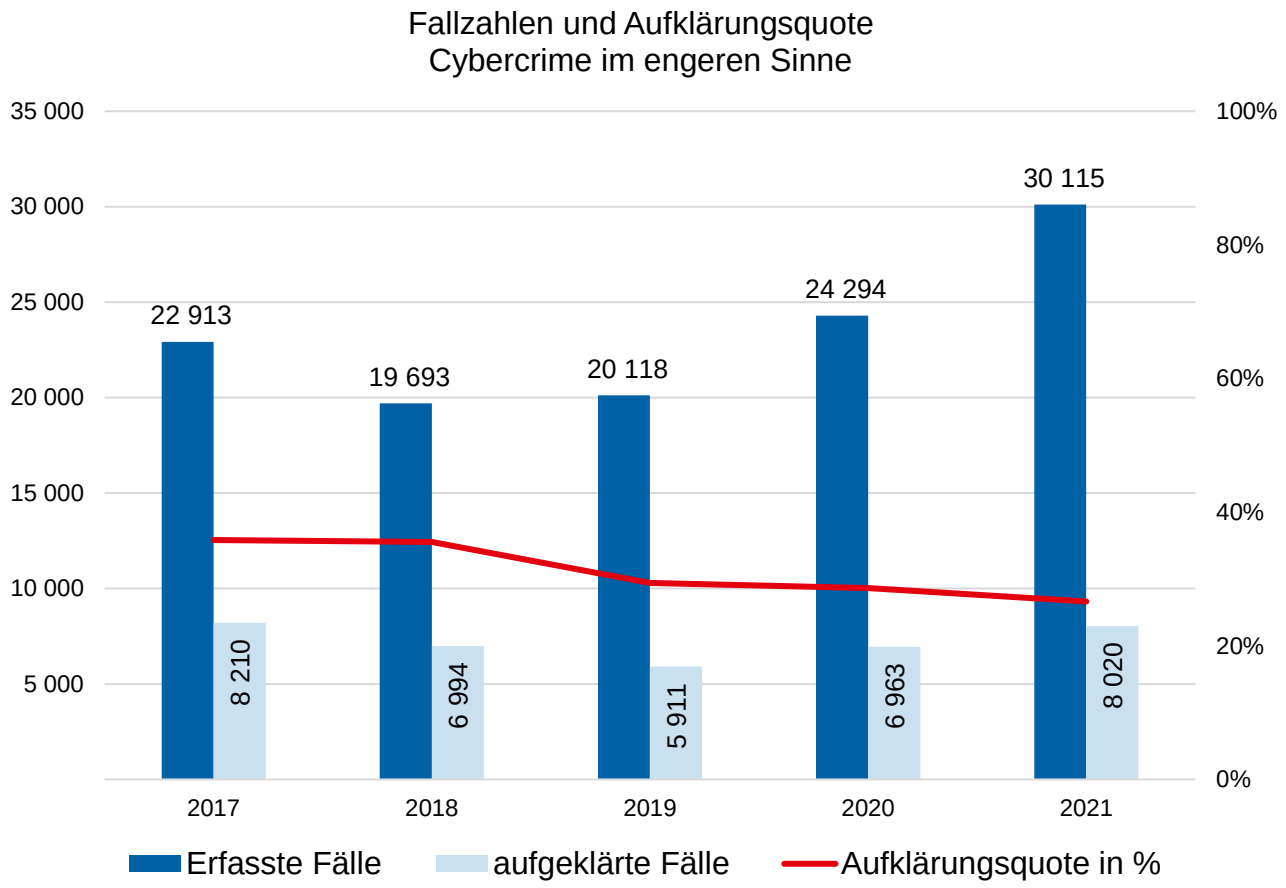


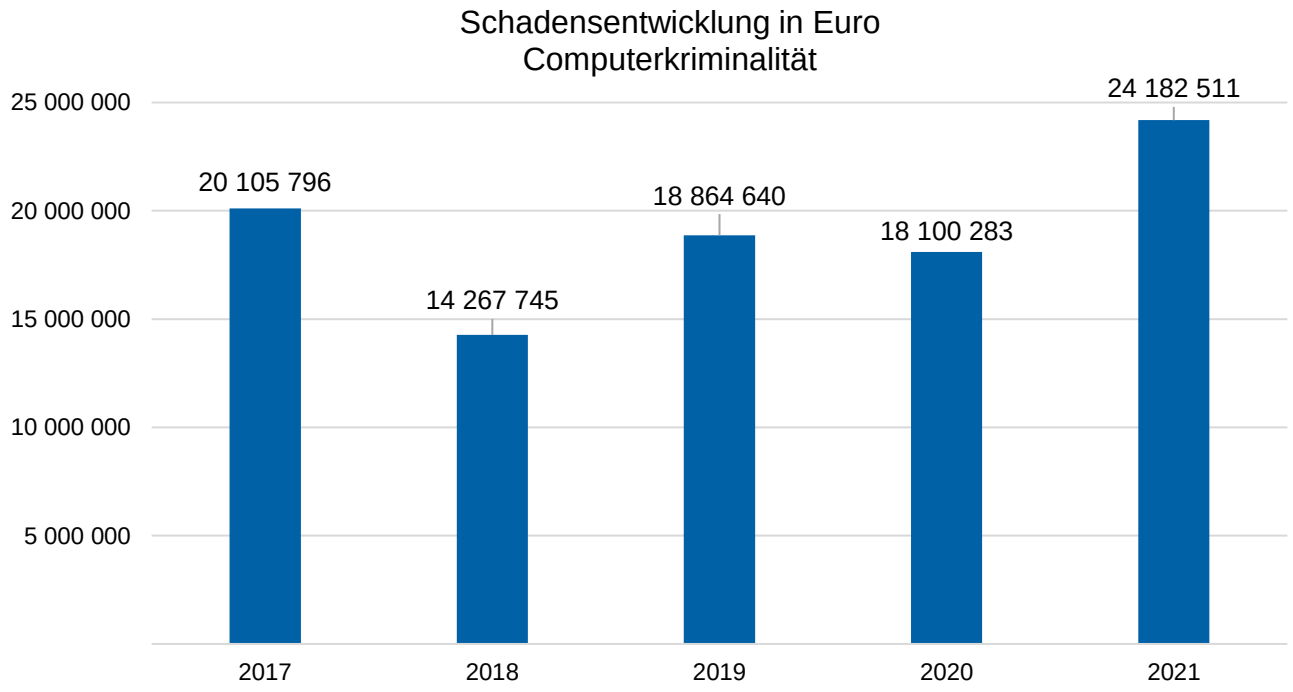
Tabelle 3
Aufklärungsquote (AQ)

Delikt	Aufgeklärte Fälle		Aufklärungsquote		Zu-/Abnahme (AQ)
	2020	2021	2020	2021	%-Punkte
Computerkriminalität (Cybercrime im engeren Sinne)	**6 963**	**8 020**	**28,66**	**26,63**	**-2,03**
Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei der Datenverarbeitung §§ 269, 270 StGB	707	1 040	25,33	25,33	0,00
Datenveränderung, Computersabotage §§ 303a, 303b StGB	198	269	15,74	16,27	0,53
Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen und Datenhehlerei §§ 202a, 202b, 202c, 202d StGB	668	864	29,14	18,18	-10,96
Softwarepiraterie (private Anwendung z.B. Computerspiele)	12	31	92,31	96,88	4,57
Softwarepiraterie in Form gewerbsmäßigen Handelns	6	7	100,00	100,00	0,00
Computerbetrug § 263a StGB	5 372	5 847	29,95	29,83	-0,12
Betrügerisches Erlangen von Kfz § 263a StGB	7	6	70,00	60,00	-10,00
Weitere Arten des Warenkreditbetruges § 263a StGB	2 506	2 789	40,05	40,49	0,44
Computerbetrug mittels rechtswidrig erlangter Zahlungskarten mit PIN § 263a StGB	607	718	23,50	21,39	-2,11
Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten § 263a StGB	450	455	17,23	18,80	1,57
Computerbetrug mittels rechtswidrig erlangter sonstiger unbarer Zahlungsmittel § 263a StGB	242	315	22,04	22,89	0,85
Leistungskreditbetrug § 263a StGB	331	277	30,71	22,02	-8,69
Computerbetrug (sonstiger)§ 263a StGB	1 157	1 033	29,07	27,30	-1,77
Missbräuchliche Nutzung von Telekommunikationsdiensten § 263a StGB	10	13	20,41	24,53	4,12
Abrechnungsbetrug im Gesundheitswesen § 263a StGB	1	3	100,00	75,00	-25,00

2.1.3 Schadensentwicklung

Schäden von Cybercrime werden in der Polizeilichen Kriminalstatistik ausschließlich für Computerbetrug und Softwarepiraterie abgebildet. Im Jahr 2021 erhöhte sich der Gesamtschaden der Computerkriminalität um 6 082 228 Euro auf 24 182 511 Euro und erreicht somit einen neuen Höchstwert innerhalb der vergangenen fünf Jahre. Ein hohes Dunkelfeld existiert bei Schäden, die durch Erpressungsdelikte, wie Ransomware zum Nachteil von Firmen, entstehen. Die Polizeiliche Kriminalstatistik weist lediglich Schäden für Erpressungen allgemein aus. Eine separate statistische Erfassung von Cybercrime-Erpressungsdelikten gibt es nicht. Zudem werden erfolgreiche Erpressungen zumeist nicht zur Anzeige gebracht.

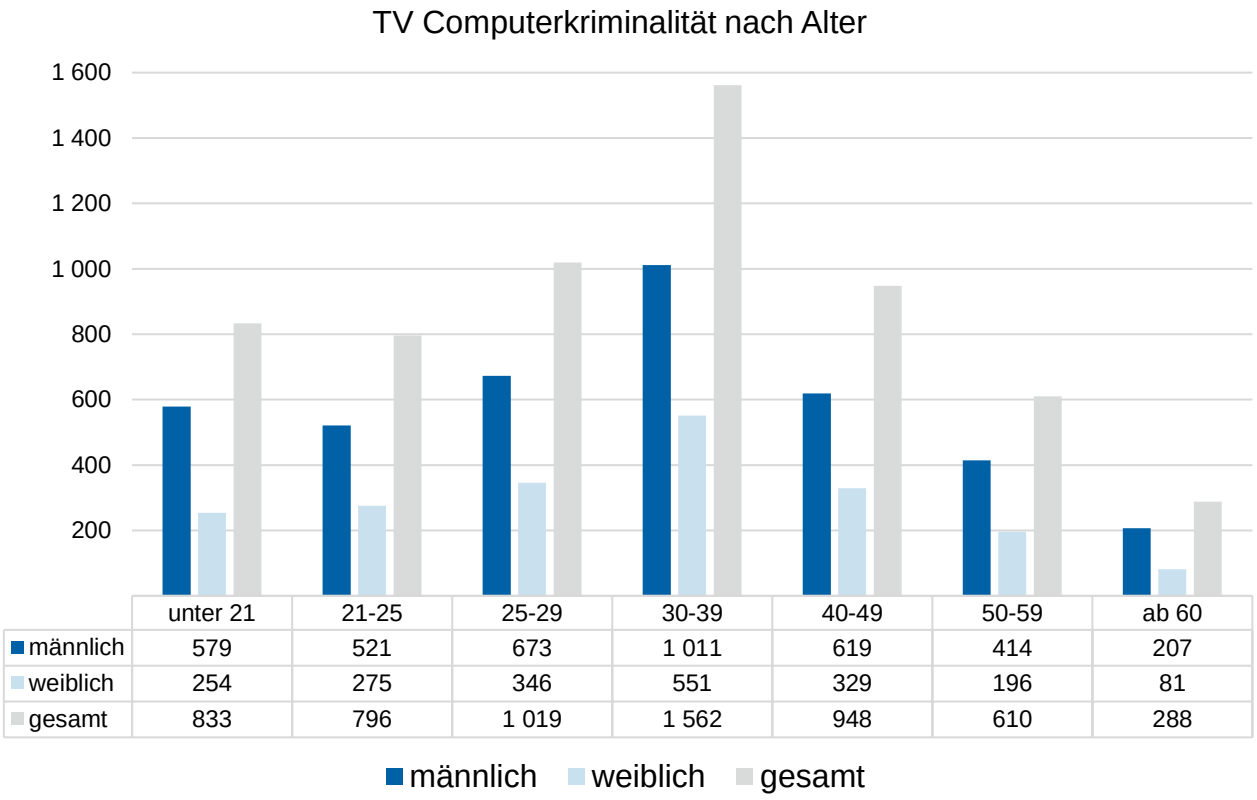
Abbildung 2
Schadensentwicklung Computerbetrug



2.1.4 Tatverdächtige

Im Jahr 2021 wurden 6 056 (5 166) Tatverdächtige ermittelt. Den größten Anteil nahm mit 1 562 ermittelten Tatverdächtigen die Gruppe der Erwachsenen im Alter von 30 bis 39 Jahren ein. Der Anteil an männlichen Tatverdächtigen ist mit 4 024 im Verhältnis zur Gesamtzahl von 6 056 überrepräsentiert.

Abbildung 3
Tatverdächtige



	unter 21	21-25	25-29	30-39	40-49	50-59	ab 60
männlich	579	521	673	1 011	619	414	207
weiblich	254	275	346	551	329	196	81
gesamt	833	796	1 019	1 562	948	610	288

2.2 Einzelne Deliktsfelder

Datenveränderung, Computersabotage

Solar Winds - „Supply Chain“ Angriff

Am Ende des Jahres 2020 und mit Beginn des Jahres 2021 wurde die seit Jahren größte Kompromittierung von IT-Infrastruktur amerikanischer Unternehmen und staatlicher Institutionen bekannt.

Zunächst schien lediglich das IT-Sicherheitsunternehmen FireEye betroffen zu sein. Es stellte sich jedoch schnell heraus, dass die Kompromittierung über ein Update der SolarWinds-Software Orion erfolgte und dieses Update, neben zahlreichen amerikanischen Unternehmen und staatlichen Institutionen, auch europäische Unternehmen betraf.

Das Unternehmen SolarWinds bietet mit der Plattform Orion eine Überwachungs- und Verwaltungssoftware für IT-Infrastruktur an. Neben amerikanischen Kunden hat das Unternehmen auch Kunden im Ausland, so auch in Deutschland. Bei dem Angriff wurden, im Gegensatz zur Verwendung von Verschlüsselungstrojanern, keine Daten verschlüsselt oder mit einer Veröffentlichung abgeflossener Daten gedroht. Das Ziel der Täter war die Ausleitung von Informationen betroffener Unternehmen und Institutionen. Dies kann als Indikator für das Handeln staatliche Akteure gewertet werden.

Das Bundeskriminalamt informierte die Polizei NRW über ein potentiell betroffenes Unternehmen in Nordrhein-Westfalen. Nach Rücksprache mit dem betroffenen Unternehmen stellte sich heraus, dass die IT-Infrastruktur aufgrund vorhandener Netzwerksegmentierung nicht betroffen war und laut Aussage des Unternehmens keine Daten abgeflossen sind.

Zumeist erfährt die Polizei von Straftaten in diesem Kontext nur, wenn die Unternehmen diese selbst zur Anzeige bringen. Die fehlende Anzeigebereitschaft durch einen drohenden Reputationsschaden oder fehlende Kenntnis über einen entsprechenden Angriff erklären die Zurückhaltung betroffener Unternehmen bei der Anzeigenerstattung. Insofern liegt nur ein Teil des Kriminalitätsgeschehens im Hellfeld polizeilicher Bearbeitung und Erfassung.

Diese sogenannten „Supply Chain“ Angriffe sind darauf ausgelegt, keine zentralen Server eines Unternehmens zu befallen und zu verschlüsseln, sondern über einen zentralen Distributionskanal auf mehrere nachgelagerte Unternehmensdaten zuzugreifen und dort entweder Daten herauszuleiten oder Systeme zu verschlüsseln. Diese Art des Cyberangriffs verlangt ein

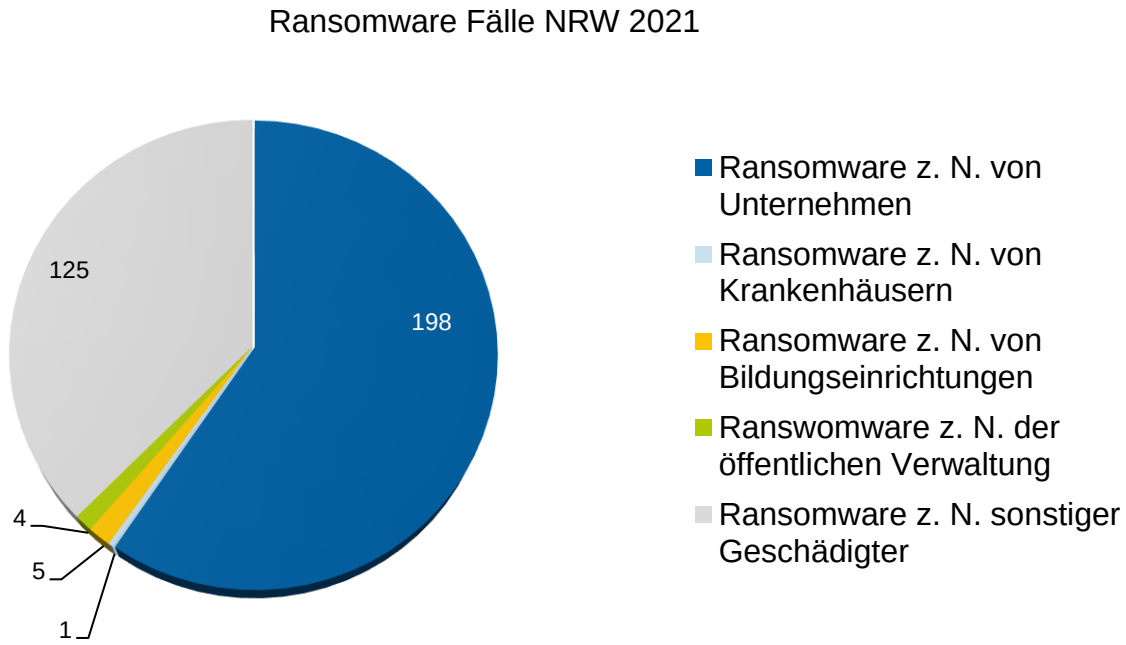
hohes Maß an technischer Expertise und ein organisatorisches Zusammenwirken mehrerer Akteure.

Ransomware

Die Delikte Datenveränderung und Computersabotage sind oftmals miteinander verbunden. So werden beispielsweise beim Phänomen Ransomware durch Täter Schadprogramme per E-Mail-Anhang in das anzugreifende System eingeschleust. Öffnet der Nutzer diesen Anhang, wird Software auf seinem System installiert, die den Abfluss und die Verschlüsselung von Daten durch die Täter ermöglicht. Initiieren die Täter die Verschlüsselung, sind die Daten für den Inhaber nicht mehr nutzbar. Zur Entschlüsselung der Daten wird ein Lösegeld gefordert. Mit der Drohung der Veröffentlichung der abgeflossenen Daten setzen die Täter ihre Opfer weiter unter Druck, um diese zur Zahlung zu bewegen.

Die Fallzahlen im Deliktsbereich „Datenveränderung, Computersabotage §§ 303a, 303b StGB“ sind im Jahr 2021 (1 653) im Vergleich zum Vorjahr (1 258) um 31,40 Prozent gestiegen. Die Aufklärungsquote im Jahr 2021 betrug 16,27 Prozent (15,74 Prozent).

Die Delikte „Datenveränderung“ und „Computersabotage“ beinhalten nicht ausschließlich Fälle des Phänomens Ransomware. Zudem werden Ransomware-Fälle nicht durchgängig als „Datenveränderung“ und „Computersabotage“ erfasst. Um für dieses Phänomen Fallzahlen darzustellen, haben die Kreispolizeibehörden NRW (KPB) diese für 2021 separat erhoben. Im Jahr 2021 kam es demnach zu insgesamt 333 Ransomware Fällen, der überwiegende Teil davon (58,26 Prozent) erfolgte zum Nachteil von Unternehmen.



Straftaten durch Ransomware betreffen Privatpersonen, Wirtschaftsunternehmen und Institutionen der öffentlichen Hand. So wurde im November 2021 ein mittelständisches Unternehmen mittels Ransomware angegriffen, das als Software-as-a-Service-Dienstleister für kleine und mittlere Messstellenbetreiber im Elektrizitätsbereich agiert. Dadurch konnten Kundensysteme, ähnlich eines „Supply Chain“ Angriffs, mittelbar getroffen werden. Durch eine offene und konstruktive Kommunikation zwischen dem Unternehmen und den zuständigen Polizei- und Bundesbehörden konnte ein größerer Schaden abgewandt werden.

Neben Wirtschaftsunternehmen sind öffentliche Institutionen Ziele von kriminellen Ransomware Gruppen. Die Stadtverwaltung Witten und die Kreisverwaltung Wesel konnten aufgrund eines Ransomwareangriffs zeitweise nicht mehr auf ihre IT-Infrastruktur zugreifen, sodass der Betrieb nur stark eingeschränkt möglich war.

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

Unter der Überschrift „Cybercrime as a Service“ bieten im Internet kriminelle Dienstleister gegen Bezahlung u. a. Schadsoftware oder DDoS-Angriffe als Auftragsleistungen an. Die Initiierung entsprechender Angriffe bedarf damit keiner fundierten Kenntnisse oder eigener technischer Infrastruktur.

Smishing

Bei diesem Phänomen, welches vor allem im ersten Halbjahr 2021 aufgetreten ist, handelt es sich um eine abgewandelte Form des Phishings. Geschädigte erhalten eine SMS mit der Aufforderung, auf einen Link zu klicken und einen Download zu starten. Eine oft verwendete Masche war die fingierte Nachricht eines Paketversandhandels, die eine Paketnachverfolgung vorgab. Sobald der Geschädigte diesen Link anklickte, wurde ein Downloadfenster geöffnet, welches ein Browserupdate simulierte. Wenn der Geschädigte dem zustimmte, wurde kein Update sondern eine Schadsoftware heruntergeladen. Im Anschluss sendete das kompromittierte Mobiltelefon weitere SMS an potentielle Opfer. Ziel der Schadsoftware ist das Auslesen von Kreditkarteninformationen und Einmalpasswörtern.

Ausspähen, Abfangen von Daten einschließlich Vorbereitungshandlungen und Datenhehlerei

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

Die Fallzahlen sind im Berichtsjahr 2021 mit 4 752 Fällen im Vergleich zu 2020 mit 2 292 Fällen um 107,33 Prozent gestiegen. Die Aufklärungsquote im Jahr 2021 betrug 18,18 Prozent (29,14 Prozent). Ein Anstieg der Fallzahlen in diesem Deliktsbereich kann durch gestiegene Smishing- und Phishingfälle erklärt werden.

Beim Phishing erhält der Geschädigte eine konspirativ gestaltete E-Mail mit der Aufforderung einem Link zu folgen, der zumeist auf eine manipulierte Webseite führt, wo das Opfer personenbezogene Daten und Passwörter eingeben soll. Oft sind es nachgebaute Seiten von Online-Banking Portalen oder Handelsplattformen wie eBay, eBay-Kleinanzeigen oder Amazon. Mit diesen Daten verschaffen sich die Täter Zugang zu den Konten, bestellen Waren oder bieten in betrügerischer Absicht nicht vorhandene Waren an.

Computerbetrug mittels rechtswidrig erlangter Zahlungskarten mit PIN

Die Fallzahlen im Deliktsbereich „Computerbetrug mittels rechtswidrig erlangter Zahlungskarten mit PIN“ sind im Jahr 2021 (3 356) im Vergleich zum Vorjahr (2 583) um 29,93 Prozent gestiegen. Die Aufklärungsquote im Jahr 2021 betrug 21,39 Prozent (23,50) Prozent.

Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten

Zahlungskartendaten, die durch Phishing oder Skimming rechtswidrig erlangt wurden, werden in betrügerischer Absicht im Internet verwandt. Zudem konnten Täter Geldautomatenkarten aus Rohlingen herstellen und damit im außereuropäischen Ausland Geldverfügungen tätigen. Die Geschädigten erfuhren erst durch die zeitversetzte Belastung ihres Kontos von dem Missbrauch ihrer Daten. Die Fallzahlen sind im Jahr 2021 (2 420) im Vergleich zum Vorjahr (2 612) um 7,35 Prozent gesunken. Die Aufklärungsquote im Jahr 2021 betrug 18,80 Prozent (17,23 Prozent).

Computerbetrug mittels rechtswidrig erlangter sonstiger unbarer Zahlungsmittel

Sonstige unbare Zahlungsmittel sind unter anderem Guthabenkarten, Schecks oder Bonuskarten. Zudem erfolgen Zahlungen zunehmend über PayPal-Konten. In den meisten Fällen wurden Waren im Online-Handel bestellt und über ein zuvor gehacktes oder ausgespähtes PayPal-Konto bezahlt. Die Fallzahlen sind im Jahr 2021 (1 376) im Vergleich zum Vorjahr (1 089) um 25,32 Prozent gestiegen. Die Aufklärungsquote im Jahr 2021 betrug 22,89 Prozent (22,04 Prozent).

Leistungskreditbetrug

Beim Leistungskreditbetrug erbringt der Verkäufer eine Leistung im Voraus. Der Täter bestellt diese Leistung über das Internet, hat jedoch von Anfang an nicht die Absicht zu zahlen. Oft werden frei erfundene Personalien oder missbräuchlich verwendete reale Personalien genutzt. Die Fallzahlen sind im Jahr 2021 (1 258) im Vergleich zum Vorjahr (1 078) um 16,70 Prozent gestiegen. Die Aufklärungsquote im Jahr 2021 betrug 22,02 Prozent (30,71 Prozent).

Überweisungsbetrug

Durch Einreichen einer ge- oder verfälschten Überweisung bzw. Zahlungsaufforderung wird dem kontoführenden Institut vorgetäuscht, der Kontoinhaber habe die Überweisung auf das Konto des Täters beauftragt. Erfolgt der Vorgang automatisiert, erfüllt dies den Tatbestand des

§ 263a StGB. Die Fallzahlen sind im Jahr 2021 mit 403 Fällen im Vergleich zum Vorjahr (208 Fälle) um 93,75 Prozent gestiegen. Die Aufklärungsquote im Jahr 2021 betrug 57,82 Prozent (27,88 Prozent).

3 Lagedarstellung Cybercrime im weiteren Sinne

3.1 Verfahrensdaten

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

Der Unterschied zwischen Cybercrime im engeren und im weiteren Sinne wird beim Betrug deutlich: Erfolgt die Täuschungshandlung gegenüber einem datenverarbeitenden System, handelt es sich um einen Computerbetrug gemäß § 263a StGB und somit Cybercrime im engeren Sinne. Erfolgt die Täuschung unter Nutzung eines Computers gegenüber einem Menschen, liegt ein Betrug gemäß § 263 StGB vor und es handelt sich um Cybercrime im weiteren Sinne. Soweit das Internet im Hinblick auf die Tatverwirklichung nur eine untergeordnete Rolle hat, wird die Sonderkennung „Tatmittel Internet“ nicht verwendet. Dies ist beispielsweise der Fall, wenn Kontakte zwischen Täter und Opfer mittels Internet ausschließlich im Vorfeld der eigentlichen Tat stattfanden. 2021 wurden 79 145 Fälle mit dem Tatmittel Internet erfasst, 17 878 mehr als 2020. Den größten Anteil nahmen hierbei Betrugsdelikte mit 51 839 Fällen ein. Bei einer Aufklärungsquote von 79,74 Prozent wurden 41 338 Fälle aufgeklärt.

Abbildung 4
Tatmittel Internet - Fallzahlen und Aufklärungsquote

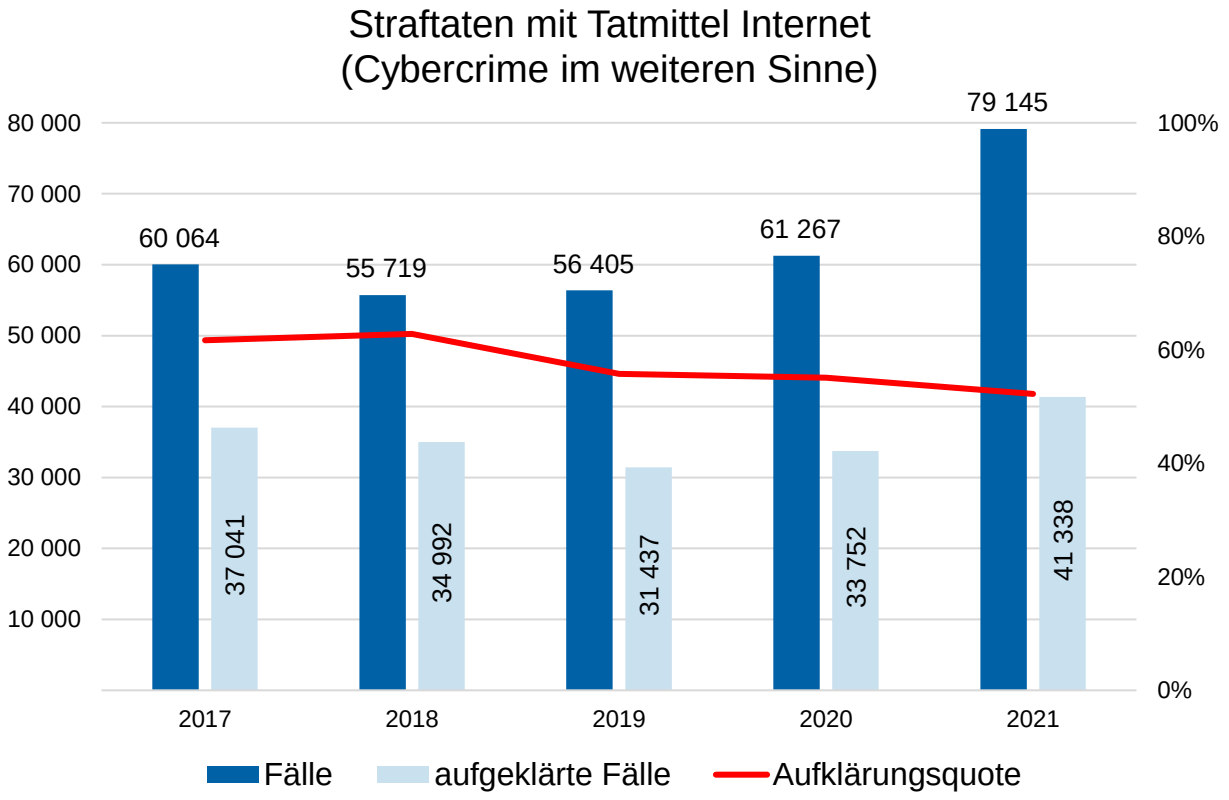


Tabelle 4
Tatmittel Internet

	Gesamt-kriminalität	darunter Tatmittel Internet	
Straftaten	**2021**	**Fälle**	**Anteil in %**
Alle Straftaten	**1 201 472**	**79 145**	**6,59**
Straftaten gegen die sexuelle Selbstbestimmung	28 995	11 056	38,13
Verbreitung pornografischer Schriften (Erzeugnisse) gem. §§ 184, 184a, 184b, 184c, 184d, 184e StGB	14 154	9 828	69,44
Verbreitung, Erwerb, Besitz und Herstellung kinder-pornographischer Schriften gemäß § 184b StGB	11 328	8 133	71,80
Verbreitung von Kinderpornographie gemäß § 184b Abs. 1 Nr. 1	4 685	3 714	79,27
Betrug §§ 263, 263a, 264, 264a, 265, 265a, 265b StGB	194 978	51 839	26,59
Waren- und Warenkreditbetrug	77 679	35 124	45,22
Computerbetrug (sonstiger) §263a StGB	3 836	2 397	62,49
Betrügerisches Erlangen von Kfz § 263a StGB	10	5	50,00
Weitere Arten des Warenkreditbetruges § 263a StGB	6 888	4 608	66,90
Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten § 263a StGB	2 420	1 151	47,56
Computerbetrug mittels rechtswidrig erlangter sonstiger unbarer Zahlungsmittel § 263a StGB	1 376	637	46,29
Leistungskreditbetrug § 263a StGB	1 258	577	45,87
Überweisungsbetrug § 263a StGB	403	229	56,82
Missbräuchliche Nutzung von Telekommunikationsdiensten § 263a StGB	53	15	28,30
Fälschung beweiserheblicher Daten, Täuschung im Rechts-verkehr bei Datenverarbeitung §§ 269, 270 StGB	4 106	2 760	67,22
Datenveränderung, Computersabotage §§ 303a, 303b StGB	1 653	1 161	70,24
Ausspähen, Abfangen von Daten einschl. Vorbereitungs-handlungen und Datenhehlerei §§ 202a, 202b, 202c, 202d StGB	4 752	3 100	65,24

3.2 Kinderpornografie

2021 wurden für den Deliktsbereich „Verbreitung, Erwerb und Besitz kinderpornographischer Schriften“ gemäß § 184b StGB 11 328 (Vorjahr 4 776) Fälle erfasst. Dies entspricht einer Zunahme von 137,19 Prozent. Bereits 2020 hatten sich die Fallzahlen gegenüber dem Vorjahr verdoppelt. In diesem Deliktsbereich besitzt das Internet eine herausragende Rolle. Bei 8 133 Fällen (71,80 Prozent) war das Internet Tatmittel. Hiervon konnten 7 357 Taten (90,46 Prozent) aufgeklärt werden.

Ein Großteil der Ermittlungsverfahren ist auf das Hinweisaufkommen durch die teilstaatliche US-amerikanische Organisation „National Center for Missing and Exploited Children“ (NCMEC) zurückzuführen. Die Anzahl der in Nordrhein-Westfalen eingehenden Hinweise hat sich nahezu verdreifacht. Dies ist einerseits auf eine Verfahrensumstellung beim Bundeskriminalamt und der Justiz und andererseits auf eine deutliche Steigerung der Meldungen des NCMEC zurückzuführen. Nach Prüfung der strafrechtlichen Relevanz und erfolgversprechender Ermittlungsansätze durch das Bundeskriminalamt wurden dem Landeskriminalamt NRW (LKA NRW) 8 632 (3 099) Verdachtsfälle bekannt und über die Zentral- und Ansprechstelle Cybercrime der Staatsanwaltschaft Köln den nordrhein-westfälischen KPB zu weiteren Ermittlungen zugeleitet.

Die Zahl der Tatverdächtigen aus Nordrhein-Westfalen in bundesweiten Umfangsverfahren blieb mit 1 774 (1 809) auf dem Stand des Vorjahres. Mit 826 Tatverdächtigen unter 14 Jahren (Vorjahr 428) und 2 325 Tatverdächtige zwischen 14 und 18 Jahren (Vorjahr 1 125) stieg die Anzahl Tatverdächtiger in diesen beiden Altersgruppen im Vergleich zum Vorjahr deutlich an. Somit handelt es sich bei 38,74 % aller bekannten Tatverdächtigen im Kinder und Jugendliche.

Seit Sommer 2021 gibt es im In- und Ausland eine unbekannte Anzahl von Fällen, bei denen Facebook-Accounts gehackt und anschließend inkriminierte Bilder oder Videos hochgeladen wurden. Dies führte zur Sperrung der betroffenen Accounts und zur Erstellung eines NCMEC-Reports. Sofern Betroffene das Hacken ihrer Accounts nicht zur Anzeige brachten und die Ermittlungsbehörden auch nicht auf anderem Wege Kenntnis von der Manipulation erhielten, richteten sich die Strafverfahren und die damit verbundenen strafprozessualen Maßnahmen folglich gegen die regulären Accountinhaber.

Hintergründe und Absichten dieser Hacking Angriffe sind bisher nicht bekannt. Forderungen oder einen finanziellen Schaden gab es in diesem Zusammenhang in sehr seltenen Fällen. Unter Federführung von EUROPOL werden Erfahrungen und Erkenntnisse zu dem Phänomen ausgetauscht und Präventionsmöglichkeiten mit Facebook und dem NCMEC erörtert. Das LKA

NRWsammelt alle Hinweise und versucht entsprechende Indizien in den NCMEC-Meldungen zu erkennen.

4 Prävention

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

Die Prävention von Cybercrime im weiteren Sinn (Tatmittel Internet) liegt vollständig in der Hand der KPB. Das LKA NRW mit dem Cybercrime-Kompetenzzentrum bearbeitet den Bereich der Cybercrime-Prävention im engeren Sinn. Adressaten sind insbesondere Unternehmen, aber auch Behörden und vergleichbare Institutionen.

Die Prävention von Cybercrime im weiteren Sinne ist vor dem Hintergrund der vielfältigen Deliktsbereiche durch intensive Kooperationen geprägt. Dabei wird das LKA NRW koordinierend tätig und setzt die Entwicklungen in diesem Deliktsbereich in Empfehlungen und Standards um.

Das LKA NRW entwickelte eine breit angelegte Kampagne zum Passwortschutz. Die Kooperationspartner Verbraucherzentrale NRW, eco-Verband der Internetwirtschaft e. V. und Bundesverband Verbraucherinitiative e. V. sind konzeptionell eingebunden. Die crossmediale Kampagne hat die Aufgabe, Präventionshinweise zu vermitteln, die auf Grundlage einer umfassenden Analyse der Schwachstellen bei den digitalen Endgeräten erstellt wurden. Am 26.10.2020 hatte der Minister des Innern des Landes Nordrhein-Westfalen, Herbert Reul, die Präventionskampagne www.mach-dein-passwort-stark.de der Öffentlichkeit vorgestellt und den Startschuss gesetzt. In 2021 lief die Kampagne durchgehend und wird fortgeschrieben. Im Bereich Cybercrime im engeren Sinn wird ein bewährtes Netzwerk unterschiedlichster Kooperationspartner wie der Bitkom, der Voice-Bundesverband der IT-Anwender und die Sicherheitspartnerschaft mit der Allianz für Sicherheit in der Wirtschaft West NRW bedient. Seit 2017 besteht eine gleichgelagerte Kooperationsvereinbarung mit dem eco-Verband der Internetwirtschaft e. V. und dem Networker NRW e. V. Dieses Netzwerk wurde im Zusammenhang mit den Herausforderungen der aktuellen Pandemie genutzt, um auf die Gefahren der sprunghaft angestiegenen Digitalisierung und die damit verbundenen Risiken aufmerksam zu machen. Insbesondere der Bereich Homeoffice und Sicherheit unternehmenskritischer Daten wurden vorangestellt. Zudem wird durch die enge Zusammenarbeit erreicht, dass das LKA NRW unterschiedlichste Akteure als Multiplikatoren innerhalb der Wirtschaft für den Bereich Prävention

von Cybercrime sensibilisiert. Durch die Beteiligung an „Round Tables“ und die Zusammenarbeit in Regionalgruppen verbessert das LKA NRW die vertrauensvolle Zusammenarbeit zwischen Wirtschaft und Polizei und steigert so die Anzeigebereitschaft und das Bewusstsein für die durch Cybercrime bestehenden Gefahren (Awareness).

Die Informations- und Wissensvermittlung umfasst neben den Möglichkeiten zum Schutz vor Angriffen auch die Sensibilisierung zur Notwendigkeit der Vorbereitung auf den „Ernstfall“. Potentiell Betroffene, die sich mit geplanten Reaktionsmustern und Notfallplänen wappnen, können Angriffe deutlich besser abwehren, so dass geringere Schäden entstehen oder ganz vermieden werden können.

Durch die vorherrschenden Distanzregeln im zweiten Corona Jahr wurden auch 2021 nahezu alle Kontakte via Video-Konferenztechnik realisiert. Dieser Technikeinsatz ermöglicht eine noch höhere Kontaktdichte und Reichweite und wird dauerhaft ein wichtiger Kommunikationskanal der polizeilichen Präventionsarbeit. Dabei gab es beinahe wöchentliche Veranstaltungen mit einer Teilnehmerzahl im dreistelligen Bereich.

Durch die pandemiebedingten Kontaktreduzierungen wurde in vielen Bereichen Arbeitsplätze in Homeoffices verlegt. Dies hat zu einer erhöhten Risikobewertung der IT-Sicherheit geführt. Das LKA NRW hat eine Handlungsempfehlung für eine Netzwerktrennung des häuslichen WLAN erstellt. Ebenso wurden die Beratungsempfehlungen in dem Kontext von Ransomware Angriffen angepasst.

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

Herausgeber

Landeskriminalamt Nordrhein-Westfalen
Völklinger Straße 49
40221 Düsseldorf

Abteilung 4
Cybercrime-Kompetenzzentrum
Dezernat 41

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

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

Bildnachweis: Titelseite – Marita Segin