POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

bürgerorientiert · professionell · rechtsstaatlich

Cybercrime in Nordrhein-Westfalen

Lagebild 2013

www.lka.nrw.de

Kriminalitätsentwicklung im Überblick

Cybercrime[1] in NRW – Entwicklung und Bewertung

- **Erneute Zunahme der Fallzahlen der Cybercrime im engeren Sinne[2]**
- **Aufwärtstrend bei Erpressung mit Tatmittel Internet setzt sich fort**
- **Erneute Zunahme im Bereich der Datenveränderung/Computersabotage**
- **Rückgang der Fallzahlen bei Betrug mittels rechtswidrig erlangter Debitkarten mit PIN setzt sich fort**
- **Anzahl der aufgeklärten Fälle bei Straftaten mit Tatmittel Internet um 30,3 % gesteigert**

	2012	2013	in %	Tendenz
Cybercrime im engeren Sinne	**22.228**	**27.016**	**+ 21,5 %**	↗
Computerbetrug	6.087	6.774	+ 11,3 %	↗
Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei der Datenverarbeitung	2.278	3.121	+ 37,0 %	↗
Datenveränderung/Computersabotage	4.118	6.713	+ 63,0 %	↗
Ausspähen, Abfangen von Daten einschließlich Vorbereitunshandlungen gem. §§ 202a, 202b, 202c StGB	4.373	5.486	+ 25,5 %	↗
Betrug mittels rechtswidrig erlangter Debitkarten mit PIN	4.880	4.553	- 6,7 %	↘
Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten	419	319	- 23,9 %	↘
Straftaten mit Tatmittel Internet	**54.339**	**70.981**	**+ 30,6 %**	↗
Betrug mit Tatmittel Internet	35.987	45.751	+ 27,1 %	↗
Erpressung mit Tatmittel Internet	1.324	1.981	+ 49,6 %	↗
Anzahl der aufgeklärten Fälle	27.485	35.810	+ 30,3 %	↗

[1] Der international gebräuchliche Begriff „Cybercrime“ ist dem Begriff Computerkriminalität gleichgesetzt (Erlass des MIK NRW vom 29.02.2012 - 423-62.18.09).
[2] Informationen zur Definition und Abgrenzung siehe Nr. 1, Vorbemerkungen

Inhaltsverzeichnis Seite

1 Lagedarstellung

1.1 Vorbemerkungen

Cybercrime umfasst die Straftaten, die sich gegen das Internet, weitere Datennetze und informationstechnische Systeme oder deren Daten richten. Cybercrime umfasst auch solche Straftaten, die mittels dieser Informationstechnik begangen werden.

Diese Definition berücksichtigt sowohl nationale als auch internationale Sicherheitsstrategien. Dabei steht sie im Einklang mit internationalen Begriffsbestimmungen wie der European Cyber Crime Convention[3] der United Nations.

Die Cybercrime im engeren Sinne[4] umfasst Straftaten, bei denen Elemente der elektronischen Datenverarbeitung in den Tatbestandsmerkmalen enthalten sind. Dazu zählen:

- Betrug mittels rechtswidrig erlangter Debitkarten mit PIN
- Computerbetrug nach § 263a StGB
- Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei der Datenverarbeitung nach §§ 269, 270 StGB
- Datenveränderung, Computersabotage nach §§ 303a, 303b StGB
- Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen gem. §§ 202a, 202b und 202c StGB[5]
- Softwarepiraterie (privates Handeln)
- Softwarepiraterie (gewerbsmäßiges Handeln)
- Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten

Das Lagebild Cybercrime stellt phänomenspezifisch und phänomenübergreifend die Entwicklung der Cybercrime im engeren Sinne im Land Nordrhein-Westfalen dar. Die Daten basieren auf Ermittlungsverfahren der Polizeibehörden in NRW, die nach einheitlichem Standard erhoben werden. Die unter Nr. 1 dargestellten Zahlen basieren auf Daten der Polizeilichen Kriminalstatistik (PKS). Einzelne Delikte, die mit Hilfe des Tatmittels Internet begangen werden, sind unter Nr. 1.6 gesondert dargestellt. Die Klammerwerte im Text beziehen sich, soweit nicht anders angegeben, auf die entsprechenden Vorjahreswerte. In einzelnen Phänomenen ist von einem großen Dunkelfeld auszugehen, da der Polizei viele Straftaten nicht bekannt werden.

Die Datenbasis für die Darstellung der einzelnen Phänomene unter Nr. 3 stammt aus dem polizeilichen Vorgangsbearbeitungssystem (vgl. Nr. 6.1), da einige Erscheinungsformen aktueller Phänomene mithilfe der deliktisch orientierten Polizeilichen Kriminalstatistik nicht hinreichend beschrieben werden können. Als Beispiel kann die Ransomware[6] dienen, die je nach Ausprägung der Tat im konkreten Einzelfall als Datenveränderung, Computersabotage oder Erpressung erfasst werden kann.

[3] Convention on Cybercrime, Budapest, 23.11.2011 (CETS No. 185), http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm, Stand: 05.05.2014
[4] Zur Definition und Unterscheidung Cybercrime im engeren/weiteren Sinne vgl. RdErl. des Ministeriums für Inneres und Kommunales vom 29.02.2012 - 423-62.18.09
[5] In diesem Umfang erst ab 2008 erfasst (vorher Ausspähen von Daten nach § 202a StGB)
[6] Schadsoftware, die infizierte Computer sperrt, ggf. die Daten verschlüsselt und für eine angebliche Freischaltung ein Lösegeld (ransom) fordert. Siehe auch Nr. 3.2

1.2 Verfahrensdaten

Die Gesamtzahl der erfassten Straftaten im Bereich Cybercrime steigt seit 2009 an (2010: +27,2 %, 2011: +1,3 %, 2012: +10,9 %). Mit 27.016 Fällen wurde im Jahr 2013 im Vergleich zum Vorjahr eine Steigerung um 21,5 % (+4.788 Fälle) und damit der bisherige Höchststand erreicht. Insbesondere bei Phänomenen wie Diebstahl und Missbrauch digitaler Identitäten, Angriff auf das Online-Banking sowie Eindringen in Datennetze mit dem Ziel der Datenveränderung und des Datendiebstahls sind Steigerungen festzustellen.

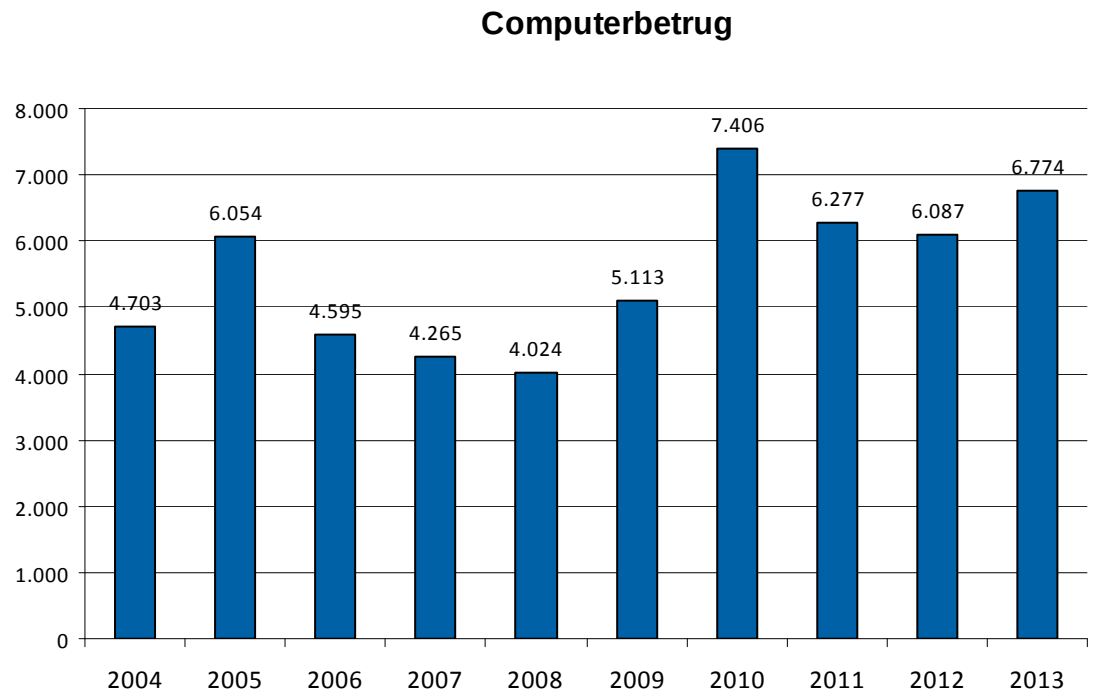
Im Jahr 2013 konnten 4.518 Fälle (16,7 %) aufgeklärt werden. Dies bedeutet einen Rückgang um 186 Fälle (-4,0 %) im Vergleich zum Vorjahr.

Die Anzahl ermittelter Tatverdächtiger ist gegenüber dem Vorjahr um 7,0 % gesunken. Von den insgesamt 3.492 (3.753) ermittelten Tatverdächtigen waren 743 (21,3 %) Nichtdeutsche. Nach der geltenden Richtlinie zur Führung der Polizeilichen Kriminalstatistik werden Auslandsstraftaten nicht erfasst. Dadurch fand wiederholt eine Vielzahl von polizeilich bekannt gewordenen Fällen wie der Datenveränderung bzw. Computersabotage (z. B. Ransomware, vgl. Nr. 3.2) statistisch keine Berücksichtigung.

1.3 Einzelne Deliktsbereiche

Computerbetrug

Nach einem Rückgang der Fallzahlen in den Jahren 2011 und 2012 auf zuletzt 6.087 Fälle ist für das Jahr 2013 wieder ein Anstieg um 687 auf 6.774 Fälle (+11,3 %) zu verzeichnen. Der Missbrauch digitaler Identitäten ist hier als zentrales Phänomen zu nennen. Vor allem Angriffe gegen das Online-Banking stellen sich zunehmend ausgefeilter dar. Mittels Schadsoftware und Methoden des social-engineering[7] wurden angepasste Sicherheitsmaßnahmen wie das mTAN[8]- oder ChipTAN-Verfahren umgangen.



[7] Bildung einer Legende, um eine Person zu beeinflussen und diese zu einer Handlung zu veranlassen (z. B. angebliche Sicherheitsmaßnahme, Test-/ Fehlüberweisung oder SEPA-Umstellung).
[8] mTAN: mobile transaction authentication number oder smsTAN: Transaktionsnummer, die per SMS auf Mobilfunkgeräte übertragen wird

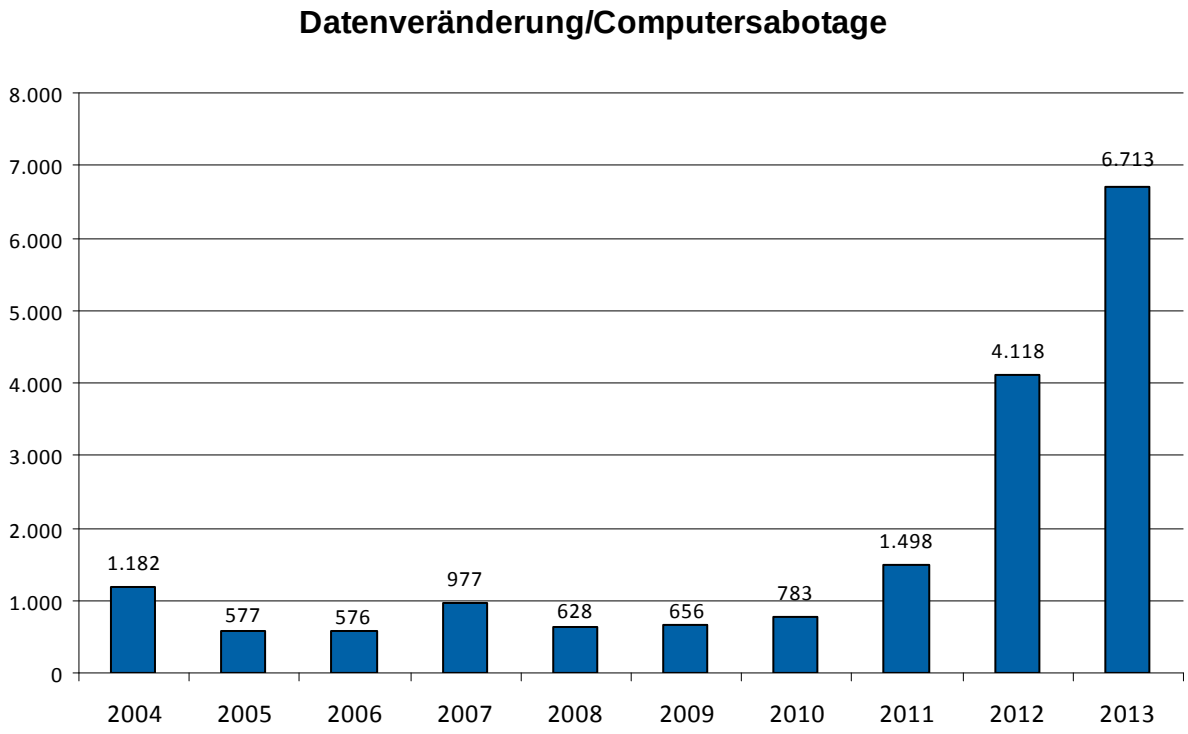
Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei der Datenverarbeitung

Unter Vorspiegelung falscher Identitäten (Banken, Online-Shops oder Kreditkartenunternehmen) sollen die Geschädigten per E-Mail oder mittels manipulierter Webseiten zur Preisgabe von Zugangs-, Kreditkartendaten, zur Anweisung von Zahlungen oder zur Ausführung übermittelter Schadsoftware veranlasst werden. Im gesamten Deliktsbereich sind die registrierten Fallzahlen im Jahr 2013 um 37,0 % (2012: 2.278; 2013: 3.121) gestiegen. Ursächlich ist die Zunahme von E-Mails mit inkriminierten Inhalten unter missbräuchlicher Verwendung von Firmenangaben. Auch die zunehmende Sensibilisierung und die erhöhte Anzeigebereitschaft der Bevölkerung tragen dazu bei.

Datenveränderung, Computersabotage

Eine Ursache für den Anstieg der Fallzahlen von 4.118 auf insgesamt 6.713 Fälle (+63,0 %) ist die zunehmende Verbreitung von Schadsoftware, insbesondere in Form von Ransomware (vgl. Nr. 3.2). Überwog im Jahr 2012 die Ransomware in den Varianten „BKA-Trojaner“ und „GEMA-/GVU-Trojaner“, wurde im Jahr 2013 zudem die Variante „ZIP-Trojaner“ mittels massenhaft versandter E-Mails verbreitet.

Die inkriminierten Anhänge in Form von vermeintlichen Rechnungen oder Mahnungen führten beim Öffnen zur Sperrung und Verschlüsselung des infizierten Systems. In anderen Fällen enthielten die Anhänge Schadsoftware mit Funktionalitäten zum Ausspähen von Daten oder zur Manipulation von Online-Banking-Transaktionen.



Ausspähen, Abfangen von Daten einschließlich Vorbereitungshandlungen

Die Polizeiliche Kriminalstatistik weist für 2013 in diesem Deliktsbereich 5.486 erfasste Fälle aus (4.373), was einem Anstieg um 1.113 Fälle (+25,5 %) entspricht. Das wesentliche Phänomen ist der Diebstahl digitaler Identitäten. Im Fokus der Täter stehen insbesondere Zugangsdaten zu Online-Banking-Konten, E-Commerce und Kreditkartendaten, die entweder durch die Cyberkriminellen selbst eingesetzt oder in der „Underground-Economy“[9] gehandelt werden.

Betrug mittels rechtswidrig erlangter Debitkarten[10] mit PIN[11]

Nach einer Abnahme um 1.228 auf 4.880 Fälle im Vorjahr sind die Fallzahlen erneut um 327 auf 4.553 erfasste Fälle gesunken. Dies entspricht einem Rückgang von 6,7 %. Der missbräuchliche Einsatz von Debitkarten wird häufig durch einen unachtsamen Umgang mit der PIN begünstigt. Debitkarten werden unmittelbar nach den sogenannten Erlangungstaten (z. B. Taschendiebstahl, Diebstahl aus Fahrzeugen oder Wohnungen) eingesetzt. In 554 Fällen ging die Tathandlung nicht über das Versuchsstadium hinaus.

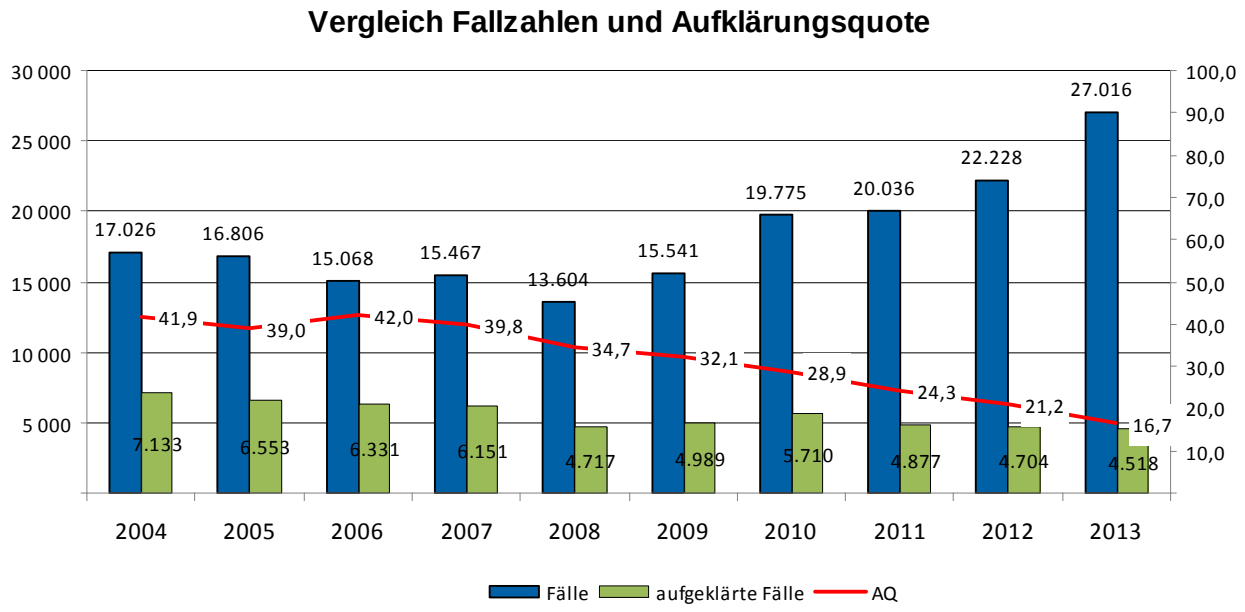
Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten

Die Fallzahlen des Jahres 2013 sind in der Polizeilichen Kriminalstatistik auf 319 Fälle gesunken. Im Vergleich zum Vorjahr ist eine Abnahme um 23,9 % (419 Fälle) festzustellen. Relevante Phänomene sind der missbräuchliche SIM[12]-Karten-Einsatz (z. B. betrügerisch erlangte Vertragsabschlüsse bei Mobilfunkanbietern unter Nutzung fremder Identitäten) sowie die Manipulation von Telekommunikationsanlagen. Unter Ausnutzung schwacher Zugangssicherungen oder Nebenstellen- bzw. Rufumleitungsfunktionen werden hierbei sowohl bei Firmen als auch bei Privatleuten teure Auslandstelefonverbindungen generiert. Abweichend zur rückläufigen Fallzahlenentwicklung im Phänomenbereich ist bei Telefonanlagenmanipulationen ein Anstieg zu verzeichnen (vgl. Nr. 3.5).

[9] Insbesondere Internetforen, in denen u. a. inkriminierte Daten und Dienstleistungen gehandelt werden
[10] Zahlungskarten, deren Einsatz unmittelbar zur Kontobelastung führt – girocard oder EC-Karte
[11] PIN: personal identification number; persönliche Geheimzahl
[12] SIM: subscriber identity modul; Chipkarte, die in Mobiltelefonen zur Identifikation des Teilnehmers im Mobilfunknetz dient

1.4 Aufklärungsquote

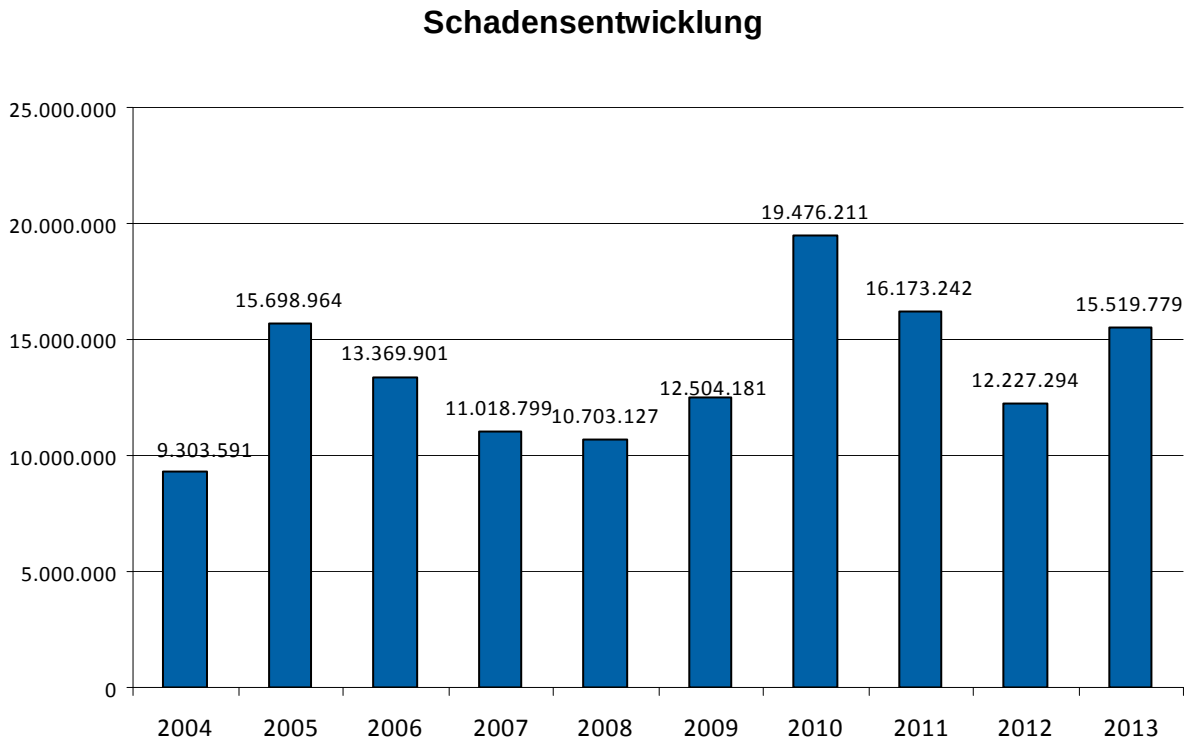
Die Aufklärungsquote der Cybercrime im engeren Sinne ist im Jahr 2013 mit 16,7 % gegenüber den Jahren 2012 (21,2 %) und 2011 (24,3 %) erneut gesunken.



Die sinkende Aufklärungsquote ist auf mehrere Einflussfaktoren zurückzuführen. Im Jahr 2013 war ein starker Anstieg der Fallzahlen bei Phänomenen mit geringen Ermittlungsansätzen und niedriger Aufklärungsquote zu verzeichnen. Andere wesentliche Ursachen für diese Entwicklung werden unter 2. „Ermittlungshemmnisse“ gesondert beleuchtet.

1.5 Schaden

Durch Delikte der Cybercrime im engeren Sinne wurde im Jahre 2013 eine Gesamtschadenssumme von 15.519.779 Euro (12.227.294) verursacht. Während in den Jahren 2011 und 2012 eine regressive Schadensentwicklung verzeichnet wurde, ist die Gesamtschadenssumme im Jahre 2013 um 26,9 % angestiegen.



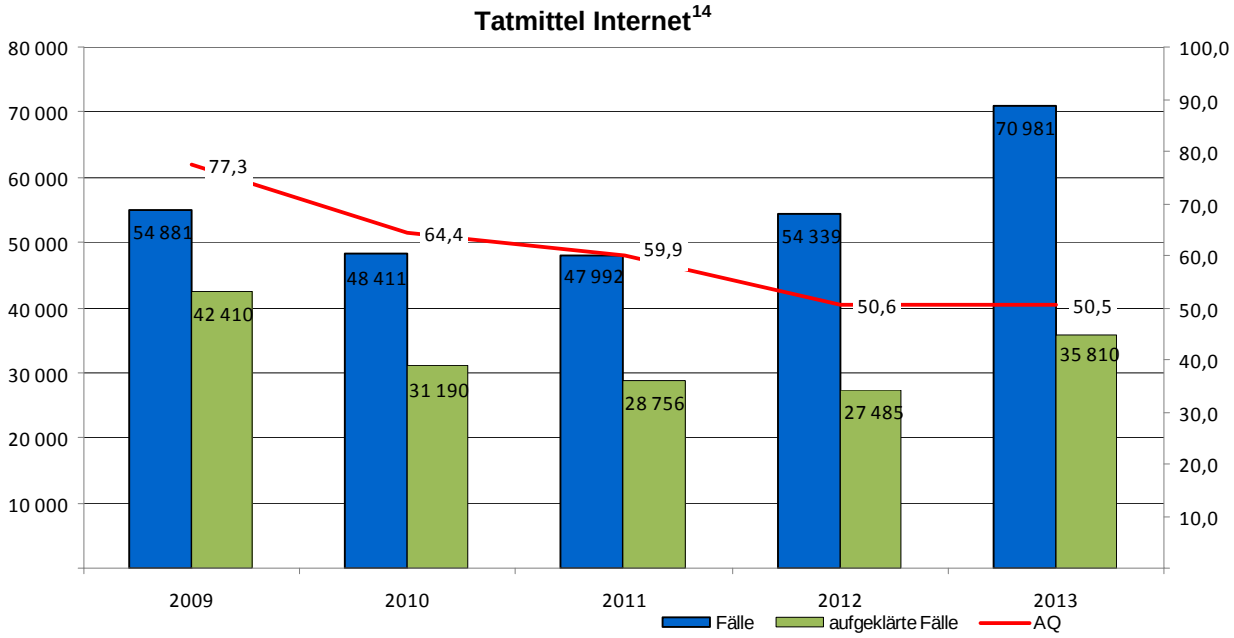
1.6 Tatmittel Internet

Straftaten, bei denen das Internet als Tatmittel verwendet wird, werden in der Polizeilichen Kriminalstatistik 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 sind (so genannte Äußerungs- bzw. Verbreitungsdelikte), als auch solche Delikte, bei denen das Internet bei der Tatbestandsverwirklichung eingesetzt wird. Spielt das Internet im Hinblick auf die Tatverwirklichung eine untergeordnete Rolle, wird die Sonderkennung „Tatmittel Internet“ nicht verwendet. Dies ist beispielsweise der Fall, wenn Kontakte zwischen Täter und Opfer mittels Internet im Vorfeld der eigentlichen Tat stattfinden.

Im Jahr 2013 wurden 70.981 (54.339) Fälle mit dieser Sonderkennung erfasst. Dies entspricht einer Zunahme um 30,6 %. Die Anzahl der aufgeklärten Fälle stieg um 8.325 auf 35.810 Fälle (27.485) an.

Straftaten mit dieser Kennung hatten einen Anteil von 4,8 % an der Gesamtkriminalität (3,6 %). In 64,5 % (66,2 %) der Fälle handelte es sich um Betrugsdelikte.

Die Erpressungsfälle mit dem „Tatmittel Internet“ nahmen um 49,6 % auf 1.981 Fälle zu (1.324). Wie schon 2012 setzten die Täter Ransomware (vgl. Nr. 3.2) und DDoS-Angriffe[13] als Druckmittel ein.



Kinderpornographie

Die Entwicklung der Fallzahlen im Deliktsbereich „Verbreitung, Besitz und Verschaffung von Kinderpornografie“ ist in besonderem Maße jährlichen Schwankungen unterworfen. Dies ist auf den Zeitpunkt des Abschlusses von Umfangsverfahren mit einer Vielzahl von Einzeltaten zurückzuführen. Die Fallzahlen nahmen um 14,8 % auf 1.578 (1.374) zu.

Die Anzahl der bekannt gewordenen Fälle der Verbreitung von Kinderpornografie sank von 837 im Jahr 2012 um 160 oder 19,1 % auf 677 Fälle im Jahr 2013.

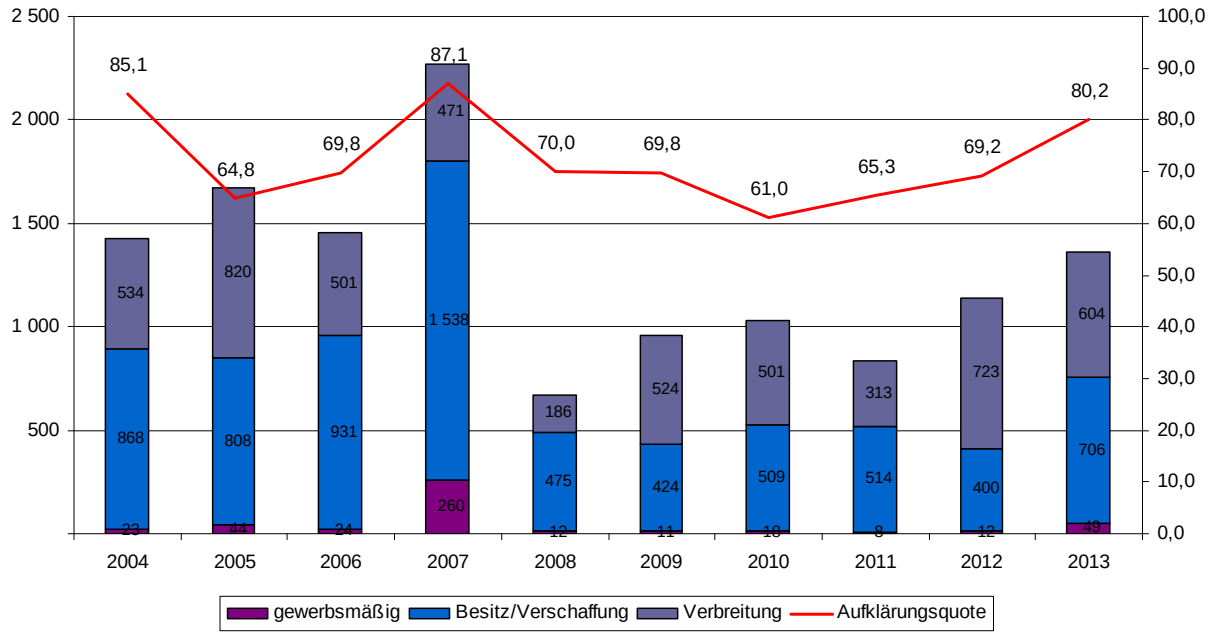
Die Anzahl der Fälle im Bereich Besitz oder Verschaffung von Kinderpornografie stieg von 519 erfassten Fällen im Jahr 2012 um 329 oder 63,4 % auf 848 Fälle an. 91,2 % dieser Fälle konnten aufgeklärt werden. Der Anstieg resultiert aus einem länderübergreifenden Umfangsverfahren mit einer Vielzahl von Tatverdächtigen mit Wohnsitz in NRW.

Die Tatverdächtigen in diesem Deliktsbereich sind - wie in den Vorjahren - fast ausschließlich männlich (95,6 %). Darüber hinaus weist die Polizeiliche Kriminalstatistik 53 (18) Fälle von gewerbs- bzw. bandenmäßiger Verbreitung von Kinderpornografie aus. Dies bedeutet eine Steigerung von 194 % gegenüber 2012.

Das **Tatmittel Internet** wurde bei der Verbreitung von Kinderpornographie in 604 Fällen (89,2 %), bei Besitz/Verschaffung von Kinderpornographie in 706 Fällen (83,3 %) und bei der Verbreitung von Kinderpornographie durch gewerbs- oder bandenmäßiges Handeln in 49 Fällen (92,5 %) erfasst.

[13] Distributed Denial of Service, Angriffe auf IT-Infrastruktur zwecks Überlastung bis zur Nichtverfügbarkeit der Dienste
[14] inklusive Delikte des Bereichs Kinderpornographie, sofern mit Tatmittel Internet begangen

Kinderpornographie mit Tatmittel Internet



2 Ermittlungshemmnisse

Die sinkende Aufklärungsquote der Cybercrime im engeren Sinne lässt sich mit den in der Polizeilichen Kriminalstatistik erfassten Daten nur unvollständig mit einer weitgehend korrelierenden Entwicklung der steigenden Fallzahlen erklären (vgl. 1.4). Obwohl die Polizei NRW seit Jahren die personellen und sächlichen Ressourcen stetig erhöht hat und ein als vorbildlich geltendes Fortbildungswesen betreibt, sinken die Aufklärungsquoten. Die Ursachen hierfür erscheinen vielfältig und werden nachfolgend beleuchtet.

2.1 Mindestdatenspeicherfrist

Wie bereits in den vergangenen Jahren hat sich im Jahr 2013 die fehlende Mindestdatenspeicherfrist von Verkehrsdaten auf die Aufklärungsquote ausgewirkt. Während die relevanten Daten von einigen Unternehmen für wenige Tage gespeichert werden, wird von anderen auf die Speicherung völlig verzichtet. Da elektronische Kommunikationsmittel in annähernd sämtlichen Bereichen der Cybercrime eingesetzt werden, stehen die für die Ermittlungen erforderlichen Daten als oftmals einzige Ermittlungsansätze in vielen Fällen nicht zur Verfügung.

Die Geschädigten bemerken den finanziellen Schaden meist erst nach einer Rechnungsstellung oder Prüfung von Kontoübersichten. Dies führt dazu, dass die Ermittlungen auf Grund fehlender Speicherfristen ergebnislos verlaufen.

Beispielsachverhalt:

Im Zuge der Auswertung eines Rechners, über den Missbrauchsabbildungen (Kinderpornografie) verbreitet worden waren, wurde festgestellt, dass der Beschuldigte über den Kommunikationsdienst ICQ mit 212 Personen Kinder- bzw. Jugendpornografie getauscht hatte. Letztlich wurden nur 113 Tatverdächtige ermittelt. In 99 Fällen (46,7 %) konnten aufgrund fehlender oder abgelaufener Speicherfristen die Personalien zu den angefragten IP-Adressen von den Providern nicht erlangt werden.

2.2 Anonymisierungspotenziale

Den im Internet agierenden Tätern ist häufig bewusst, dass sie über ihre IP-Adresse identifiziert werden können. Um dies zu vermeiden, nutzen sie verschiedene Möglichkeiten der Anonymisierung, beispielsweise durch Umleitung des Datenverkehrs über zwischengeschaltete Server[15]. Anbieter so genannter VPN-Dienste[16] werben damit, die Datenübertragung zwischen dem Computer des Benutzers und dem jeweiligen Ziel im Internet verschlüsselt über ihre im Ausland befindlichen Server umzuleiten und keine eigene Protokollierung vorzunehmen.

Eine darüber hinaus häufig genutzte Form der Anonymisierung erfolgt über das TOR-Netzwerk[17]. Dieser kostenlose Dienst besteht aus einer Vielzahl von weltweit verteilten Servern, über die die Datenpakete geleitet werden. Beim Verbindungsaufbau wird durch das Programm eine zufällige Route über einen Teil dieser Server festgelegt. Die Server führen keine Protokollierung über Herkunft oder Ziel der Daten. Die Notwendigkeit des TOR-Projekts wird mit der Möglichkeit begründet, unabhängig von Zensur oder politischer Verfolgung über etwaige Missstände berichten zu können. Als weiterer Grund für die Nutzung wird die durch TOR erhöhte Privatsphäre, zum Schutz vor der Analyse des Surfverhaltens der Nutzer durch Firmen oder den Staat, angegeben. Ein nicht unwesentlicher Anteil liegt jedoch nach kriminalpolizeilicher Erfahrung in der Nutzung des Netzwerks für kriminelle Zwecke. Über das TOR-Netzwerk erfolgt z. B. der Zugang zu dem so genannten Darknet[18]. Das Darknet bietet Kriminellen die Möglichkeit, innerhalb anonymer Serverstrukturen wie des TOR-Netzwerks Internetseiten zu betreiben, deren Inhalte angezeigt, deren tatsächlicher Standort jedoch nicht über die IP-Adresse ermittelt werden kann. Diese Möglichkeit nutzen Kriminelle, um z. B. illegalen Handel mit Drogen zu betreiben oder für die Verbreitung kinderpornografischen Materials. Dies führt dazu, dass die polizeilichen Ermittlungen nicht oder nur mit einem erheblich höheren Aufwand durchgeführt werden können.

Virtuelle Dienste wie z. B. „Voice/Fax-to-E-Mail“ sowie der Zugriff auf gespeicherte Daten (z. B. „Dropbox“) erfreuen sich durch die zunehmende Nutzung von Smartphones und Tablet-PCs einer immer größeren Beliebtheit. Die Anbieter dieser Dienste unterliegen dem Telemediengesetz, nicht aber dem Telekommunikationsgesetz und sind daher nicht in gleichem Maße zu technischen und/oder organisatorischen Maßnahmen verpflichtet wie die Telekommunikationsdienstleister.

2.3 Internationalisierung

Trotz der weltumspannenden Funktionsweise des Internets war in zurück liegender Zeit eine zumindest am jeweiligen Sprachraum, oft an den nationalen Grenzen orientierte Präferenz im Hinblick auf die Zielsysteme der Cyberkriminellen zu beobachten: Deutsche Hacker griffen meist auch deutsche Server an. Zwischenzeitlich haben insbesondere organisierte Tätergruppierungen mit kommerziellen Zielen sowie Online-Communities (z. B. Anonymous) diese Perseveranz aufgegeben. Zudem nutzen viele Täter Anonymisierungsmethoden, die auf der Weiterleitung über im Ausland befindliche Server basieren. Damit führen Ermittlungen immer häufiger und schneller zu Spuren, die nur noch im Ausland weiter verfolgt werden können. Der weitere Erfolg hängt dann von vielen Faktoren ab. In einigen Fällen können die erforderlichen Daten internationaler Konzerne von ausländischen Niederlassungen rechtmäßig auch ins Inland übermittelt werden, wo ein Zugriff mittels eines deutschen richterlichen Beschlusses möglich ist. In anderen Fällen bleibt lediglich der Weg über polizeiliche oder justizielle Rechtshilfeersuchen. Die Erfolgsaussichten richten sich dann nicht nur nach den jeweiligen Rechtshilfeabkommen, sondern auch nach der Leistungsfähigkeit und -willigkeit der dortigen Ermittlungsbehörden. Die Ermittlungschancen erhöhen sich gelegentlich sogar durch eine solche Konstellation, nämlich dann, wenn Rechtshilfeabkommen existieren und organisatorisch schnell und kompetent umgesetzt werden. Dann profitieren deutsche

[15] z. B. Proxy-Server
[16] VPN = Virtual Private Network
[17] TOR = The Onion Router, mehrschichtiges Servernetzwerk
[18] Darknet oder Hidden Services = versteckte Subnetze des Internet, die die Identität des Nutzers verbergen

Ermittlungsbehörden von der in nahezu allen Staaten geregelten Speicherung so genannter Vorratsdaten, während umgekehrt Rechtshilfeersuchen an deutsche Ermittlungsbehörden wegen der zu kurzen oder nicht vorhandenen Speicherung von Verbindungsdaten ins Leere laufen. In vielen Ermittlungsverfahren werden Rechtshilfeersuchen jedoch nicht oder zu spät beantwortet oder Rechtshilfeabkommen bestehen nicht.

2.4 Big Data[19]

Die polizeilich sichergestellten Datenmengen sind in den zurückliegenden Jahren angewachsen. Auch auf privat genutzten Computern von Opfern oder Straftätern können große Datenmengen gespeichert sein. So wurden allein in den Ermittlungskommissionen des Cybercrime-Kompetenzzentrums im Landeskriminalamt NRW im Jahr 2013 ca. 170 Terabyte Daten analysiert. Dies stellt die IuK-Forensik technisch und methodisch vor neue Herausforderungen. Neben den negativen Auswirkungen bietet „Big Data“ aber auch Chancen für die polizeilichen Ermittlungen.

[19] Der Begriff Big Data ist nicht einheitlich definiert, siehe umseitiger Expertenbeitrag des Herrn Geschonneck

Alexander Geschonneck

„Die zunehmende Verbreitung, Vernetzung und Komplexität von unterschiedlichsten, oft mobilen, Anwendungen und Systemen hat das weltweite Datenaufkommen in den letzten Jahren dramatisch erhöht. Hinzu kommt, dass die individuellen Speichermöglichkeiten auf privaten und geschäftlichen IT-Systemen ebenfalls steigen.
Das eigentlich Neue an „Big Data“ ist bei genauer Betrachtung nicht alleine die Datenmenge, sondern auch die ständig wachsende Vielfältigkeit und Vernetzung der Daten unterschiedlichster Quellen. Diese wird von den Anwendern mit der Erwartungshaltung verbunden, in Echtzeit Zusammenhänge zwischen den Daten herstellen zu können.
Im Hinblick auf forensische Untersuchungen bedeutet Big Data vor allem die Möglichkeit, umfassendere Erkenntnisse als bisher aus den vorhandenen Datenbeständen zu gewinnen. Dabei stehen zwei Herausforderungen im Vordergrund:

Erstens erfordert die Korrelation von Daten aus unterschiedlichen Quellen die detaillierte Kenntnis einer ständig wachsenden Zahl an Dateitypen, Artefakten und ihren Verbindungen. Dabei bestehen datenschutzrechtliche Risiken, wenn Herkunft und Inhalt der einzelnen Datenquellen nicht im Vorfeld bewertet wurden.
Zweitens sind nicht alle für die Untersuchung eines Sachverhalts zur Verfügung stehenden Daten für dessen Aufklärung auch von Bedeutung. Je nach Datenmenge ist eine manuelle Sichtung und Bewertung aller Daten zum Zeitpunkt der Untersuchung jedoch nicht praktikabel. Im Umgang mit Big Data gewinnt die forensisch sichere Identifikation potentiell relevanter Daten zur Eingrenzung der Menge der im Detail zu untersuchenden Daten deswegen zunehmend an Bedeutung. Diese Identifikation kann zum Beispiel über Filterung von Inhalt und Metadaten erfolgen. Dabei finden auch Big Data-spezifische Technologien zunehmend Anwendung, etwa bei der semantischen Analyse von Dateiinhalten, der automatischen Erkennung von Auffälligkeiten und der Visualisierung von Datenbeständen und Untersuchungsergebnissen. Die Datenreduktion ermöglicht nicht nur die Erfüllung datenschutzrechtlicher Anforderungen, sondern verkürzt häufig auch ressourcenintensive Auswertungsschritte.
Die Entwickler forensischer Software und die forensische Praxis stellen sich den aufgezeigten Herausforderungen zunehmend, und es ist davon auszugehen, dass IT-Forensik in Zukunft in vielen Fällen gleichbedeutend mit “Big Data Forensik” sein wird. Neben technischen Lösungen und standardisierten Prozessen ist jedoch die genaue Kenntnis vorhandener Daten und ihre routinemäßige Klassifizierung und Bewertung auch in der IT-Forensik ein Erfolgsfaktor - es gilt der Grundsatz: know your data.“

Alexander Geschonneck, KPMG AG Wirtschaftsprüfungsgesellschaft

2.5 Ubiquität des Internets und steigende Qualitätsanforderungen

In nahezu allen Bevölkerungsschichten ist die Nutzung des Internets zum selbstverständlichen Bestandteil des Alltags geworden. Die Miniaturisierung der erforderlichen Geräte fördert diese Entwicklung noch. Potenzielle Opfer wie Täter führen jederzeit komplexe IT-Systeme im Westentaschenformat mit sich und nutzen diese. Daher wird das Internet nicht nur immer häufiger unmittelbar zur Begehung von Straftaten genutzt, sondern die damit verbundenen Kommunikationsabläufe bilden zunehmend auch wichtige Ermittlungsansätze in allen klassischen Kriminalitätsphänomenen ab, vom Betrug bis zum Tötungsdelikt. Dies führt dazu, dass die Ermittlungskräfte in diesen Bereichen technische Ermittlungsmaßnahmen durchführen oder initiieren müssen, die noch vor wenigen Jahren ausschließlich den hoch spezialisierten Cyberkriminalisten und Kräften der IuK-Ermittlungsunterstützung vorbehalten waren. Auch die Anforderungen an diese Spezialisten steigen durch die beschriebene Entwicklung qualitativ und quantitativ stetig an. Sie leisten zudem mit einem wesentlichen Anteil der zur Verfügung stehenden Arbeitszeit auch ermittlungsun-

terstützende Hilfe in anderen, teilweise hoch priorisierten Kriminalitätsbereichen, wie z. B. bei Produkterpressungen. Eine weitere Folge dieser Entwicklung ist, dass der Fortbildungs-, Informations- und der Vernetzungsbedarf der Spezialisten in den letzten Jahren enorm gestiegen sind.

3 Darstellung und Bewertung ausgewählter Phänomene

3.1 Identitätsdiebstahl/Onlinebanking, mTAN

Cyberkriminelle wollen neben den Zugangsdaten für den Zugriff auf die Konten eines potentiell Geschädigten auch die notwendigen Transaktionsnummern (TAN) zur Ausführung von Überweisungen erlangen. Die Einführung neuer Sicherheitsvorkehrungen wie mTAN und TAN-Generatoren zur Autorisierung von Finanztransaktionen erschweren ihnen den Zugriff auf die nur kurzzeitig verwendbaren Transaktionsnummern. Hier bieten sich aufgrund der steigenden Verbreitung von Smartphones und Tablets neue Angriffsvektoren. Die Täter greifen mobile Endgeräte gezielt mit spezieller Schadsoftware an. Gelingt es den Tätern, Zugriff auf die Konten der Geschädigten zu erhalten sowie deren mobile Endgeräte zu kompromittieren, können mTAN auf Mobilgeräte der Täter umgeleitet und Überweisungen durchgeführt werden.

Beispielsachverhalt:
Die Geschädigte erhielt eine SMS. In der Kurzmitteilung befand sich ein Link sowie die Aufforderung, ein neues Sicherheitszertifikat für das Mobiltelefon herunterzuladen. Durch das Anklicken des Links wurde Schadsoftware auf dem Smartphone installiert. Der Täter erhielt dann die Kontodaten sowie Transaktionsnummern und überwies insgesamt 30.000 Euro auf ein Konto im Ausland.

(Grafik: Beispiel für ein angebliches Sicherheitszertifikat, tatsächlich Variante der Onlinebanking-Schadsoftware „ZEUS“ für Mobilgeräte.)
Quelle: GData Software AG

Mit einer anderen Variante verschafften sich die Täter Zugriff auf das Online-Banking-Konto des Opfers. Sie veranlassten die Ausstellung weiterer SIM-Karten zu den mit den Konten verbundenen Mobilfunknummern. Durch die Portierung der Rufnummern auf die neuen SIM-Karten konnten die Täter dann auch die TAN empfangen.

Im Jahr 2013 erfasste das Vorgangsbearbeitungssystem der Polizei NRW 3.177 Fälle (2.070) von Angriffen auf das Online-Banking. Hieraus ergibt sich im Vorjahresvergleich eine Steigerung um 53,5 %. Es entstand ein Schaden von 7.400.000 Euro, bei durchschnittlich 5.000 Euro pro Fall.


Candid Wüest

„Das Jahr 2014 markiert das zehnjährige Jubiläum für Malware auf mobilen Geräten und in dieser Dekade hat sich einiges verändert. Mobile Endgeräte wie Smartphones und Tablets sind allgegenwärtig und somit ein attraktives Ziel für die Angreifer geworden. Auf den verbreiteten Betriebssystemen gibt es derzeit ca. 7.500 bekannte Smartphone Schädlinge, mit unzähligen Varianten. Der häufigste Infektionsweg ist das Herunterladen und Installieren von infizierten Applikationen. Oft als Kopie von legitimen Spielen getarnt und auch auf offiziellen Märkten versteckt, werden diese Trojaner von ahnungslosen Benutzern installiert. In 32 % der Fälle – und somit am häufigsten – wird der Benutzer anschließend ausspioniert und seine Daten überwacht. Mit 15 % am zweithäufigsten ist der Versand teurer Premium SMS, welche dem Opfer einen finanziellen Schaden zufügen können. Leider ist die Unterscheidung nicht immer einfach. Sogenannte „Grayware", also Programme welche nicht per-se schädliches – aber sicher ungewolltes – Verhalten an den Tag legen, hat stark zugenommen. Im Jahr 2013 haben wir über 1,5 Millionen mobile Applikationen als Grayware identifiziert. Ein Exemplar versuchte zum Beispiel das Passwort eines sozialen Netzwerkes zu ergattern, indem es dem Benutzer versprach, mehr Freunde zu generieren. Diese App war kurzzeitig in allen offiziellen Märkten zu finden. Dies zeigt, dass kein Betriebssystem immun gegenüber Malware ist. Die Betreiber der Märkte sind stets bemüht, Malware Apps schnellstmöglich zu entfernen, was heutzutage auch meistens in unter zwei Tagen gelingt. Der rigorose Überprüfungsprozess einiger Hersteller zeigt hier einen Vorteil und macht es Malware fast unmöglich auf diesem Weg auf die Smartphones zu gelangen. Bis heute sehen wir eher selten den Einsatz von Exploits, um Schädlinge auf Smartphones zu installieren, wie wir es von der Desktop-Computer-Welt her kennen. Dies könnte sich ändern, sobald die Angreifer mit dem derzeitigen Modell nicht mehr erfolgreich sind.
Die mobilen Endgeräte werden auch in Zukunft weiterhin stark im Fokus der Angreifer stehen. Bereits jetzt greifen clevere Malware-Familien das Smartphone an, um zum Beispiel Zwei-Faktoren-Authentifizierung (2FA) wie mTAN erfolgreich auszuhebeln. Mit dem Aufkommen neuer mobiler Zahlungsmethoden auf Smartphones und der Nutzung von Tablets für das Online Banking erwarten wir hier eine deutliche Zunahme der Angriffe.
Es ist also unabdingbar, das Anwender ihre mobilen Geräte ausreichend schützen, egal ob diese privat oder geschäftlich genutzt werden – sofern sich dies überhaupt noch trennen lässt. Bei der Installation von neuen Applikationen sollten Nutzer Vorsicht walten lassen und die Berechtigungen genau überprüfen."

Candid Wüest, Principal Threat Researcher, Symantec

3.2 Erpressung mit Tatmittel Internet

Die unterschiedlichen Modi Operandi der Erpressung mit Tatmittel Internet gehen meist mit der Verwirklichung klassischer Cybercrimedelikte wie Datenveränderung/Computersabotage einher. Neben den hohen Fallzahlen der Ransomware registriert der Kriminalpolizeiliche Meldedienst (KPMD)[20] auch Erpressungsfälle, die gezielt gegen Personen oder Unternehmen gerichtet sind.

Ransomware

Ransomware ist eine Schadsoftware, die Computersysteme sperrt und/oder verschlüsselt und den Nutzer anschließend zu einer Zahlung auffordert. Dem Geschädigten wird suggeriert, dass der Computer durch eine Behörde oder eine anderen Organisation (Bundespolizei, BKA, GEMA) aufgrund der Verbreitung kinderpornografischer Schriften oder eines Verstoßes gegen das Urheberrecht gesperrt wurde. Um den

[20] Bundesweiter Nachrichtenaustausch der Polizeien zur Erkennung von Tatzusammenhängen, Erlangung von Hinweisen auf Täter und Erfassung von Straftaten von herausragender Bedeutung

Sperrmeldungen einen formellen Charakter zu verleihen, werden z. B. offizielle Logos der Behörden verwendet. Den Opfern wird vorgetäuscht, dass die Sperrung gegen Leistung einer Zahlung über ein elektronisches Zahlungssystem wie Bitcoin[21] oder Ukash[22] aufgehoben werde.

Die Schadsoftware wird überwiegend durch Anhänge in massenhaft versandten E-Mails und durch die Manipulation von Web-Seiten (Drive-by infection) verbreitet. Durch die Manipulation von Werbebannern bei Advertising Providern[23] erreichen die Kriminellen eine enorme Reichweite innerhalb kürzester Zeit. In einer Variante[24] wird der Forderung durch einen Countdown Nachdruck verliehen. Dieser gibt den vermeintlich verbleibenden Zeitraum an, in dem das System noch entsperrt werden könne.

(Grafik: Beispiel für den Countdown bei der Ransomware Cryptolocker)

Auch bei der Betrugsvariante per Telefon, bei der sich der Täter als Servicemitarbeiter eines Softwareunternehmens ausgibt und unter Vorwand zu einer Zahlung auffordert, wird in einigen Fällen Ransomware eingesetzt. Unter Vorspiegelung, dass auf dem Computer ein Programm zur Beseitigung von Schadsoftware installiert werden müsse, bringen die Täter ihre Opfer dazu, die eigentliche Schadsoftware aus dem Internet herunterzuladen und auszuführen.

Erpressung in Social Media[25]/Sexting[26]

Im Verlauf des Jahres 2013 konnte ein neuer Modus Operandi im Zusammenhang mit Erpressungen mit Tatmittel Internet festgestellt werden. Die Täter erschleichen sich hierbei während eines Chats das Vertrauen der Geschädigten und veranlassen diese, sexuelle Handlungen an sich vorzunehmen. Mit den dabei gefertigten Aufnahmen werden die Geschädigten im Anschluss erpresst.

Beispielsachverhalt:

Der Geschädigte chattete in einem sozialen Netzwerk mit einer ihm unbekannten Frau. Im Verlaufe des Gesprächs äußerte die Frau den Wunsch, den Geschädigten sehen zu können und schlug den Wechsel auf eine Videochat-Plattform vor. Nachdem der Geschädigte die Verbindung hergestellt hatte, sah er eine junge Frau, die aufreizend tanzte und sich langsam ihrer Kleidung entledigte. Der Aufforderung, es ihr

[21] Virtuelle Währung als elektronisches Zahlungsmittel
[22] Elektronisches Zahlungsmittel
[23] Anbieter für Werbeanzeigen auf Webseiten, z. B. Werbebanner
[24] Z. B. Cryptolocker
[25] Soziale Medien, ermöglichen den Nutzern sich mittels digitaler Medien und Technologien untereinander auszutauschen.
[26] Abgeleitet aus den Wörtern „sex“ und „texting“, gegenseitiges Zusenden von Abbildungen sexueller Handlungen

nachzutun sowie sexuelle Handlungen an sich selbst vorzunehmen, kam der Geschädigte nach. Im Anschluss erhielt er einen Link für ein Videoportal und sah dort eine Aufzeichnung seiner soeben vorgenommenen Handlungen. Unter Androhung, die Aufnahme an alle Freunde im sozialen Netzwerk zu senden, wurde von einem nun agierenden männlichen Täter eine sofortige Geldüberweisung gefordert.

Erpressung von Unternehmen

Auch im Jahr 2013 wurden Unternehmen Opfer von gezielten Angriffen von Cyberkriminellen. Sie wurden entweder nach dem Ausspähen unternehmensinterner Daten oder im Zuge von DDoS-Attacken zu Zahlungen aufgefordert.

Beispielsachverhalt:

Per DDoS-Angriff wurde der Webserver eines Unternehmens attackiert, wodurch dessen Online-Shop mehrere Tage lang nicht erreichbar war. Die Täter meldeten sich per E-Mail, forderten 10.000 Euro und kündigten bei Verweigerung der Zahlung weitere Angriffe an.

3.3 Mobile Endgeräte (Smartphones/Tablets)

In der Polizeilichen Kriminalstatistik werden die jeweils angegriffenen Systeme nicht erfasst. Das Vorgangsbearbeitungssystem der Polizei NRW weist für den Bereich Cybercrime[27] 26 Fälle von Angriffen auf mobile Endgeräte sowie 407 Fälle von Phishing beim Online-Banking mit mTAN aus. Diese Angriffe dienen jedoch meist der Vorbereitung einer sich anschließenden Verwertungstat, z. B. einer missbräuchlichen Kontoüberweisung. Sie werden daher weder in der Polizeilichen Kriminalstatistik noch im Vorgangsbearbeitungssystem der Polizei NRW gesondert erfasst. Erkenntnisse aus einzelnen Ermittlungsverfahren zeigen jedoch, dass Angriffe auf mobile Endgeräte ohne umfangreiche forensische Analysen häufig unentdeckt bleiben. Diese sind nicht in jedem Ermittlungsverfahren durchführbar. Es ist daher von einem großen Dunkelfeld auszugehen.

Beispielsachverhalt:
Der Geschädigte lud sich eine kostenlose App auf sein Smartphone. Durch Anklicken eines Werbebanners wurde das Smartphone mit einer Schadsoftware infiziert, die das Passwort des E-Mail-Accounts ausspähte. Anschließend wurde das E-Mail-Konto des Geschädigten zum Versand von Ransomware benutzt.

[27] Ohne sonstige Straftaten mit Tatmittel Internet

Thomas Tschersich

"Die Telekom beobachtet die Gefahrenlage im Netz kontinuierlich und hat ein Frühwarnsystem aufgebaut. Dazu gehören mittlerweile 180 weltweit eingesetzte Locksysteme - so genannte Honeypots. Wir simulieren damit unter anderem auch leicht angreifbare Smartphones. Die Anzahl der Angriffe nimmt stetig zu. Mit den Honeypots können wir das Verhalten von Angreifern analysieren und neue Trends identifizieren. Unsere Erkenntnisse teilen wir dann beispielsweise mit den Herstellern von Schutzsoftware, so dass sie ihre Programme verbessern können. Im letzten Jahr haben wir wieder eine deutliche Zunahme der Angriffe auf Mobiltelefone gesehen.

So stieg die Zahl der Angriffe auf die mittels solcher Honeypots simulierten Smartphones von insgesamt 345.017 im Jahr 2012 auf 1.486.096 im Jahr 2013.

Eine Ursache dafür dürfte darin liegen, dass diese Geräte im Gegensatz zu klassischen PCs deutlich schlechter gesichert sind. Viele Kunden setzen hier keine besonderen Sicherheitspakete ein. Wir empfehlen unseren Kunden, die entsprechende Sicherheitssoftware zu nutzen und stets die aktuellsten Sicherheitsupdates einzuspielen."

Thomas Tschersich, Senior Vice President Group Cyber- and Datasecurity Deutsche Telekom AG, Vorsitzender LA Sicherheit, BITKOM e. V.

3.4 Skimming/PoS-Terminals[28]

Die Zahl der Skimming-Fälle ist weiterhin rückläufig. Im Vergleich zu den 212 Skimming-Manipulationen mittels so genannter Vorsatzgeräte an Geldautomaten im Jahr 2012 ist die Anzahl der Fälle im Jahr 2013 auf 128 Fälle gesunken. Im zweiten Halbjahr 2013 wurden im polizeilichen Vorgangsbearbeitungssystem nur noch 14 Fälle dieser Art erfasst.

Sicherungsmaßnahmen der Kreditwirtschaft durch den Austausch veralteter Geldautomaten und Maßnahmen zur Betrugsabwehr greifen zunehmend. Vor allem die Einführung des EMV-Chips[29] und die zunehmende Einrichtung von Auslandstransaktionssperren für Länder ohne Chip-Prüfung erschweren den Tätern die Verwirklichung von Verwertungstaten wie das Cashing[30]. Gleichzeitig ist jedoch eine zunehmende „Qualitätssteigerung“ bei der Manipulation von PoS-Terminals festzustellen. So konnte beispielsweise nur durch eine aufwendige forensische Untersuchung im Cybercrime-Kompetenzzentrum des Landeskriminalamts NRW eine Manipulation mit hochwertigen technischen Bauteilen (einschließlich Bluetooth-Sendeempfänger) nachgewiesen und auf der Grundlage der so gewonnenen Erkenntnisse in Zusammenarbeit mit dem BKA ein Tatzusammenhang zu gleichgelagerten Straftaten hergestellt werden. Äußerlich war das PoS-Terminal einschließlich vorhandener Klebesiegel unversehrt.

Nachdem im Jahr 2012 bei Manipulationen an PoS-Terminals eine deutliche Steigerung im Vergleich zum Vorjahr zu verzeichnen war (2011: 9 Fälle, 2012: 47 Fälle), setzte sich dieser Trend im Jahr 2013 nicht fort. Der Rückgang auf 24 erkannte Manipulationsfälle im Jahr 2013 lässt sich den Reaktionen des Handels durch mechanische Sicherungs- sowie technische und optische Überwachungsmaßnahmen und den Verwertungshemmnissen im Ausland zurechnen. Eine erfolgreiche Verwertung erlangter Zahlungskartendaten wurde in lediglich vier Fällen bekannt. Der Gesamtschaden betrug 341.311,78 Euro[31].

Obwohl die Täter in diesem Phänomenbereich im Jahr 2012 noch hohe Gewinne im sechsstelligen Bereich erzielen konnten, sanken die Fallzahlen im Jahr 2013. Hier zeigt sich, welche Wirkung die konsequente und flächendeckende Anwendung technischer Sicherungsmaßnahmen entfalten kann. Dies unter-

[28] Point of Sale; Kartenzahlterminals im Handel
[29] Sicherheitstechnik im Kartenzahlungsverkehr als Nachfolger des Magnetstreifens
[30] Abhebung von Bargeld mittels Kartendubletten
[31] Nach Angaben der EURO Kartensysteme GmbH (EKS)

streicht auch die Verantwortung der betroffenen Unternehmen bei der Bekämpfung zukünftiger Modi Operandi.

3.5 Telekommunikationsanlagenmanipulation

Die Anzahl der im polizeilichen Vorgangsbearbeitungssystem erfassten Fälle von Manipulationen an Telekommunikationsanlagen hat sich mit 220 Fällen (103) im Vergleich zum zurückliegenden Jahr mehr als verdoppelt. Die Schadenssumme hat sich mit etwa 900.000 Euro[32] nahezu verdreifacht. Die Täter verschafften sich vorwiegend an Wochenenden bzw. außerhalb der Arbeitszeiten über bekannte Schwachstellen in der Kommunikationssoftware und mangelnde Zugangssicherungen Zugriff auf die Anlagen. Die Systeme wurden missbraucht, um kostenintensive Auslandsgespräche zu führen und Premium- bzw. Mehrwertdienste in Anspruch zu nehmen. Im Jahr 2013 gerieten auch private Telefonanlagen in den Fokus der Kriminellen. Die Täter griffen Router[33] von Privathaushalten über Schwachstellen in der Firmware[34] an. Von 220 in NRW erfassten Fällen wiesen 56 diesen Modus Operandi auf.

Beispielsachverhalt:

Unbekannte Täter hackten sich über die Mobilboxfernabfrage in das computergesteuerte Telefonnetz einer Firma ein und führten 500 Gespräche mit insgesamt 4.500 Gesprächsminuten in den Kongo. Der wirtschaftliche Schaden beläuft sich nach ersten Schätzungen auf etwa 5.000 Euro.

Martin
Bürstenbinder

Telekommunikationsanlagen vor Manipulation schützen

"Das Hacken von TK-Anlagen mit dem Ziel des Gebührenbetrugs hat im Verlauf des Jahres 2013 bundesweit einen sehr deutlichen Zuwachs erfahren. Dies betrifft sowohl die uns bekannt gewordenen Fallzahlen als auch die Höhe der Schadenssummen. Zwar können umfassende Schutzkonzepte für TK-Systeme durchaus komplexe Anforderungen darstellen. Jedoch war zu beobachten, dass die Täter in vielen Fällen leichtes Spiel hatten. Denn selbst sehr einfache und zugleich effektive Vorbeugungsmaßnahmen finden in Unternehmen oft keine Anwendung. Ein Beispiel ist das hochriskante Belassen von einfachen, werkseitigen Standardpasswörtern in persönlichen Sprachboxen.

Die Möglichkeiten der Problemsensibilisierung und Aufklärung spielten darum eine wichtige Rolle in den Gesprächen mit dem Cybercrime-Kompetenzzentrum des LKA NRW und im Herbst wurde die Konzipierung einer Präventionsbroschüre in Angriff genommen. Weite Fachkreise beteiligten sich an der Ausarbeitung. Dank der pragmatischen Zusammenarbeit mit dem Cybercrime-Kompetenzzentrum des LKA NRW und der Ergebnisorientiertheit aller Beteiligten konnte die Veröffentlichung im Web und als Druckerzeugnis bereits im Januar 2014 erfolgen. Unter dem Titel „Wichtige Hinweise für den Schutz Ihres Telekommunikationssystems“ informieren das LKA NRW und die Bundesverbände BITKOM und VAF in zielgruppenorientierter Aufbereitung zur Problemlage sowie zu wichtigen Schutzmaßnahmen. Bisher wurden zudem einige zehntausend Druckexemplare an Unternehmen verteilt. Aus unserer Sicht wurde hier in kurzer Zeit ein wichtiger Baustein für die Prävention geschaffen.“

Martin Bürstenbinder, Geschäftsführer des VAF, Bundesverband Telekommunikation e. V.

[32] Im polizeilichen Vorgangsbearbeitungssystem wurden in 164 Fällen Schäden erfasst
[33] Netzwerkgerät beispielsweise zur Anbindung von Netzwerken und den daran angeschlossenen Endgeräten an das Internet
[34] Betriebssystem des Routers

3.6 Kinderpornografie/Missbrauchsabbildungen

Die Polizei nutzt im Zusammenhang mit Kinderpornografie die auch im internationalen Sprachgebrauch verwendete Bezeichnung „Missbrauchsabbildungen“. Durch Verbreitung der Missbrauchsabbildungen über Datennetze kommt es zu einer andauernden Viktimisierung der kindlichen Opfer. Die persönlichen Folgen für die Opfer währen oft ein Leben lang, z. B. in Form gestörter Sexualität, körperlicher Probleme, Suchtverhalten, Prostitution, Suizid. Nicht selten werden männliche Opfer zu Tätern[35].

Nicht alle Konsumenten von Missbrauchsabbildungen sind sexuelle Missbraucher, aber einer Studie zu Folge ist jeder Konsument auch ein potentieller sexueller Missbraucher[36]. Dauerhafter und exzessiver Konsum dieses Materials kann nach kriminalistischen Erkenntnissen den Wunsch, selbst Kinder zu missbrauchen, fördern und zum realen Missbrauch führen. Daher ist eine konsequente Strafverfolgung in diesem Deliktsbereich unerlässlich.

Sebastian Gutknecht

Folgen sexuellen Missbrauchs für Opfer

„Wenn Mädchen und Jungen sexuell missbraucht werden, kann dies unterschiedliche Folgen haben. Die Folgen sind abhängig von der Intensität und Dauer des Missbrauchs, vom Grad der Abhängigkeit zu dem Missbrauchenden, vom Entwicklungsalter des Kindes und den sozialen Beziehungen der Mädchen und Jungen. Auch das Geschlecht des betroffenen Kindes kann eine Rolle spielen, wie das Erlebte verarbeitet wird.
Die Folgen von sexuellem Missbrauch sind um so größer, je größer die verwandtschaftliche Nähe zwischen Täter und Opfer ist, je länger die Tathandlungen andauern, je jünger das Kind bei Beginn der Tat ist, je mehr Gewalt angedroht und angewendet wird, je mehr Druck auf das Kind ausgeübt wird und je weniger Personen dem Kind als Ansprechpartner zur Verfügung stehen.

Jedes Kind reagiert individuell auf Missbrauchssituationen. Einige missbrauchte Kinder können Angststörungen, Depressionen, ein geringes Selbstwertgefühl sowie Essstörungen entwickeln. Es können Auffälligkeiten wie z. B. intime Distanzlosigkeit oder nicht altersgemäße sexuelle Aktivitäten auftreten.
Bei anderen Kindern können Schlafstörungen, sozialer Rückzug, plötzlicher Leistungsabfall, Aggressivität oder auch psychosomatische Beschwerden wie Kopf- oder Bauchweh Folge eines sexuellen Missbrauchs sein. Manche Kinder fügen sich selbst Verletzungen zu, bleiben der Schule fern oder reißen aus.
Die genannten Verhaltensänderungen können in Folge eines sexuellen Missbrauchs auftreten. Hintergrund können aber auch organische Krankheiten, andere traumatische Erfahrungen wie z. B. Todesfälle im nahen Umfeld, Verkehrsunfälle oder die Trennung der Eltern sein. Die Ursache sollte jedoch abgeklärt werden, denn alle Verhaltensänderungen signalisieren, dass ein Kind Probleme hat und Hilfe benötigt.

Wie schwer und tiefgreifend die Auswirkungen von sexuellem Missbrauch sind, hängt sehr von den Reaktionen des Umfelds ab. Kinder müssen keine Langzeitfolgen entwickeln, auch wenn sie zunächst starke Auffälligkeiten zeigen. Entscheidend ist, dass Eltern die Aussagen von Mädchen und Jungen nicht infrage stellen, sie vor weiterer Gewalt schützen und ihnen zeitnah Hilfe bei der Verarbeitung der belastenden Erlebnisse anbieten.“

Sebastian Gutknecht, Geschäftsführer Arbeitsgemeinschaft für Kinder- und Jugendschutz, Landesstelle Nordrhein-Westfalen e. V.

[35] Vgl. Priv. Doz. Dr. Manuela Dudeck, Universität Greifswald, „Langstrafenvollzug und die Frage der Menschenrechte in Staaten der Europäischen Union, 2006-2008“,
[36] Vgl. Seto / Cantor, Universität Toronto (2006) „Child Pornography Offenses Are a Valid Diagnostic Indicator of Pedophilia“

Beispielsachverhalt:
Ein Jahr lang fahndeten Ermittler des Landeskriminalamts NRW nach einem Kind und dessen Peiniger. Der Mann hatte das Kind über Jahre missbraucht und die Vergewaltigungsszenen auf Fotos und Filmen an Gleichgesinnte im Internet verteilt. Er sperrte das Kind in einen Käfig, entzog es einer nennenswerten Schulbildung und stellte es weiteren Tätern, die teilweise aus Übersee anreisten, für sexuelle Handlungen zur Verfügung. Durch aufwändige Maßnahmen wurden die Täter ermittelt und das Kind befreit.

3.7 Cyber-Grooming

Cyber-Grooming bezeichnet die Kontaktaufnahme erwachsener Täter mit Kindern oder Jugendlichen mittels Internet zur Anbahnung sexueller Handlungen.

Laut Polizeilicher Kriminalstatistik sind in NRW im Jahr 2013 insgesamt 275 Fälle (178) bekannt geworden, die unter § 176 Abs. 4 Nr. 3 oder 4 StGB subsumiert werden können. Dies stellt eine Steigerung von 54,5 % dar. Dabei handelt es sich um Einwirkungen auf Kinder, um sexuelle Handlungen zu bewirken bzw. Einwirkungen auf Kinder mittels pornografischer Inhalte. Der Versuch ist gem. § 176 Abs. 6 StGB nicht strafbar. In der Polizeilichen Kriminalstatistik wird bei diesem Delikt die Begehung mit dem Tatmittel Internet nicht gesondert erfasst. Konkrete Fallzahlen zum Cyber-Grooming liegen daher nicht vor.

Die Opfer bewerten oftmals ein solches Verhalten zunächst nicht als strafbare Handlung. Für viele Kinder und Jugendliche ist die Annäherung mit sexuellen Motiven bereits selbstverständlicher Teil der Kommunikation im Internet. Die Polizei erhält daher häufig keine Kenntnis von solchen Sachverhalten. Es ist von einem großen Dunkelfeld auszugehen.

Beispielsachverhalt:
Ermittler der Zentralen Internetrecherche des Landeskriminalamts NRW identifizierten in einem Fall von Cyber-Grooming einen 32-jährigen Tatverdächtigen. Der Mann suchte in sozialen Netzwerken Chat-Kontakt zu offensichtlich Minderjährigen. Er sendete ihnen Nachrichten mit sexualbezogenem Inhalt und versuchte, reale Treffen mit ihnen zu verabreden. Über die Notruffunktion im Chat gingen 228 Notrufe bei dem Chat-Betreiber ein, die dem Tatverdächtigen zugeordnet werden konnten. Der Tatverdächtige konnte ermittelt werden, er verwendete 37 Pseudonyme. Zu einem realen Treffen zwischen den Minderjährigen und dem Tatverdächtigen ist es nicht gekommen.

4 Initiativen

4.1 Prävention

Polizeiliche Kriminalprävention im Bereich Cybercrime

Die Arbeit der polizeilichen Kriminalprävention konzentriert sich auf polizeilich relevante Vorbeugungsthemen. Betrachtet man dies im Kontext der vollflächigen Vernetzung und der hohen Nutzungsrate digitaler Medien, wird deutlich, dass die Polizei andere wesentliche Akteure in die Bewältigung dieser Aufgabe einbinden muss.

Die Prävention von Cybercrime im Land Nordrhein-Westfalen ist auf den Bereich der Verhaltensprävention ausgerichtet. Für die technische Prävention hat sich neben dem Bundesamt für Sicherheit in der Informationstechnik (BSI) ein ganzer Wirtschaftszweig etabliert. Hier hat sich vernetztes und aufeinander abgestimmtes Handeln bewährt.

Ein Beispiel für die Vernetzung mit Experten aus der Wirtschaft ist die Sicherheitskooperation Cybercrime, die der BITKOM e. V. und das Landeskriminalamt NRW 2011 vereinbarten. Ein Ziel der Sicherheitskooperation ist die Verbesserung der Prävention im Bereich Cybercrime. In mehreren gemeinsamen Projekten konnte das bereits erreicht werden. So arbeiten der BITKOM e. V. und das Landeskriminalamt

NRW gemeinsam im Landespräventionsrat NRW mit anderen Behörden und Einrichtungen zum Thema Prävention von Cybercrime. In diesem Kontext entwickelte sich das Filmkonzept „Sichere Netzwelten“.

Sichere Netzwelten

Didaktisches Konzept zu den Filmen „Sichere Netzwelten“

Die Filme „Sichere Netzwelten“ haben das Ziel, ein Bewusstsein für die Gefahren im Bereich Cybercrime zu entwickeln (Awareness). Gemeinsam arbeiten Lehrer und die Verbraucherzentrale NRW an einem didaktischen Konzept, das die Filme einbindet. Das didaktische Konzept ist anwenderfreundlich, da es keine besonderen Vorkenntnisse voraussetzt und zielgruppenunabhängig umsetzbar ist. Die Awareness-Filme sind unabhängig voneinander variabel einsetzbar.

Didaktisches Konzept

Zeigen des Films	Kooperatives Lernen	Erneutes Zeigen des Films	eigene Lösungen
Film als Einstieg in die jeweilige Thematik	Teilnehmer erarbeiten sich die Problematik selbst	Fokus auf Botschaften und Tipps der Experten	Erarbeiten eigener Lösungsansätze

Filme zum Thema „Cyber-Mobbing“

Der Landespräventionsrat NRW hat im Herbst 2013 die Filmreihe „Cyber-Mobbing“ produziert. Das Cybercrime-Kompetenzzentrum im Landeskriminalamt NRW koordinierte die Beiträge der Kooperationspartner sowie die Dreharbeiten. Die Reihe besteht aus vier Filmen und einem Making-of und stellt einen konkreten Mobbing-Fall dar. Dieser Mobbing-Fall wird aus unterschiedlichen Perspektiven dargestellt. Der erste Film zeigt die Sicht des Täters, seine Motivation und die Mobbing-Handlung. Der zweite Film zeigt die Perspektive des Opfers. Im dritten Film wird das Umfeld des Cyber-Mobbings dargestellt. Alle drei Filme werden von Experteninterviews begleitet, die das Cyber-Mobbing strafrechtlich bewerten, die psychischen Folgen für die Opfer beleuchten sowie die Bedeutung des Umfeldes aufzeigen. Der vierte Film führt die verschiedenen Perspektiven chronologisch zusammen. Das Making-of gibt Einblicke in die Produktion der Filmreihe. In O-Tönen kommen die Experten, Darsteller sowie der Regisseur zu Wort.

Der Landespräventionsrat NRW bietet auf der Interseite der Justiz NRW alle Filme zum freien Download[37] an.

[37] https://www.justiz.nrw.de/JM/praevention/computerkriminalitaet/index.php, Stand: 05.05.2014

Neuausrichtung im Bereich Prävention Cybercrime

Smarthome-Technologie und digitale Hausvernetzung mit rasanten Verbreitungsraten stellen die klassische technische Prävention zum Thema Einbruchschutz vor neue Herausforderungen. Das Gleiche gilt für die an Zielgruppen ausgerichtete Verhaltensprävention. Vor allem die Senioren entdecken das Internet für sich und stellen die Nutzergruppe mit den höchsten Zuwachsraten dar. Hier sind neue Präventionskonzepte und Handlungsempfehlungen gefordert.

Im Jahr 2013 beteiligte sich die Polizei NRW an der Aktionswoche „Internet“ der BAGSO (Bundesarbeitsgemeinschaft der Senioren-Organisationen). Das Landeskriminalamt NRW entwickelte ein Handlungskonzept sowie einen Standardbaukasten für Vorträge. Die Filme „Sichere Netzwelten“ sind integriert. Mit diesem Material beteiligten sich zehn Polizeibehörden des Landes NRW an der Aktionswoche. Die Planungen für das Jahr 2014 setzen hier aufgrund der positiven Resonanzen nahtlos an.

Barbara Keck

BAGSO-InternetWoche: **Die Älteren erobern das Netz!**

„Anlässlich des Internationalen Internettages startete die BAGSO am 29. Oktober 2013 die 2. BAGSO-InternetWoche. Vom 29. Oktober bis 4. November 2013 fanden bundesweit verschiedene Aktionen und Veranstaltungen statt, sowohl bei und mit den BAGSO-Verbänden als auch mit weiteren Partnern. Die Partner der BAGSO-InternetWoche waren in diesem Jahr die Deutsche Telekom AG und das soziale Netzwerk seniorbook. Insgesamt 53 Mitwirkende griffen in 75 bundesweiten und regionalen Informationsveranstaltungen, Kursen und Workshops sowie Umfragen, Checklisten und Tipps die Themen der InternetWoche auf. Diese waren:

1. Chancen des Internets – Ich nutze das Internet, weil …
2. Vernetzung und soziale Netzwerke – So geht’s!
3. Sicherheit im Netz – Datenschutz, Privatsphäre
4. Mobil ins Internet – Tablet-PC, Smartphone und E-Book
5. Barrierefrei durch das Internet – Barrierefrei im Internet
6. Ehrenamt und Internet – Tue Gutes und rede im Internet darüber
7. Internet und Bildung – Bequem und vielfältig

Zudem konnten alle Interessierten während und nach der InternetWoche aktiv ihre Erfahrungen, Fragen, Meinungen und Tipps im sozialen Netzwerk seniorbook weitergeben.

Mit der InternetWoche wollten wir erreichen, dass diese Menschen anderen berichten, wie sie das Internet nutzen. Sie sollten anderen Mut machen und zeigen: Da sind welche, die nutzen das Netz ganz selbstverständlich und ziehen für sich daraus einen echten Mehrwert Denn mittlerweile sind über 60% der über 60-Jährigen und immerhin 26% der über 70-Jährigen im Netz aktiv. Es gibt sie also, die älteren Menschen, die die Chancen des Internets für sich entdeckt haben.“

Dr. Barbara Keck, Geschäftsführerin der BAGSO Service Gesellschaft

Prävention vor Ort

2013 hat sich das regionale Netzwerk „s.i.n.us – Sicher im Netz unterwegs“[38] mit den Themen Datensicherheit in sozialen Netzwerken, Online-Betrug und Smartphone-Apps sowie Cyber-Mobbing befasst. Das Netzwerk ist ein Zusammenschluss von Institutionen aus den Bereichen Schule, Eltern, Jugend- und Suchthilfe und der Kreispolizeibehörde Rhein-Kreis Neuss. Durch diese Kooperation kann das breite Spektrum der Cybercrime umfassend in Veranstaltungen abgebildet werden. Ein Themenschwerpunkt der Kreispolizeibehörde Rhein-Kreis Neuss ist die Datensicherheit in Sozialen Netzwerken. Das Projekt fördert die Medienkompetenz von Schülern, Lehrern und Eltern. Es informiert die jeweiligen Zielgruppen über die möglichen Risiken sowie die sichere und verantwortungsbewusste Internetnutzung.

Bistand

„Bistand“ behandelt das Thema Cyber-Mobbing für Schüler der Jahrgangsstufen fünf bis zehn. An der Kampagne „Bistand“ des Gremiums „Sicherheit in Rheine“ (SIR) beteiligt sich auch die Kreispolizeibehörde Steinfurt[39]. Der Name „Bistand“ stammt aus dem Plattdeutschen und bedeutet „Helfer“ oder „Beschützer“. Ausgangspunkt ist eine anonyme Umfrage unter Schülern in Rheine im Frühjahr 2012 mit dem Ergebnis: Cyber-Mobbing ist ein Problem an den Schulen. Nach den Sommerferien 2012 wurde an allen weiterführenden Schulen in Rheine ein Informations- und Medienpaket verteilt, um das Thema im Unterricht zu behandeln. Am Ende des Unterrichts stehen eine Selbstverpflichtungserklärung zum verantwortungsvollen Umgang mit dem Internet sowie eine Bescheinigung in Form einer Scheckkarte. Geplant ist im Frühjahr 2014 in einer erneuten Umfrage zu überprüfen, ob die Kampagne erfolgreich ist.

4.2 Kooperation des Landeskriminalamts NRW mit der Fachhochschule Aachen

Die für beide Seiten gewinnbringende und bereits im Lagebild 2012 erwähnte Kooperation zwischen dem Cybercrime-Kompetenzzentrum des Landeskriminalamts NRW und der Fachhochschule Aachen konnte erfolgreich mit weiteren Praxissemestern, einem Workshop zur forensischen Software X-Ways[40] in der Fachhochschule Aachen und dem Ausbau einer im Landeskriminalamt NRW eingerichteten Mobilfunkzelle[41] fortgeführt werden.

[38] http://www.sinus-netzwerk.de/home/, Stand: 05.05.2014
[39] https://www.polizei.nrw.de/steinfurt/artikel__2602.html, Stand: 05.05.2014
[40] Produkt der X-Ways AG
[41] Zu Testzwecken in einem abgeschirmten Raum eingerichtet

4.3 Workshop mit kleinen und mittelständischen Unternehmen in Oberhausen

Ein weiterer Baustein im Bereich „Sicherheitskooperation Cybercrime“[42] ist die Entwicklung eines zweitägigen Workshop-Konzepts für kleine und mittelständische Unternehmen (KMU). Mit diesem Konzept sollen die örtlichen Polizeibehörden dem höheren Beratungsbedarf und der Beratungstiefe der Zielgruppe KMU nachkommen können.
Im Rahmen der Sicherheitskooperation Cybercrime fand am 27. und 28.11.2013 ein Workshop für kleine und mittelständische Unternehmen in Oberhausen statt. Das Polizeipräsidium Oberhausen sowie Partner aus der örtlichen Wirtschaft richteten gemeinsam mit dem Landeskriminalamt NRW die Veranstaltung aus, unterstützt durch den Kooperationspartner BITKOM e. V. Ziel der Veranstaltung war die Sensibilisierung der IT-Verantwortlichen der örtlichen KMU sowie die Vernetzung der örtlichen Wirtschaft und lokaler Polizei.
Verschiedene Phänomene der Cybercrime, wie die Arbeitsweise von Schadsoftware und Varianten zur Durchführung von DDoS-Angriffen wurden veranschaulicht. Die Teilnehmer konnten die Szenarien an vorbereiteten Rechnern „live“ miterleben und versuchen, selbst Gegenmaßnahmen zu ergreifen. Kriminalbeamte des Fachkommissariats des Polizeipräsidiums Oberhausen erläuterten das polizeiliche Vorgehen und gaben Handlungs- sowie Präventionsempfehlungen. Den Abschluss bildete ein gemeinsamer Erfahrungsaustausch im Plenum.
Die Rückmeldungen der Teilnehmer am Ende des zweitägigen Workshops waren positiv. Die im Vorfeld gesteckten Ziele, die Möglichkeit einer kostenlosen und effizienten Sensibilisierung der IT-Verantwortlichen im Bereich Cybercrime sowie der Vertrauensaufbau zwischen örtlicher Wirtschaft und Polizei konnten erreicht werden. Eine Fortsetzung des erfolgreichen Pilotprojekts mit weiteren Polizeibehörden ist geplant.

Dieter Kempf

„Die ITK-Branche muss der natürliche Ansprechpartner der Behörden sein, wenn es um die Cybersicherheit geht, da es sich hierbei um ihr ureigenes Aufgabenfeld handelt. Durch die Sicherheitskooperation Cybercrime wurde eine vertrauensbasierte Grundlage gelegt, die es allen Beteiligten ermöglicht, in großer Offenheit Kompetenzen auf- und auszubauen, neu zu entwickeln und auch voneinander zu lernen. Die Wirtschaft profitiert hierbei unter verschiedenen Gesichtspunkten. Einerseits ermöglicht der stetige Austausch ein besseres Verständnis für die Bedürfnisse der Ermittlungsbehörden und damit verbunden einer Verbesserung der eigenen Produkte. Anderseits profitieren alle Unternehmen unterschiedlichster Größe von den Präventionsmaßnahmen, die diese Kooperation zur Verfügung stellt. Ziel muss es auch in Zukunft sein, noch besser für die Herausforderungen gewappnet zu sein, vor welche uns eine sich industrialisierende und internationalisierende Organisierte Kriminalität im Cyberraum stellt.“

Prof. Dieter Kempf, Präsident des BITKOM e. V.

[42] Kooperation zur Förderung der Sicherheit bei der Nutzung von Informations- und Kommunikationstechnologien sowie zur präventiven und repressiven Bekämpfung der Cybercrime des BITKOM e. V. und der Landeskriminalämter Baden-Württemberg, Niedersachsen und Nordrhein-Westfalen

5 Fazit

Die immer kürzeren Entwicklungszyklen in der Technik, die Vielzahl neuer Phänomene und die zunehmende Professionalisierung der Täter stellen die nordrhein-westfälische Polizei vor große Herausforderungen. Zwei Aspekte sind herauszuheben:

Zunahme der Fallzahlen

Die Zunahme der Fallzahlen in den Bereichen der Cybercrime im engeren Sinne sowie bei der Kriminalität unter Nutzung des Tatmittels Internet ist groß (vgl. Nrn. 1.4 und 1.6). Gleichzeitig werden die für eine Aufklärung erforderlichen Ermittlungsmaßnahmen komplexer und aufwändiger. Eine Folge ist die seit Jahren sinkende Aufklärungsquote. Mit den im Jahr 2012 eingeleiteten Maßnahmen zur Neuausrichtung der Cybercrimebekämpfung der Polizei NRW sollte dem bereits erkennbaren Trend entgegen gewirkt werden. So wurden neben anderen Maßnahmen die organisatorischen Strukturen im Landeskriminalamt NRW sowie in den Kreispolizeibehörden optimiert, es wurden beispielsweise mehr Informatiker eingestellt. Für den Bereich der Cybercrimebekämpfung im engeren Sinne führten diese erhöhten Aufwände trotz der Zunahme der Fallzahlen zu einer Konsolidierung der Anzahl der aufgeklärten Fälle.

Mit der Neuausrichtung der Cybercrimebekämpfung wurde die Fortbildung der Sachbearbeiter in der Bekämpfung der allgemeinen Kriminalität verbessert, z. B. bei den Betrugsdelikten oder in der Wirtschaftskriminalität. Hier werden alle Fertigkeiten und Kenntnisse vermittelt, um solche Straftaten erfolgreich aufklären zu können, die mit dem Tatmittel Internet begangen wurden. Zusätzlich verstärkten die Dienststellen zur Bekäpfung der Cybercrime ihre ermittlungsunterstützenden Maßnahmen in diesen Bereichen. Dies führte im Jahr 2013 erstmals seit 2010 wieder zu einem Anstieg der aufgeklärten Fälle um 30,3 % im Vergleich zum Vorjahr und damit zu einer Umkehr des bisher negativen Trends. Insgesamt wurden 8.325 Straftaten mehr aufgeklärt als 2012.

Big Data und andere technischen Herausforderungen

Die technische Komplexität des Internets, die Datenmengen und die Durchdringung aller Lebensbereiche mit Internettechnologien nehmen mit hoher Dynamik weiter zu. Während z. B. noch vor wenigen Jahren die Auswirkungen von Big Data (vgl. Nr. 2.3) auf die polizeiliche Arbeit nur theoretisch erörtert wurden, ist Big Data für die Polizei NRW heute hoch aktuell. Die Experten des Cybercrime-Kompetenzzentrums beim Landeskriminalamt NRW analysierten im Jahr 2013 ca. 170 Terabyte Daten, die bei Straftätern sichergestellt worden waren. In den ersten drei Monaten des Jahres 2014 waren es bereits mehr als 100 Terabyte. Die steigenden Anforderungen werden in Zukunft jedoch allein durch quantitative Input-Steuerungen bei Sachmitteln und Personal nicht zu bewältigen sein. Nur neue, effiziente Ermittlungsmethoden und -techniken, z. B. Cloud-basierte Lösungen sowie intelligente Analysewerkzeuge, werden dies gewährleisten können. Diese Herausforderungen können gemeinsam mit starken und verlässlichen Partnern aus Forschung und Lehre sowie der Wirtschaft bewältigt werden.

6 Anlagen

6.1 Datenbasis

Grundlage dieses Lagebildes sind Daten aus der Polizeilichen Kriminalstatistik, Sachverhalte aus dem polizeilichen Vorgangsbearbeitungssystem und dem Kriminalpolizeilichen Sondermeldedienst Cybercrime. In der Polizeilichen Kriminalstatistik werden unter dem Summenschlüssel 897000 nur die Delikte der Cybercrime im engeren Sinne zusammengefasst (siehe Vorbemerkungen, Seite 1).

Im Kriminalpolizeilichen Sondermeldedienst Cybercrime melden die Polizeibehörden folgende Straftaten der Cybercrime im engeren Sinne:

- § 202a StGB Ausspähen von Daten
- § 202b StGB Abfangen von Daten
- § 202c StGB Vorbereitungshandlungen zum Ausspähen von Daten
- § 263a StGB Computerbetrug (ohne: Missbrauch von Zahlungskarten- und Missbrauch von Internetzugangsdaten)
- § 269 StGB Fälschung beweiserheblicher Daten
- § 270 StGB Täuschung im Rechtsverkehr bei Datenverarbeitung
- §§ 271, 274 Nr. 2, Falschbeurkundung/Urkundenunterdrückung, § 348 StGB im Zusammenhang mit Datenverarbeitung
- § 303a StGB Datenveränderung
- § 303b StGB Computersabotage

Während sich aus der Polizeilichen Kriminalstatistik nicht alle Informationen zu den einzelnen Straftaten entnehmen lassen, bietet der Kriminalpolizeiliche Sondermeldedienst Cybercrime eine zusätzliche Möglichkeit einer differenzierten Auswertung von Informationen zur Phänomenologie einzelner Delikte.

Um neue Tatbegehungsformen der Cybercrime zeitnah erkennen zu können, bietet der Kriminalpolizeiliche Sondermeldedienst Cybercrime den sachbearbeitenden Dienststellen auch die Möglichkeit, Straftaten über den Katalog hinaus zu melden, wenn

- zur Tatbegehung hohes IuK-Fachwissen auf Täterseite erforderlich ist
- Täter besondere Techniken zur konspirativen Kommunikation nutzen
- eine Tat von grundsätzlicher bzw. bundesweiter Bedeutung ist
- ein überdurchschnittlich hoher Schaden vorliegt oder
- ein besonderer Modus Operandi festgestellt wird.

Zur umfassenden Darstellung der Cybercrime wurde eine ergänzende Auswertung der im polizeilichen Vorgangsbearbeitungssystem erfassten Datensätze vorgenommen.

6.2 Tabellen – Polizeiliche Kriminalstatistik

Tabelle 1: Fallzahlen in einzelnen Deliktsfeldern der Cybercrime im engeren Sinne

	Delikte		Zu- bzw. Abnahme	
	2012	2013		in %
Computerbetrug	6.087	6.774	+ 687	+ 11,3
Fälschung beweiserheblicher	2.278	3.121	+ 843	+ 37,0
Daten, Täuschung im Rechtsverkehr				
bei Datenverarbeitung				
Datenveränderung/	4.118	6.713	+ 2.595	+ 63,0
Computersabotage				
Ausspähen, Abfangen von Daten einschl.	4.373	5.486	+ 1.113	+ 25,5
Vorbereitungshandlungen				
Betrug mittels rechtswidrig	4.880	4.553	- 327	- 6,7
erlangter Debitkarte mit PIN				
Betrug mit Zugangsberechtigungen	419	319	- 100	- 23,9
zu Kommunikationsdiensten				
Softwarepiraterie	25	34	+ 9	+ 36,0
private Anwendung				
Softwarepiraterie	48	16	- 32	- 66,7
gewerbsmäßiges Handeln				
Computerkriminalität	22.228	27.016	+ 4.788	+ 21,5
insgesamt				

Tabelle2: Aufklärungsquoten

	aufgeklärte Fälle		Aufklärungsquote %		Zu- bzw. Abnahme
	2012	2013	2012	2013	% - Punkte
Computerbetrug	1.555	1.452	25,6	21,4	- 4,2
Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung	617	643	27,1	20,6	- 6,5
Datenveränderung/ Computersabotage	252	342	6,1	5,1	- 1,0
Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen	570	489	13,0	8,9	- 4,1
Betrug mittels rechtswidrig erlangter Debitkarte mit PIN	1.516	1.482	31,1	32,6	+ 1,5
Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten	127	65	30,3	20,4	- 9,9
Softwarepiraterie private Anwendung	21	29	84,0	85,3	+ 1,3
Softwarepiraterie gewerbsmäßiges Handeln	46	16	95,8	100,0	+ 4,2
Computerkriminalität insgesamt	4.704	4.518	21,2	16,7	- 4,5

Tabelle 3: Entwicklung der Fallzahlen und Aufklärungsquoten der Cybercrime im engeren Sinne

	bekannt gewordene Fälle		Aufklärung	
	erfasste Fälle	Zu- bzw Abnahme	aufgeklärte	Aufklärungs-
Jahr	insgesamt	%	Fälle	Quote %
2004	17.026	+ 20,8	7.133	41,9
2005	16.806	- 1,3	6.553	39,0
2006	15.068	- 1,0	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	+ 21,1	4.518	16,7

Tabelle 4: Entwicklung der Altersverteilung der Tatverdächtigen

Tatverdächtige													
	unter 21		21 bis unter 30		30 bis unter 40		40 bis unter 50		50 bis unter 60		über 60		insgesamt
Jahr	absolut	Anteil %	absolut	Anteil %	absolut	Anteil %	absolut	Anteil %	absolut	Anteil %	absolut	Anteil %	
2004	916	25,1%	1119	30,6%	885	24,2%	537	14,7%	147	4,0%	51	1,4%	3.655
2005	850	23,7%	1070	29,8%	909	25,3%	515	14,3%	189	5,3%	58	1,6%	3.591
2006	862	25,0%	927	26,9%	793	23,0%	563	16,3%	234	6,8%	72	2,1%	3.451
2007	1006	25,2%	1020	25,6%	820	20,5%	714	17,9%	337	8,4%	94	2,4%	3.991
2008	901	24,0%	1042	27,8%	859	22,9%	618	16,5%	246	6,6%	84	2,2%	3.750
2009	1021	22,6%	1264	28,0%	979	21,7%	798	17,7%	336	7,4%	122	2,7%	4.520
2010	1195	24,6%	1433	29,4%	1054	21,7%	736	15,1%	338	6,9%	110	2,3%	4.866
2011	876	20,8%	1348	32,1%	925	22,0%	666	15,8%	291	6,9%	96	2,3%	4.202
2012	772	20,6%	1116	29,7%	813	21,7%	647	17,2%	301	8,0%	104	2,8%	3.753
2013	691	19,8%	1018	29,2%	779	22,3%	607	17,4%	276	7,9%	121	3,5%	3.492

Tabelle 5: Tatmittel Internet

Tatmittel Internet			
	erfasste Fälle insgesamt	darunter Tatmittel Internet	
	2013	absolut	Anteil %
Straftaten insgesamt	**1.484.943**	**70.981**	**4,8**
Straftaten gegen die sexuelle Selbstbestimmung	10.484	1.879	17,9
- Verbreitung pornografischer Erzeugnisse	2.073	1.677	80,9
darunter:			
- Besitz/Verschaffen von Kinderpornografie	848	706	83,3
- Verbreitung von Kinderpornografie	677	604	89,2
Betrug	246.039	45.751	18,6
darunter:			
- Waren- und Warenkreditbetrug	74.279	26.469	35,6
- Computerbetrug	6.774	5.684	83,9
- Betrug mit Zugangsdaten zu Kommunikationsdiensten	319	168	52,7
Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung	3.121	2.663	85,3
Datenveränderung, Computersabotage	6.713	6.492	96,7
Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen	5.486	4.870	88,8
Erpressung	3.509	1.981	56,5

Herausgeber

Landeskriminalamt Nordrhein-Westfalen
Völklinger Str. 49
40221 Düsseldorf

Abteilung 4
Cybercrime-Kompetenzzentrum
Dezernat 41
Redaktion: KR Helmut Picko
Tel.: 0211-939-4100 oder Polizeinetz 07-224-4100
Fax: 0211-939-194100 oder Polizeinetz 07-224-194100

Dez41.LKA@polizei.nrw.de

Impressum

Landeskriminalamt Nordrhein-Westfalen
Abteilung 4, Cybercrime-Kompetenzzentrum
Völklinger Str. 49
40221 Düsseldorf

Telefon: (0211) 939-0
Telefax: (0211) 939-4119

landeskriminalamt@polizei.nrw.de
www.lka.nrw.de

Titelbild: Landeskriminalamt NRW, ZA 3.3, Fotografin: C. Franken