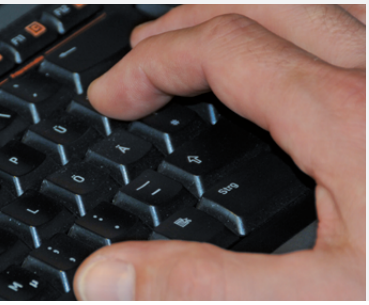
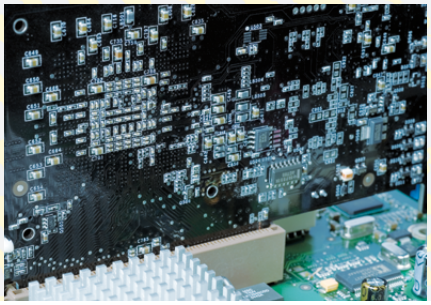





2014

LKA BW

# Cybercrime/ Digitale Spuren

JAHRESBERICHT 2014

Baden-Württemberg

LANDESKRIMINALAMT

# CYBERCRIME / DIGITALE SPUREN
## AUF EINEN BLICK

DER RÜCKGANG DER COMPUTERKRIMINALITÄT IN DER PKS SPIEGELT NICHT DIE TATSÄCHLICHE KRIMINALITÄTSBELASTUNG WIEDER.

DAS DUNKELFELD MUSS NACH KRIMINALISTISCHER ERFAHRUNG NACH WIE VOR ALS SEHR HOCH EINGESCHÄTZT WERDEN.

UM MIT DEN STEIGENDEN HERAUSFORDERUNGEN DER DIGITALISIERTEN WELT SCHRITT HALTEN ZU KÖNNEN, WIRD HOCHQUALIFIZIERTES PERSONAL BENÖTIGT.

| | 2013 | 2014 | IN % | |
|---|---|---|---|---|
| **GESAMT[1]** | **23.014** | **21.898** | **- 4,8** | ↘ |
| COMPUTERKRIMINALITÄT | 8.893 | 7.941 | - 10,7 | ↘ |
| INTERNETKRIMINALITÄT | 18.804 | 17.949 | - 4,5 | ↘ |
| GESAMTBEREICH KINDERPORNO-GRAFISCHE SCHRIFTEN | 693 | 578 | - 16,6 | ↘ |
| VERFAHRENSINITIIERUNGEN AIR | 297 | 731 | + 146,1 | ↗ |
| RANSOMWARE | 2.417 | 267 | - 89 | ↘ |
| NEUE AUFTRÄGE ITB | 11.225 | 10.339 | - 8 | → |
| MOBILFUNKAUFKLÄRUNG | 789 | 1.027 | + 30,2 | ↗ |

[1] *Eine Teilmenge der Computerkriminalität ist Bestandteil der Internetkriminalität. Der als „Gesamt" dargestellte Wert stellt den bereinigten Wert ohne Doppelzählung dar.*

# INHALT

## 1 ANALYSE

Kein anderer Bereich veränderte das Berufsbild des Polizeibeamten in den letzten Jahrzehnten so sehr wie die Entwicklungen im Internet mit all ihren Begleiterscheinungen. Die Alltäglichkeit der virtuellen Welt hat sich in der Polizeiarbeit längst niedergeschlagen. Die Bedingungen für die Polizei haben sich in nahezu allen Tätigkeitsfeldern verändert. Von der Beweissicherung auf elektronischen Datenträgern, der gerichtsfesten Aufbereitung riesiger Datenmengen bis hin zur Bearbeitung von hochkomplexen und komplizierten Ermittlungsverfahren der Cybercrime ist zwischenzeitlich eine technische Expertise erforderlich. Dies stellt die polizeiliche Aus- und Fortbildung vor bislang nicht bekannte Herausforderungen. In keinem anderen Bereich der Kriminalitätsbekämpfung ist die Inanspruchnahme externer Angebote von Hochschulen so notwendig wie im Aufgabenfeld der Cybercrimebekämpfung.

Die Polizei in Baden-Württemberg reagierte organisatorisch auf die Entwicklung dieser Kriminalitätsform. Nachdem im Landeskriminalamt Baden-Württemberg (LKA BW) bereits im Jahr 2012 die Abteilung Cybercrime und Digitale Spuren eingerichtet wurde, nahm sich auch die zum 1. Januar 2014 umgesetzte Polizeireform des Landes dieses Themas an. In den Kriminaldirektionen der zwölf neu geschaffenen Polizeipräsidien wurden jeweils Kriminalinspektionen analog der neu geschaffenen Abteilung im LKA BW eingerichtet. Die Polizei des Landes Baden-Württemberg hat damit eine bislang bundesweit einzigartige flächendeckende Struktur geschaffen, die nun Bürgerinnen und Bürgern, aber auch Behörden und Wirtschaftsunternehmen zur Verfügung steht. Diesen organisatorischen Musterbedingungen muss nun die flächendeckende Versorgung mit Expertise folgen.

Bei den mit der Polizeireform neu eingerichteten Organisationseinheiten müssen sich übergreifende Prozesse einspielen, qualifiziertes Personal muss gefunden und fortgebildet werden. Bereits mit der aktuellen flächendeckenden Qualifikation der Mitarbeiterinnen und Mitarbeiter zur Bekämpfung der Cybercrime und zur Bewältigung des Aufkommens digitaler Spuren braucht das Land keinen Vergleich zu scheuen.

Sorge bereiten die enormen Datenmengen, die insbesondere für die Spezialisten der IT-Forensik zunehmend zur Herausforderung werden. Sichergestellte Daten in einem Umfang von Terabyte im oberen zweistelligen Bereich alleine in einem einzigen Ermittlungsverfahren fordern das Personal der IT-Forensik in einem ganz besonderen Maße. Derartige Datenmengen bringen auch die zur Aufbereitung verwendeten Tools und ebenso die Speicherkapazitäten an ihre Grenzen.

Nach den Enthüllungen der Tätigkeiten eines amerikanischen Nachrichtendienstes war im vergangenen Jahr eine deutliche Zunahme der Nutzung von Verschlüsselungstechnologien zu beobachten. Was für die um die Sicherheit ihrer Daten besorgten Internetnutzer eine positive Entwicklung ist, bereitet der Polizei im Fall von richterlich angeordneten Überwachungsmaßnahmen zunehmend Probleme. Reaktionen von Politik und Rechtsprechung sind in diesem Bereich dringend erforderlich.

Unsere Gesetzgebung hat sich in ersten Schritten den Entwicklungen der Cybercrime angepasst. Die Möglichkeiten der Cybercrimebekämpfung stoßen jedoch nach wie vor an rechtliche Grenzen. International machen Hürden und Zeitverzug im grenzüberschreitenden Rechtshilfeverkehr die

Täterermittlung nahezu unmöglich. National steht einer effektiven Bekämpfung von Straftaten in vielen Fällen immer noch die fehlende Verpflichtung der Provider zur Speicherung der Verbindungsdaten für einen angemessenen Zeitraum entgegen.

#### ONLINE-NUTZUNG

Die Forschungsgruppe Wahlen erhebt seit dem Jahr 2000 regelmäßig in repräsentativen Telefonumfragen Daten zur Internet-Nutzung[2] und untersucht hierbei das Nutzungsverhalten der deutschen Bevölkerung ab 18 Jahren.

Im Jahr 2014 nutzten 78 % der deutschen Erwachsenen das Internet zu Hause, am Arbeitsplatz oder anderswo. Im Einzelnen waren 83 % der Männer und 72 % der Frauen online. Im Vergleich zum Vorjahr ergibt sich nur bei der Verteilung zwischen Männern (2013: 85 %) und Frauen (2013: 71 %) eine leichte Veränderung, während die Gesamtzahl unverändert bleibt.

Nahezu alle unter 50-Jährigen nutzten im Jahr 2014 das Internet: Im Detail waren es 99 % der 18- bis 24-Jährigen, jeweils 98 % der 25- bis 29-Jährigen sowie der 30- bis 39-Jährigen und 96 % der 40- bis 49-Jährigen. Bei den 50- bis 59-Jährigen lag der Anteil bei 88 %. Bei Befragten ab 60 Jahren nutzten nur 48 % das Internet. Größere geschlechtsspezifische Unterschiede zeigten sich dabei einzig in der Altersgruppe ab 60 Jahren: (Männer: 59 %, Frauen: 40 %).

#### MOBILE NUTZUNG DES INTERNETS

Einer Studie des Bundesverbands Digitale Wirtschaft, die in Kooperation mit Google und TNS Infratest zwischen Januar und Februar 2014 durchgeführt wurde[3], ist zu entnehmen, dass mittlerweile 50 % der Deutschen ihr Smartphone nutzen, um mobil online zu gehen. Die Nutzung von Smartphones stieg somit um 25 % im Vergleich zum Vorjahr.

Mittlerweile werden im Durchschnitt mehr als zwei internetfähige Endgeräte pro Person genutzt und mehr als die Hälfte der Befragten (54 %) sind durch das Smartphone häufiger online als in der Vergangenheit. Die Altersstruktur der Befragten weist deutliche Unterschiede auf. Während 71 % der 14- bis 29-Järigen angeben, durch ein Smartphone häufiger online zu sein, sind es in der Altersgruppe der ab 50-Jährigen weniger als 8 %.

#### EINFLÜSSE AUF NUTZERVERHALTEN

Neben den selbsterlebten Schadensfällen tragen auch medienwirksame Vorfälle wie spektakuläre Hackerangriffe oder die öffentlich gewordenen Abhöraktionen staatlicher Geheimdienste im Internet massiv zur Verunsicherung der Internetnutzer bei. In der Folge verzichten viele Internetnutzer auf bestimmte Online-Dienste und schränken ihr Verbraucherverhalten ein. Fast ein Drittel (29 %)

2 *http://www.forschungsgruppe.de/umfragen/internet-strukturdaten/ (aufgerufen am 3. Februar 2015).*

3 *http://www.bvdw.org/presseserver/studie_faszination_mobile/bvdw_faszination_mobile_2014.pdf (aufgerufen am 3. Februar 2015).*

verzichtet auf Online-Banking und ein Viertel (24 %) auf das Einkaufen im Internet, ein Fünftel (21 %) nutzt keine Cloud-Dienste und 17 % buchen weder Reisen noch Mietwagen im Netz.[4]

### DUNKELFELD

Zwischen den polizeilich registrierten Fallzahlen und der tatsächlich begangenen Kriminalität ergibt sich eine Differenz, die als Dunkelfeld bezeichnet wird. Dieses entsteht im Wesentlichen, weil Straftaten nicht entdeckt oder auch nicht angezeigt werden. Die Polizei schätzt das Dunkelfeld bei Cybercrime besonders hoch ein.

Zur Erforschung des Dunkelfeldes hat der Bundesverband für Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) im Jahr 2014 eine repräsentative Befragung von 1.000 Internetnutzern durchgeführt.[5]
Das alarmierende, aber nicht unbedingt überraschende Ergebnis ist, dass in den vorangegangenen zwölf Monaten 55 % der Internetnutzer nach eigener Aussage Opfer von Cybercrime geworden sind. Das entspricht rund 29 Millionen Betroffenen in Deutschland.

Bei vier von zehn Internetnutzern wurden laut der BITKOM-Umfrage die Computer mit Schadprogrammen infiziert. Knapp ein Fünftel (19 %) gab an, dass Zugangsdaten zu Internetdiensten ausspioniert wurden. 14 % sind von einem Geschäftspartner betrogen worden, zum Beispiel beim Online-Shopping oder einer Auktion. Ein weiteres häufig genanntes Delikt (16 %) ist der illegale Versand von E-Mails in fremdem Namen.

### ZENTRALE ANSPRECHSTELLE CYBERCRIME

Die Zentrale Ansprechstelle Cybercrime (ZAC) des LKA BW hat sich als Single Point of Contact für Wirtschaftsunternehmen sowie öffentliche und nichtöffentliche Stellen bewährt.
Sie kann zwischenzeitlich im Bedarfsfall auf ein bundesweites Netzwerk von ZAC-Dienststellen zurückgreifen, die beim Bundeskriminalamt (BKA) und den Landeskriminalämtern eingerichtet sind.
Zunehmend sind die Mitarbeiter der ZAC im Zusammenhang mit Awarenessveranstaltungen von Konzernen oder Unternehmensverbänden gefragt. Dem Wunsch kleiner und mittelständischer Unternehmen (KMU) nach Präventionsaktivitäten wie Vorträgen kommt die ZAC im Rahmen ihrer personellen Möglichkeiten als kompetenter Ansprechpartner nach.
Die rasante Entwicklung der Informationstechnologie und damit verbunden die ständig neuen Möglichkeiten für Straftäter, diese Technologie einzusetzen, machen es stärker als in anderen Kriminalitätsfeldern erforderlich, mit Unternehmen und Unternehmensverbänden der IT, aber auch mit Forschung und Lehre Kooperationen einzugehen. Die Geschäftsführungen dieser Kooperationen sind in der ZAC angesiedelt.

4 *http://www.bitkom.org/files/documents/bitkom_vortrag_kempf_pk_it-sicherheit_mit_dem_bka_27_08_2014_final_druck.pdf (aufgerufen am 3. Februar 2015).*

5 *http://www.bitkom.org/files/documents/bitkom_vortrag_kempf_pk_it-sicherheit_mit_dem_bka_27_08_2014_final_druck.pdf (aufgerufen am 3. Februar 2015).*

# ANALYSE

## CYBERCRIME IM ENGEREN SINNE (COMPUTERKRIMINALITÄT)

Anlagen | 1-3

Bei der Cybercrime im engeren Sinne ist ein Rückgang um 10,7 % auf 7.941 Fälle zu verzeichnen. Parallel dazu ging auch die Schadenshöhe um 33 % auf 6.868.663 Euro zurück.

Anlagen | 4

Die Anzahl der erfassten Fälle des Computerbetrugs verringerte sich um 10,1 % auf 3.182 Fälle. Die Schadenshöhe für den Tatbestand des Computerbetrugs sank ebenfalls um 45,4 % auf 4.181.895 Euro.

Anlagen | 5

Der Tatbestand des Ausspähens von Daten (§ 202a StGB) ging im Vergleich zu den Vorjahren im Jahr 2014 stärker zurück. Im Jahr 2014 sind mit 1.160 Fällen 174 weniger als im Vorjahr erfasst, was einer Abnahme um 13 % entspricht.

Diese Entwicklung spiegelt sich auch in der Betrachtung der Computerkriminalität mit Sonderkenner „Internet“ wider. Dieser Trend widerspricht dem tatsächlich zu bearbeitenden Fallaufkommen. Eine Begründung hierfür ergibt sich aus den Richtlinien der Polizeilichen Kriminalstatistik (PKS), die eine Erfassung von Straftaten mit Handlungsort im Ausland oder weltweit ungeklärtem Handlungsort nicht vorsehen. Diese Umstände sind bei Ermittlungen in den Bereichen Cybercrime Tatmittel und Cybercrime im engeren Sinne regelmäßig gegeben, so dass diese Fälle keinen Eingang in die PKS finden.

Betrachtet man die Entwicklung der Auslandsstraftaten oder Fälle, deren Tatort nicht in Deutschland liegt, im Polizeilichen Auskunftssystem Baden-Württemberg (POLAS-BW), so wird ersichtlich, dass diese Fälle seit 2007 kontinuierlich angestiegen sind. Allein im Jahr 2013 stieg die Zahl um 31,2 % im Vergleich zum Vorjahr.

Die Ursache dieser Zunahme an Auslandsstraftaten lässt sich insbesondere aus dem Täterverhalten herleiten. Die Cyberkriminellen entwickeln ihre Techniken zur Verschleierung ihrer Identität immer weiter und nutzen weltweit zur Verfügung stehende Ressourcen, um sich zu anonymisieren.

Die Tatorte verlagern sich deshalb zunehmend ins Ausland.

## ARBEITSBEREICH ERMITTLUNGEN CYBERCRIME

Die im Jahr 2014 beim LKA BW bearbeiteten Ermittlungsverfahren bestätigen die Erfahrungen aus den Vorjahren, dass Straftäter im virtuellen Raum die Techniken und Möglichkeiten zur Verschleierung ihrer Identitäten stetig weiterentwickeln und den polizeilichen Ermittlungsmethoden anpassen. Anonymisierungsmöglichkeiten wie z. B. TOR und Botnetze werden zielgerichtet eingesetzt, um eine Rückverfolgung zu erschweren. Die Täter passen sich zeitnah technischen Sicherungsmechanismen an und ändern häufig ihre Vorgehensweise, um einer Strafverfolgung zu entgehen.

Neben rein technischen Angriffen der Täter auf Computer privater Nutzer, Firmennetzwerke und die öffentliche Infrastruktur, ist immer häufiger das Social Engineering zu beobachten.

## INTERNATIONALE DURCHSUCHUNGSAKTION IM BEREICH CYBERCRIME AM 13. MAI 2014

Das Federal Bureau of Investigation (FBI) ermittelt gegen die Verbreiter einer Schadsoftware. Im Rahmen der dortigen Ermittlungen wurden bereits ein Teil der Betreiber der Vertriebsseite sowie die Autoren der Schadsoftware festgenommen.

Nach einer staatenbezogenen Auswertung einer beschlagnahmten Datenbank der Täter wurden die festgestellten Hinweise auf Schadsoftwareankäufer an die jeweiligen Staaten übermittelt.
An einer auf internationaler Ebene abgestimmten Operation am 13. Mai 2014 wurden weltweit Durchsuchungen vorgenommen. Auch 14 Tatverdächtige aus Baden-Württemberg waren betroffen.
Das LKA BW hatte im Rahmen der Durchsuchungen eine koordinierende Funktion.
Die Durchsuchungen selbst wurden von den Polizeipräsidien in eigener Zuständigkeit durchgeführt.

#### RANSOMWARE – EINE VARIANTE DER DIGITALEN SCHUTZGELDERPRESSUNG

Die Erpressungsdelikte mit Tatmittel Internet sind in der PKS deutlich rückläufig. Es wurden 2014 lediglich 42 Fälle erfasst, was einem Rückgang um 434 Fälle entspricht. Verantwortlich hierfür könnte der insgesamt auffällige Rückgang an Ransomware-Straftaten sein, welcher sich durch eine INPOL-Fall-Auswertung in der Datei „Cybercrime“ belegen lässt. Für das Jahr 2014 lassen sich bundesweit nur 267 erfasste Fälle zählen – 2013 waren es noch 2.417 Fälle.

#### IDENTITÄTSDIEBSTAHL

Der Begriff „Identitätsdiebstahl“ ist ein weit gefasster Begriff, welcher die missbräuchliche Nutzung personenbezogener Daten einer natürlichen Person durch Dritte bezeichnet. Identitätsdiebstahl im Kontext der Cybercrime kann in vielerlei Ausprägungen stattfinden. Einen eigenen Straftatbestand gibt es im StGB oder in den strafrechtlichen Nebengesetzen nicht. Vielmehr können verschiedene Straftaten begangen werden. Als konkreter Straftatbestand kommt vor allem § 202a StGB, Ausspähen von Daten, in Betracht. „Ausspähen von Daten“ im Sinne dieser Strafvorschrift kann aber auch jegliches Ausspähen anderer Daten betreffen, weshalb über eine Abfrage dieses Straftatenschlüssels in der PKS keine verwertbaren Aussagen getroffen werden können. „Identitätsdiebstahl“ oder artverwandte, aber thematisch passende, Begriffe sind auch in POLAS BW derzeit als Katalogbegriffe weder für die Begehungsweise noch als erstrebtes/erlangtes Gut hinterlegt.

### SICHERHEITSTEST BSI

Im Rahmen eines niedersächsischen Ermittlungsverfahrens der Staatsanwaltschaft Verden wurden jeweils 16 bzw. 18 Mio. Datensätze von E-Mail-Accounts aufgefunden, welche u. a. zum Versenden von sogenannten Spam-Mails benutzt worden sind. Diese Datenfunde wurden dem Bundesamt für Sicherheit in der Informationstechnik (BSI) zwecks weiterer Maßnahmen übergeben.
Das BSI entwickelte daraufhin ein Verfahren zur Benachrichtigung der betroffenen Internetnutzer. Diese wurden aufgerufen zu überprüfen, ob sie von Identitätsdiebstahl betroffen waren. Die Überprüfung erfolgte mithilfe des vom BSI bereitgestellten, webbasierten Sicherheitstests unter der Website „https://www.sicherheitstest.bsi.de“. Im Falle eines Treffers sendete das BSI eine digital signierte Nachricht an die angegebene E-Mail-Adresse. Den Betroffenen wurde angeraten, ihre Adressen und Passwörter zu ändern und weitere Sicherheitsmaßnahmen zu ergreifen.

### CYBERCRIME TATMITTEL (INTERNETKRIMINALITÄT)

Anlagen | 6

Die in der PKS registrierten Fallzahlen gingen im Jahr 2014 wie im Vorjahr leicht um 4,5 % auf 17.949 Fälle zurück. Davon wurden 13.396 Fälle aufgeklärt. Die Aufklärungsquote ist damit um 7,4 %-Punkte auf 74,6 % angestiegen.

Anlagen | 7

Über 70 % der Delikte Cybercrime Tatmittel sind den Vermögens- und Fälschungsdelikten zuzurechnen. Im Jahr 2014 sind die Fälle um 4,8 % auf 12.936 gefallen. Neben den Fallzahlen hat sich auch die Aufklärungsquote annähernd analog zu den Gesamtzahlen entwickelt. Die Aufklärungsquote beträgt 75,1 % (+ 5,3 %-Punkte). Als Schaden wurden bei den Vermögens- und Fälschungsdelikten mit Tatmittel Internet 8.729.056 Euro registriert, etwa zwei Millionen Euro weniger als im Vorjahr. Die jeweiligen Delikte bei den Vermögens- und Fälschungsdelikten haben sich nicht einheitlich entwickelt. Warenbetrug ist um 384 auf 4.747 Fälle und der Warenkreditbetrug um 142 auf 2.626 Fälle angestiegen. Rückläufig ist hingegen der Betrug mit rechtswidrig erlangten unbaren Zahlungsmitteln (- 265 auf 548 Fälle) und der sonstige Betrug (- 926 auf 4.574 Fälle). Unter den letztgenannten Betrugsarten wird auch der Computerbetrug mit einem Rückgang um 303 auf 2.516 Fälle erfasst.

Die Straftaten gegen die sexuelle Selbstbestimmung gingen um 59 auf 792 Fälle zurück. Bestimmend in diesem Deliktsfeld ist die Verbreitung pornografischer Schriften. Die Fallzahlen sind im Jahr 2014 leicht um 52 auf 605 Fälle zurückgegangen. Ein weiterer Deliktsbereich ist der sexuelle Missbrauch, der leicht von 188 auf 176 Fälle abgenommen hat. Darunter fällt auch der sexuelle Missbrauch von Kindern unter Einwirkung mittels Schriften oder Informations- oder Kommunikationstechnologie nach § 176 IV Nr. 3 StGB. Wird dieses Delikt mit dem Tatmittel Internet begangen, so wird es als Cybergrooming bezeichnet[6].

[6] *Weitere Ausführungen finden Sie unter „Ansprechstelle Kinderpornografie“.*

Die Rohheitsdelikte/Straftaten gegen die persönliche Freiheit sind im Jahr 2014 um 109 auf 463 Fälle angestiegen. In diesem Zusammenhang spielen bei Cybercrime Tatmittel fast überwiegend drei Delikte eine Rolle: Nötigung, Bedrohung und das Nachstellen (auch Stalking genannt). Bei allen drei Delikten sind trotz geringer Gesamtfallzahlen Anstiege zu verzeichnen. Nötigung stieg um 16 auf 102 Fälle, Bedrohung um 78 auf 263 Fälle und Nachstellen um 4 auf 77 Fälle.

Andere Delikte der Internetkriminalität aus den sonstigen Straftatbeständen des Strafgesetzbuches sind insgesamt um 272 auf 3.069 Fälle rückläufig. Angestiegen sind unter diesen Tatbeständen die Androhung von Straftaten (+ 69 auf 88 Fälle), die Volksverhetzung (+ 38 auf 55 Fälle), die Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen (+ 28 auf 122 Fälle), die (allgemeine) Beleidigung (+ 201 auf 696 Fälle), die Beleidigung auf sexueller Grundlage (+ 50 auf 198), die üble Nachrede (+ 23 auf 86 Fälle) und die Verleumdung (+ 41 auf 143 Fälle). Diesen Delikten ist wie Nötigung, Bedrohung und Nachstellen mit Tatmittel Internet gemein, dass sie der Polizei häufig nur durch die Anzeige der oder des Geschädigten bzw. Anzeigen Dritter (z. B. Forenmoderatoren, Chatteilnehmer etc.) bekannt werden. Betrachtet man die Entwicklungen der letzten Jahre, so kann man daraus schließen, dass sich das Anzeigeverhalten verändert hat. Heute werden mehr Delikte angezeigt, als noch vor einigen Jahren. Einen deutlichen Rückgang in der Statistik verzeichnen unter den sonstigen Straftatbeständen nach dem StGB die Erpressungsdelikte. Hier wurden im Jahr 2014 lediglich 42 Fälle erfasst, dies entspricht einem Rückgang um 434 Fälle[7].

Bei den strafrechtlichen Nebengesetzen wurden 687 Fälle in der PKS erfasst, das sind 23 Fälle mehr als im Vorjahr. Zu diesen Nebengesetzen gehören die Straftaten gegen Urheberrechtsbestimmungen, die insgesamt im Mehrjahresvergleich rückläufig sind. Im Jahr 2014 wurden noch 395 Fälle registriert, 76 Fälle weniger als im Vorjahr. Viele dieser Fälle werden bei der Polizei oder der Staatsanwaltschaft nicht mehr zur Anzeige gebracht und ausschließlich zivilrechtlich geklärt. Dennoch verursachen gerade gewerbsmäßig oder bandenmäßig begangene Urheberrechtsverletzungen große Schäden. In einem Fall des Polizeipräsidiums Ludwigsburg wegen gewerbsmäßiger Softwarepiraterie wurde beispielsweise ein Schaden von 407.782 Euro festgestellt.

Im Jahr 2014 sind die Straftaten gegen das Kunsturhebergesetz um 38 auf 183 Fälle angestiegen. Ursächlich ist die vermehrte Verfolgung von Straftaten nach § 22 Kunsturhebergesetz, wonach Bildnisse nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden dürfen. Der Tatbestand ist bereits dann erfüllt, wenn ein Foto online in ein öffentliches Forum oder soziale Netzwerke gestellt wird, ohne vorher die Einwilligung der abgebildeten Person einzuholen. Im Bereich der strafrechtlichen Nebengesetze sind außerdem das Arzneimittelgesetz und das Betäubungsmittelgesetz (BtMG) nennenswert. Bei Straftaten gegen das Arzneimittelgesetz ist ein Anstieg um 53 auf 76 Fälle zu verzeichnen. Bei der Rauschgiftkriminalität mit Tatmittel Internet ist die Anzahl der

[7] *Weitere Ausführungen finden Sie unter „Ransomware".*

Delikte von 101 auf 163 Straftaten gestiegen. Ursächlich für die Anstiege sind zunehmend im Internet gehandelte Substanzen, die den Vorschriften des Arzneimittelgesetzes bzw. dem BtMG unterliegen. Hierzu zählen beispielsweise Kräutermischungen und Research Chemicals aber auch klassische Betäubungsmittel wie Cannabis, Kokain und Amphetamine.

Weitere Informationen zur Internetkriminalität in den Deliktsfeldern Organisierte, Politisch Motivierte und Wirtschaftskriminalität finden sich in den jeweiligen Jahresberichten.

#### ANSPRECHSTELLE KINDERPORNOGRAFIE

Die Ansprechstelle Kinderpornografie (ASt KiPo) ist die zentrale Ansprech- und Koordinierungsstelle des Landes für den Straftatenkomplex Besitz/Verschaffen und Verbreitung von Kinderpornografie. Kann der Nachweis der Verbreitung nicht geführt werden, wird der Vorgang wegen Besitzes von kinderpornografischen Schriften der Staatsanwaltschaft vorgelegt.

Anlagen | 8,9

#### FALLZAHLEN KINDERPORNOGRAPHIE

Die Fälle im Deliktsbereich Besitz/Verschaffen kinderpornografischer Schriften sind im Jahr 2014 um 25 % auf 369 Fälle gefallen. Die Fallzahlen mit Sonderkenner „Internet“ (Tatmittel Cybercrime) nahmen ebenfalls um 22,4 % auf 246 Fälle ab. Die Aufklärungsquote ist in diesem Bereich sehr hoch und betrug im Jahr 2014 90,7 %. Die Verbreitung von kinderpornografischen Schriften mit 209 Fällen nahm um 4 % zu. Der Anteil der Straftaten mit Tatmittel Internet hat dabei von 136 Fällen auf 152 Fälle im Jahr 2014 zugenommen.
Der Gesamtbereich Besitz/Verschaffen und Verbreitung kinderpornografischer Schriften bewegt sich mit 578 Fällen auf gleichbleibendem Niveau der Vorjahre (2013: 693, 2012: 559, 2011: 630, 2010: 607).

#### OPERATIONEN / UMFANGSVERFAHREN

Im Jahr 2014 wurden durch die Ast KiPo 71 Sammelverfahren (sog. Umfangsverfahren) mit 286 Tatverdächtigen bearbeitet. 22 Umfangsverfahren resultierten aus Verfahren, die in Baden-Württemberg geführt oder initiiert wurden. In einem Umfangsverfahren wurden 166 deutsche Tatverdächtige wegen der Verbreitung kinderpornografischer Schriften im Internet angezeigt.
Bereits im November 2013 ging bei der Internetwache des LKA BW ein Hinweis auf den Besitz und die Verbreitung von kinderpornografischen Schriften in einem Chatforum ein. Im Rahmen der Ermittlungen wurden bei der ASt Kipo insgesamt 311 Seiten Chatverlauf ausgewertet. Gegen zehn Beschuldigte wurden Ermittlungsverfahren wegen des Besitzes bzw. der Verbreitung kinderpornografischer Schriften eingeleitet. Bei dem Haupttäter, der sich im Chat als 14-jähriges Mädchen ausgab, handelte es sich um einen 52-jährigen Sexualstraftäter aus Mönchengladbach, der bereits mehrfach einschlägig in Erscheinung getreten ist.

Weiterhin wurden im Jahr 2014 durch die ASt Kipo vier umfangreiche Ermittlungsverfahren wegen des Besitzes/der Verbreitung kinderpornografischer Schriften im Internet bearbeitet.
Dabei wurden gegen die Betreiber/Hoster von 1.473 kinderpornografischen, 479 jugendpornografischen, 18 tierpornografischen und 275 pornografischen Webseiten Anzeigen bei der Staatsanwaltschaft Stuttgart vorgelegt.

#### LÖSCHUNG VON INTERNETSEITEN MIT KINDERPORNOGRAFISCHEM INHALT

Das BKA ist für die Überwachung der Löschung von ausländischen Internetseiten mit kinderpornografischen Inhalten zuständig. Laut der mit den Internet-Beschwerdestellen abgestimmten Jahresstatistik 2013 des BKA wurden im Jahre 2013 insgesamt 3.504 URLs weltweit festgestellt. Die Jahresstatistik 2014 liegt derzeit noch nicht vor.
Im Falle von ausländischen URLs waren nach einer Woche noch 45 % verfügbar. Nach vier Wochen war noch eine Verfügbarkeit von 23 % feststellbar.
Durch das BKA wurde im Rückblick auf die letzten drei Jahre ein Anstieg der Meldungen ausländischer URLs festgestellt. Die relevanten Inhalte wurden mehrheitlich in den USA (27 %), Japan (20 %) und in den Niederlanden (16 %) gehostet.

#### HASH-DATENBANK PORNOGRAFISCHE SCHRIFTEN

Die Hash-Datenbank Pornografische Schriften (Hash-DB PS) ging als Nachfolger des bislang von den Sachbearbeitern Kinderpornografie bundesweit verwendeten Programms PERKEO[8] am 2. Juni 2014 in den Wirkbetrieb. Die Länder haben hierüber die Möglichkeit, Hashwerte von kinderpornografischen (Kategorie 1) und jugendpornografischen (Kategorie 2) Dateien, die durch die Ansprechstellen Kinderpornografie bewertet wurden, bundesweit bereitzustellen. Der Einsatz dieser Hashwerte in laufenden Ermittlungsverfahren führt zu einer deutlichen Reduktion der händisch zu bewertenden Dateien und damit einer Beschleunigung der Auswertung in Verfahren wegen Kinder- bzw. Jugendpornografie.

#### ZIUZ

Beim Produkt ZIUZ handelt es sich um eine Software zur Auswertung von Bild- und Videodateien, die hauptsächlich für den Bereich der Bekämpfung der Kinderpornografie und des sexuellen Missbrauchs von Kindern entwickelt wurde. Mit dieser kann der polizeiliche Sachbearbeiter große Datenmengen schnell sichten und bewerten, so dass zeitliche und psychische Belastungen reduziert werden. Das System wurde landesweit für die Polizeipräsidien und das LKA BW beschafft. Baden-Württemberg ist damit das erste Bundesland mit einer einheitlichen Infrastruktur in diesem Deliktsbereich. Die Geschäftsprozesse werden aktuell durch eine Fachanwendergruppe unter Leitung des LKA BW festgelegt.

8 *Programm zur Erkennung relevanter kinderpornografisch eindeutiger Objekte (Software zur Feststellung bereits bekannter kinderpornografischer Bild- und Videodateien bei der Auswertung des Datenmaterials i. Z. m. Ermittlungsverfahren wegen des Besitzes bzw. der Verbreitung von kinderpornografischen Schriften).*

Die durch die Dienststellen kategorisierten Bilder und Videos (Kinder-, Jugendpornografie, Präferenz und Pornografie) werden alle der ASt Kipo übermittelt. Hier erfolgt die Qualitätsprüfung und Einstellung in die bundesweite HashDB-PS.

Anlagen | 10

Die steigende Zahl der zu bewertenden Dateien wird anhand der Datenzulieferungen der Polizeipräsidien an die Ast KiPo des LKA BW deutlich. Im Jahre 2014 hat die Anzahl der angelieferten Bilder 2 Millionen und die der Videos 420.000 überschritten. Im Vorjahr waren dies noch 1,3 Millionen Bilder und 30.000 Videos.

### SCHULFAHNDUNG

Im Zuge einer im Herbst 2014 durchgeführten Schulfahndung wegen des schweren sexuellen Missbrauchs eines Kindes bzw. der Herstellung und Verbreitung kinderpornografischer Schriften konnten sowohl Täter als auch das Opfer in Bayern identifiziert werden. Der 49 Jahre alte Täter und Vater des Opfers wurde festgenommen, nachdem eine Schulleiterin den siebenjährigen Jungen identifiziert hatte.

Der Ermittlungserfolg verdeutlicht die Bedeutung des Instruments der zielgruppenorientieren Öffentlichkeitsfahndung in Form der „Schulfahndung“ bei der Identifizierung von Opfern des sexuellen Missbrauchs. Sie wird mit dem Hintergrund der geringeren sekundären Viktimisierung des Opfers bevorzugt.

### ARBEITSBEREICH INTERNETRECHERCHE

Anlagen | 11

### INITIIERUNG VON ERMITTLUNGSVERFAHREN

Im Rahmen einiger diesjähriger Operationen zur Bekämpfung von Kinderpornografie wurde die Verbreitung mehrerer eindeutiger kinderpornografischer Dateien in dezentralen Netzwerken (Tauschbörsen) beobachtet und aufgezeichnet. Bis zum Jahresende wurden weltweit über 10.000 Strafverfahren initiiert. 7 % davon entfielen auf die Nutzer deutscher IP-Adressen. Es handelt sich um die höchste Anzahl von Verfahrensinitiierungen im Zeitraum eines Kalenderjahres seit Bestehen des Arbeitsbereichs.

### VORRATSDATENSPEICHERUNG

Aus polizeilicher Sicht ist nach wie vor festzustellen, dass es nach dem Wegfall der Vorratsdatenspeicherung kein einheitliches Speicherverhalten der Provider mehr gibt. Die Dauer der Speicherung der Verkehrsdaten obliegt aufgrund der Freiwilligkeit dem Ermessen der Verpflichteten und variiert zwischen null und sieben Kalendertagen. Da Straftaten allerdings häufig erst bekannt werden, nachdem die Daten bereits gelöscht oder anonymisiert sind, erschwert die fehlende Vorratsdatenspeicherung die Ermittlungen erheblich oder macht sie unmöglich.

Bei den im Jahr 2014 durch den Arbeitsbereich Internetrecherche (AIR) durchgeführten Operationen zur Bekämpfung von Kinderpornografie konnten 30,5 % der Bestandsdaten deutscher IP-Adressen aufgrund fehlender Verpflichtung zur Vorratsdatenspeicherung nicht erhoben werden. Andere Möglichkeiten zur Identifizierung der Beschuldigten bestanden nicht, so dass der Staatsanwaltschaft eine Strafanzeige gegen Unbekannt vorgelegt werden musste.

Hinsichtlich der Auskunftsquote ist zu berücksichtigen, dass der AIR Bestandsdaten nach § 113 TKG in der Regel zu einem Zeitpunkt erhebt, zu dem der Täter noch online ist. Außerhalb der Regelarbeitszeit der Auskunftsstellen der Provider erfolgen die Anfragen in einem maximalen Abstand von drei Tagen. Die Auskunftsquote ist durch diese zeitnahe Reaktion deutlich höher als bei sonstigen Cybercrime-Ermittlungsverfahren, bei denen relevante IP-Adressen erst im Rahmen der Ermittlungen nach und nach bekannt werden. Das bedeutet, dass die Anzahl der Fälle, in denen eine Auskunft durch den Provider nicht mehr möglich ist, in anderen Verfahren deutlich höher ist.

Im Ergebnis bleibt festzustellen, dass die Verbreitung kinderpornografischer Dateien in den Netzwerken nur unzureichend verfolgt werden kann. Aufgrund fehlender rechtlicher Vorgaben zur Vorratsdatenspeicherung kann damit auch in vielen Fällen die noch anhaltende fortlaufende Missbrauchshandlung nicht beendet werden.

## PHÄNOMENE

### BUNDESWEITE ERPRESSUNGSSERIE GEGEN WEBSEITENBETREIBER MIT BITCOIN-ZAHLUNGS-AUFFORDERUNG

Seit Anfang Oktober 2014 wurden bundesweit neun Fälle mit identischem Modus Operandi bekannt. Unter dem Aliasnamen „Mark“ wurden per E-Mail die jeweiligen Administratoren oder Betreiber einer Webseite bzw. eines Webservers kontaktiert. „Mark“ behauptete, dass mehrere z. T. gravierende Sicherheitslücken auf der jeweiligen Webseite bestünden. Zur Bestätigung wurden jeweils Screenshots und Datenbankauszüge als Anlage beigefügt.

Die jeweiligen E-Mails enthalten das Bedrohungsszenario, dass die Kunden bzw. die Öffentlichkeit über den „Datenverlust“ informiert werden könnten. Man verzichte aber gegen eine Zahlung von zwei und bis sechs Bitcoins (aktueller Wert eines Bitcoin beträgt ca. 300 Euro) und übersende dafür einen 40-80 Seiten umfassenden Sicherheitsbericht über die vorgefundenen Sicherheitslücken.

In allen Fällen ist es dem Täter tatsächlich gelungen, Sicherheitsbarrieren zu überwinden und in die jeweilige Dateisystem- und Datenbankstruktur der Webserver einzudringen. Zur Anonymisierung verwendete der Täter Wegwerf-E-Mail-Adressen und machte sich das TOR-Netzwerk zunutze. In drei Fällen wurde eine Zahlung – teilweise entgegen des Rates der jeweils ermittelnden Polizeidienststelle – geleistet. In keinem Fall wurde der angekündigte Sicherheitsbericht übersandt. Es ist auch kein Fall bekannt, in dem es zu einer Veröffentlichung von Daten gekommen ist.

Der Serie konnten bundesweit drei Fälle in Baden-Württemberg, zwei Fälle in Bayern und jeweils ein Fall in Hessen, Niedersachsen, Rheinland-Pfalz und Saarland zugeordnet werden.

### AUSHEBELUNG DES MTAN-VERFAHRENS

Im Jahr 2014 wurde im bundesweiten polizeilichen Informationsaustausch immer wieder ein Modus Operandi bekannt, über den es Tätergruppierungen gelungen ist, das mTAN-Verfahren auszuhebeln. Hierbei erlangen die Täter die Identitätsdaten der Geschädigten, insbesondere die Zugangsdaten und die Kennwörter für das Online-Banking sowie das Geburtsdatum, die Wohnadresse und die Handynummer. Dies geschieht durch Phishing-Mails, welche eine seriöse Nachricht einer Bank vortäuschen. Diese beinhalten einen Link, der den Nutzer auf eine angebliche Seite der Bank weiterleitet und ihn auffordert, seine Daten einzugeben. In anderen Fällen wird eine Schadsoftware auf dem PC eingeschleust, welche bei der nächsten Online-Banking-Sitzung die Zugangsdaten ausspäht. Mit den Daten können die Täter vom Online-Banking-Account des Geschädigten Besitz ergreifen. Gleichzeitig wird eine zweite SIM-Karte des Geschädigten beantragt, auf die anschließend sämtliche SMS und somit auch alle mTAN weitergeleitet werden. In der Folge werden hohe Beträge an mutmaßliche oftmals gutgläubige Finanzagenten überwiesen. Von diesen wird das Geld auf unterschiedliche Art, über mehrere Stationen und meist nicht oder nur sehr schwer nachvollziehbar, an die eigentlichen Täter ins Ausland weitergeleitet.

## DIGITALE FORENSIK

Anlagen | 12

### AUFTRAGSAUFKOMMEN IT BEWEISSICHERUNG

Die landesweiten Aufträge der IT-Beweissicherung werden seit 2006 statistisch erfasst. Der seitdem festgestellte fortlaufende Anstieg wird im Jahr 2014 erstmals gestoppt. Insgesamt wurden in Baden-Württemberg 10.339 Aufträge rund um die IT-Beweissicherung an die im Rahmen der Polizeireform neu eingerichteten Kriminalinspektionen 5 adressiert. Die Aufträge sind somit um 7,9 % im Vergleich zum Vorjahr mit 11.225 Aufträgen zurückgegangen. Die untersuchten Mobilgeräte sind um 6,3 % im Vergleich zum Vorjahr auf 9.789 untersuchte Einheiten zurückgegangen. Die Entwicklung der Quartalszahlen zeigt jedoch auf, dass nach Auftragsrückgang bis in das dritte Quartal hinein ein deutlicher Anstieg im vierten Quartal 2014 festzustellen ist. Im LKA BW gingen im Jahr 2014 insgesamt 226 Aufträge ein, was einen Anstieg um 13 % im Vergleich zum Vorjahr bedeutet. Bei den zu untersuchenden Mobilgeräten ist eine Zunahme um 45,4 % auf 269 festzustellen.

### ARBEITSBEREICH DATENANALYSE

Mit Umsetzung der Polizeireform wurden zum 1. Januar 2014 die dezentralen Analysestellen bei den zwölf regionalen Polizeipräsidien eingerichtet. Die Aufgaben der Datenanalyse wurden den Kriminalinspektionen 5, Cybercrime/Digitale Spuren, zugewiesen. Bei der Inspektion 520 des LKA BW wurde bereits mit Einrichtung der Abteilung 5 im Jahr 2012 eine zentrale Analysestelle eingerichtet. Somit ist der Bereich der Datenanalyse in der Polizei des Landes nunmehr klar strukturiert.
Bei der Datenanalyse handelt es sich um keine Teildisziplin der operativen Auswertung. Sie stellt die polizeiliche Verarbeitung eines eigenständigen und sehr speziellen Beweisthemas dar, deren Ergebnis neben anderen Beweisthemen in den analytischen Prozess innerhalb eines Ermittlungsverfahrens oder einer operativen Auswertung einfließt.
Kernaufgabe der Datenanalyse ist die Aufbereitung und forensische Untersuchung strukturierter (Massen-)Daten, die in polizeirechtlichen und strafverfahrensrechtlichen Ermittlungsverfahren erhoben werden. Aufgaben der Analyse sind beispielhaft die Aufbereitung und Analyse von Telekommunikationsverkehrsdaten, die Aufbereitung und der Abgleich sonstiger Datenarten wie Personen- und Fahrzeugdaten, sowie georeferenzierte Analyse und grafische Aufbereitung.

Die Arbeitsbereiche Datenanalyse in den Polizeipräsidien des Landes sind personell unterschiedlich besetzt. Auswirkungen zeigt dies insbesondere in der Abarbeitung von polizeilichen Sonderlagen. In derartigen Lagen, die zumeist in Form von Sonderkommissionen, Besonderen Aufbauorganisationen oder Ermittlungsgruppen abgearbeitet werden, ist auf die Datenanalyse nicht mehr zu verzichten. Die Aus- und Fortbildung der Sachbearbeiter Datenanalyse war im Jahr 2014 ein zentrales Thema. Die Analysestellen wurden mit jeweils einer Lizenz für die Software InfoZoom sowie weiteren analysespezifischen Anwendungen ausgestattet. Insgesamt bleibt festzustellen, dass sich die Analysestellen hinsichtlich Personal, Ausrüstung und Fortbildung weiterhin im Aufbauprozess befinden.

#### KOMPETENZZENTRUM TELEKOMMUNIKATIONSÜBERWACHUNG

Der moderne Kommunikationsmarkt ist von rasanten Entwicklungen geprägt. Übertragungsgeschwindigkeiten, Bandbreiten und Datenmengen nehmen stark zu. Darüber hinaus zeichnet er sich durch eine zunehmende Verschlüsselung der Kommunikationsinhalte, technisch bedingte oder absichtlich erzeugte Anonymisierung von Teilnehmeranschlüssen, Internationalisierung und die Einführung neuer technischer Standards aus.
Herkömmliche Kommunikationsdienste und das Internet verschmelzen miteinander und führen zu einer steigenden Anzahl an Kommunikationsmöglichkeiten und vielfältigen Nutzungsmöglichkeiten. Begleitet wird dies durch immer kürzere Entwicklungszyklen mit umfassenden Neuerungen. Diesen Herausforderungen mit unmittelbaren Auswirkungen auf die Telekommunikationsüberwachung (TKÜ) muss begegnet werden, sonst entzieht sich die gesamte beweiserhebliche Täterkommunikation den Strafverfolgungsbehörden.
Kernstück der technischen Plattform für die TKÜ ist die leistungsfähige TKÜ-Anlage des LKA BW. Um diese auf dem neuesten Stand zu halten, wurden die Hardwarekomponenten im Jahr 2014 ersetzt.
Dem Landtag Baden-Württemberg wird jährlich ein Bericht über Umfang und Erfolg von TKÜ-Maßnahmen erstattet. Er gibt Aufschluss über Anzahl und durchschnittliche Dauer einer Telefonüberwachungsmaßnahme sowie die betroffene Katalogstraftat (vgl. § 100a StPO), für die eine Telefonüberwachung angeordnet wurde.
Statistische Daten zu Maßnahmen nach §§ 100a und 100g StPO sind daneben über das Bundesamt für Justiz im Internet abrufbar: https://www.bundesjustizamt.de/de/themen/buergerdienste/justizstatistik/telekommunikation/telekommunikationsueberwachung.html

#### PROJEKT FUNKZELLENINFORMATIONSSYSTEM BADEN-WÜRTTEMBERG

Das Funkzelleninformationssystem Baden-Württemberg (FISBW) enthält Informationen über die tatsächliche Funkausbreitung von GSM-/UMTS-Mobilfunkzellen. FISBW wurde in enger Abstimmung mit den Dienststellen der zu vermessenden Gebiete umgesetzt und die landesweite Erstvermessung im November 2013 abgeschlossen. Die Bereitschaftspolizei unterstützte das LKA BW bei diesen zentralen Aufgaben.

Aufgrund des geschaffenen qualitativ hochwertigen Datenpools ist eine Darstellung der Funkzellen nahe der tatsächlichen funktechnischen Ausbreitung möglich. Die kartografische Darstellung und Nutzung der Daten erlaubt im Rahmen von Sucheinsätzen die gezielte und ressourcenschonende Einweisung von Kräften. Polizeitaktische Entscheidungen der Führungs- und Lagezentren können auf eine verbesserte Datenbasis gestützt werden. Die Daten haben insbesondere im Bereich der Gefahrenabwehr, z. B. bei der Lokalisierung von Mobiltelefonen und der Auswertung von Standortdaten bei einer Vermisstenfahndung einen hohen Einsatzwert. Zudem können Sondereinsatzmittel wie Hubschrauber und IMSI-Catcher zielgerichtet im Einsatzgebiet eingesetzt und Einsatzzeiten deutlich verkürzt werden.

Im Jahr 2014 wurden im Zeitraum 1. Januar 2014 bis 1. Oktober 2014 insgesamt 5.538 Anfragen an die FISBW-Datenbank gestellt. Nach dem Rollout von FIS 2.0 ist eine Protokollierung der Abfragen noch nicht umgesetzt, so dass Zahlenmaterial ab Oktober nicht mehr vorliegt. Im Vorjahr waren es insgesamt 7.529 Anfragen. Die Anzahl der Anfragen dürfte auf ähnlich hohem Niveau liegen und weist auf die hohe Relevanz für die polizeiliche Arbeit hin.

#### MOBILFUNKAUFKLÄRUNG

Der Arbeitsbereich Mobilfunkaufklärung führt IMSI-Catcher- bzw. WLAN-Catcher-Einsätze sowie Funkzellenbestimmungen und -vermessungen (gem. § 23a Polizeigesetz BW oder § 100i bzw. § 100a StPO) durch. Die Funkzellenbestimmung wird zur Vorbereitung einer Funkzellenabfrage gem. § 100g StPO durchgeführt.
Die Funkzellenvermessung dient der Bestimmung des konkreten Ausmaßes einer Funkzelle, insbesondere zur Alibiüberprüfung und für gutachterliche Aussagen vor Gericht. Die durch die Vermessungen gewonnenen Daten werden auch für die Datenbank FISBW genutzt.

Im Jahr 2014 ist die Anzahl der Anforderungen der Mobilfunkaufklärung nochmals von 789 auf 1.027 angestiegen. Davon entfielen 905 Anforderungen auf Funkzellenvermessungen.
Aufgrund der Kapazitätsgrenzen mussten davon 31 Anträge abgelehnt werden. Neben der Funkzellenvermessung wurde der IMSI-Catcher 122 mal angefordert:

- 61 Mal aufgrund von Identifizierungsmaßnahmen (Ermittlung eines unbekannten Mobilfunkanschlusses).
- 51 (2013: 34) Mal auf Rechtsgrundlage der Strafprozessordnung bei der Suche bekannter Straftäter durch Ortungsmessungen (Lokalisierungen).
- In zehn (2013: neun) Fällen um den Aufenthaltsort vermisster oder suizidgefährdeter Personen zu bestimmen.
- In zehn Fällen in Auftragslagen für andere, teilweise angrenzende Bundesländer.

Im Jahr 2014 lagen keine Anforderungen für den Einsatz des WLAN-Catchers vor.

# MASSNAHMEN

## 2 MASSNAHMEN / HANDLUNGSEMPFEHLUNGEN

### GESAMTKONZEPTION „CYBERCRIME / DIGITALE SPUREN“

Die im Auftrag des Innenministeriums Baden-Württemberg, Landespolizeipräsidium (IM-LPP), zu Beginn des Jahres 2013 erstellte Gesamtkonzeption „Cybercrime/Digitale Spuren“ hat sich bewährt. Die 25 Handlungsempfehlungen wurden im Jahr 2014 zusammen mit den neu eingerichteten Kriminalinspektionen Cybercrime/Digitale Spuren der Polizeipräsidien teilweise umgesetzt.
Die Umsetzung aller Handlungsempfehlungen ist jedoch erst mittelfristig möglich, da sie beispielsweise von im Zuge der Polizeireform aktuell noch umzusetzender Baumaßnahmen abhängig ist.
Die Gesamtkonzeption stößt bei anderen Bundesländern und auch im benachbarten deutschsprachigen Ausland auf großes Interesse und wurde zwischenzeitlich zahlreichen Ländern zur Verfügung gestellt.
Zu Beginn des Jahres 2015 wird die Gesamtkonzeption evaluiert.

### SONDERLAUFBAHN CYBERKRIMINALIST

Zwischenzeitlich stehen erste Absolventen der Sonderlaufbahn Cyberkriminalist kurz vor dem Abschluss ihrer Ausbildung. Im November 2014 konnten landesweit insgesamt 15 Stellen ausgeschrieben werden. Nach Durchführung von Auswahlgesprächen konnten letztlich sieben Absolventen in Probezeit eingestellt werden. Noch Ende des Jahres 2014 erfolgte abermals die Ausschreibung von 18 Stellen zur Sonderlaufbahn Cyberkriminalist.
Formale Voraussetzungen für die Bewerbung zur Sonderlaufbahn sind ein mindestens drei Jahre dauerndes Hochschulstudium mit einem entsprechenden Abschluss in einem für die Bearbeitung von Cybercrime geeigneten Studiengang sowie eine anschließend mindestens drei Jahre ausgeübte einschlägige Tätigkeit.

### BUND-/LÄNDER-PROJEKTGRUPPE „BEKÄMPFUNGSSTRATEGIE CYBERCRIME“

Bereits im Jahr 2009 erstellte eine Bund-Länder-Projektgruppe (BLPG) im Auftrag der Innenministerkonferenz (IMK) die „Strategie zur Bekämpfung der IuK-Kriminalität“. Nach nunmehr fünf Jahren erteilte die IMK den Auftrag, die damalige Strategie zu überarbeiten. Eine im Sommer 2014 eingesetzte BLPG hat sich dazu entschieden, die Strategie aufgrund der rasanten Entwicklungen rund um das Thema Cybercrime komplett neu zu erstellen. Die „Bekämpfungsstrategie Cybercrime“ wird unter Einbindung von über fünfzig externen Partnern, darunter Nachrichtendiensten, Gremien der Europäischen Union und IT-Unternehmensverbänden, der Antiviren-Industrie sowie des Versicherungsgewerbes, in die Zukunft gerichtet erstellt und wird der IMK noch 2015 vorgelegt.
Das LKA BW beteiligt sich maßgeblich an der Entwicklung der Strategie.

# MASSNAHMEN

### ZENTRALE ANSPRECHSTELLE CYBERCRIME

Im Jahr 2014 wurden durch die ZAC 474 Anzeigen und sonstige Hinweise entgegen genommen und bearbeitet. Davon gingen 55 Hinweise und Anfragen von Wirtschaftsunternehmen ein. Insbesondere bei dieser Zielgruppe wird nach wie vor von einem erheblichen Dunkelfeld ausgegangen.
Nicht zuletzt vor diesem Hintergrund waren Angehörige der ZAC im Laufe des Jahres 2014 an der Gestaltung von ca. 20 ein- oder mehrtägigen Veranstaltungen von Wirtschaftsunternehmen oder Unternehmensverbänden beteiligt, die ausschließlich oder überwiegend präventiven Charakter hatten. Fachvorträge der ZAC-Angehörigen auf derartigen Awareness-Veranstaltungen wurden teilweise durch Informationsangebote am ZAC-Messestand begleitet. Der äußerst ansprechend gestaltete Messestand steht seit Sommer 2014 zur Verfügung und trifft bei derartigen Veranstaltungen auf großes Interesse.
Die Abteilung Cybercrime/Digitale Spuren des LKA BW veranstaltete als Mitglied der Sicherheitskooperation Cybercrime 2014 die jährliche Kooperationsveranstaltung. 200 Teilnehmer der Veranstaltung informierten sich zwei Tage lang über aktuelle Entwicklungen der Cybercrime und die von Sicherheitsbehörden zu bewältigenden Probleme. Die Teilnehmer aus Bund und Ländern sowie dem benachbarten Ausland stammten von Sicherheitsbehörden und Angehörigen der IT-Branche. Das anspruchsvolle Programm auf einer Hauptbühne, begleitet von zahlreichen Panels, die teilweise tief in die Fachebene eindrangen, fand großen Anklang. Das Pressehaus in Stuttgart als Veranstaltungsörtlichkeit sorgte zwei Tage lang für äußerst niveauvolle Rahmenbedingungen. Der Sicherheitskooperation Cybercrime gehören neben dem LKA BW die Landeskriminalämter von Nordrhein-Westfalen, Niedersachsen und Sachsen sowie der zwischenzeitlich über 2.200 Mitglieder starke Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM ) an.
Die Sicherheitskooperation Cybercrime präsentiert sich alljährlich auf der CeBIT in Hannover.
Die ZAC des LKA Baden-Württemberg war im Jahr 2014 darüber hinaus mit dem Messestand auf der mehrtägigen Messe IT & Business in Stuttgart vertreten.

### OPEN COMPETENCE CENTER FOR CYBER SECURITY

Die Angebote des Hochschulverbunds wurden durch Mitarbeiterinnen und Mitarbeiter der Kriminalinspektionen 5 sowie des LKA BW im Jahr 2014 intensiv wahrgenommen. Die Hochschulzertifikate bieten aus Sicht der Abteilung Cybercrime/Digitale Spuren eine sinnvolle Ergänzung zur polizeilichen Aus- und Fortbildung, bieten zusätzliche Spezialisierungen an und sind gerade für Fachleute aus den Themenbereichen Cybercrime und Digitale Spuren äußerst wertvoll. Dies gilt für zusätzliche Inhalte, den unmittelbaren Zugang zum aktuellen Forschungsstand sowie zur Knüpfung von Kontakten mit anderen Absolventinnen und Absolventen. Das Programm besteht aus vier Angeboten. Dem Studium Initiale zur Erlangung einer Zugangsberechtigung für den Hochschulstudiengang, dem Bachelorstudiengang IT-Sicherheit, dem Masterstudiengang IT-Governance, Risk and Compliance Management und einem Hochschulzertifikatprogramm.
Weitere Informationen können auf https://www.open-c3s.de abgerufen werden.

### IDENTITÄTSDIEBSTAHL / BUND-LÄNDER-PROJEKTGRUPPE ID-THEFT

Vorfälle wie das Ermittlungsverfahren der Staatsanwaltschaft Verden, in welchem 16 bis 18 Mio. offensichtlich entwendete Datensätze aufgefunden wurden, führten zur Erkenntnis, dass einer möglichst standardisierten Vorgehensweise zwischen Polizeibehörden, dem BSI, der Justiz und den Diensteanbietern im Falle des Auffindens großer Mengen mutmaßlich gestohlener Daten Geschädigter dringend erforderlich ist. Vor diesem Hintergrund hat die AG Kripo im März 2014 eine Bund-Länder-Projektgruppe (BLPG „ID-Theft“) eingerichtet. Die Federführung hatte das Bundeskriminalamt und Teilnehmer waren die Länder Baden-Württemberg, Bayern, Hessen, Niedersachsen, Nordrhein-Westfalen, Rheinland-Pfalz, Sachsen, Sachsen-Anhalt, Schleswig-Holstein, der Bundespolizei sowie des BSI.

Die BLPG „ID Theft“ hat in der Folge Verfahrensabläufe im Falle des Auffindens großer Mengen durch Identitätsdiebstahl erlangter Daten, wie z. B. IP-Adressen, Kreditkartendaten oder Zugangsdaten zu Online-Bankkonten festgelegt. Ziel war es, sowohl präventive als auch repressive Maßnahmen effektiv zu bündeln. Über die beteiligten Institutionen, wie beispielsweise Bankinstitute und Diensteanbieter, soll künftig eine zeitnahe Information der betroffenen Kunden gewährleistet werden, um weiteren Schaden möglichst zu vermeiden.

### EINFÜHRUNG EINES SUPERVISIONSKONZEPTS

Die Bearbeitung von Dateien, welche z. T. schwerste sexuelle Misshandlungen von Kindern zum Inhalt haben, setzt die damit befassten Mitarbeiter besonderen psychischen Belastungen aus.
Diese Belastungen haben das Potenzial, Traumatisierungen und Krisen auszulösen. Als Supervisoren stehen die Mitarbeiterinnen und Mitarbeiter der Fachgruppe 213/Arbeitsbereich Kriminal- und Einsatzpsychologie des LKA BW zur Verfügung. Die Supervision findet für alle Mitarbeiter der Ast KiPo in vierteljährlichen Abständen statt.

### CYBERGROOMING

Am 27. Januar 2015 trat das 49. Gesetz zur Änderung des Strafgesetzbuches, die Umsetzung europäischer Vorgaben zum Sexualstrafrecht, in Kraft.

Der für Cybergrooming maßgebliche Straftatbestand des § 176 Absatz 4 Nr. 3 und Nr. 4 StGB wurde überarbeitet. Neben dem Einwirken mittels Schriften wurde nun ausdrücklich auch das sog. Einwirken mittels Informations- und Kommunikationstechnologie in den Tatbestand aufgenommen. Nicht verändert wurde durch den Gesetzgeber die Versuchsstrafbarkeit, die gemäß § 176 Absatz 6 StGB nach wie vor nicht vorgesehen ist.

# MASSNAHMEN

### TECHNIKER-WORKSHOP 2014

Vom 7. bis 9. Oktober fand beim LKA BW der Techniker-Workshop 2014 statt. Auf der jährlich stattfindenden Veranstaltung tauschen sich Informatiker sowie Polizeibeamte der entsprechenden EDV-Bereiche aus und stellen aktuelle Eigenentwicklungen vor.
Teilnehmer waren in diesem Jahr Kollegen des Bundeskriminalamts Österreich, der Stadtpolizei Zürich, der Bundeskriminalpolizei Schweiz, des BKA Wiesbaden und Berlin, des Landesamts für Verfassungsschutz Bayern sowie Kollegen aus den Landeskriminalämtern der Länder Brandenburg, Niedersachsen, Saarland, Sachsen, Thüringen, Sachsen-Anhalt und Hamburg.
Der Schwerpunkt der Themen lag im Bereich der Forensik, in der Software-Entwicklung via API-Schnittstellen der aktuellen Internet-Dienste sowie im Bereich der IT-Sicherheit.

### INVESTITIONEN IN AUSSTATTUNG DER DIENSTSTELLEN

Aus Mitteln der sogenannten Sicherheitsoffensive Polizeitechnik konnte wie in den Vorjahren die technische Ausrüstung der Kriminalinspektionen 5 und der Abteilung 5 des LKA BW weiter verbessert werden. Für die IT-Beweissicherung wurden insbesondere Untersuchungsumgebungen für Apple-Systeme beschafft. Aufgrund der stetigen Zunahme der Auftragslage hatte man mit Umsetzung der Polizeireform einen Spezialisierungsbereich „Apple-Macintosh-Systeme“ auch bei den regionalen Polizeipräsidien eingeführt. Für knapp 60.000 Euro konnte Hard- und Software für diese neue Aufgabe der Präsidien beschafft werden.
Aufgrund der zunehmenden Bedeutung als potenzielles Beweismittel mobiler Geräte in zahlreichen Ermittlungsverfahren wurde ein weiteres Mobilfunkuntersuchungssystem für jedes Präsidium beschafft. Diese Beschaffung konnte ebenfalls umgesetzt werden. Ziel ist es, die Bearbeitungszeiten zu reduzieren.

### AUS- UND FORTBILDUNG / SPEZIALISIERUNG

Mit Einführung des Spezialisierungsbereichs „Apple-Macintosh-Systeme“ war für die örtlichen Sachbearbeiter der IT-Beweissicherung erheblicher Fortbildungsbedarf entstanden. Hierzu wurde vom LKA BW in einer einwöchigen Schulung im November 2014 Spezialwissen an die Sachbearbeiter für Mac-Forensik der Polizeipräsidien vermittelt.
In drei Workshops des LKA BW in Stuttgart und Karlsruhe wurden die Sachbearbeiter IT-Beweissicherung in die Mobilfunkuntersuchungssysteme eingewiesen.

### FORTENTWICKLUNG DES KOMPETENZZENTRUMS TELEKOMMUNIKATIONSÜBERWACHUNG BW

Im Berichtsjahr 2014 wurden Grundlagen zur Einrichtung einer Projektgruppe geschaffen, die sich mit der Fortentwicklung des TKÜ-Zentrums in den Folgejahren unter Beachtung der engen haushalterischen Rahmenbedingungen befassen soll. Die Beachtung der personellen, strategischen, organisatorischen, haushalterischen und technischen Fragestellungen wäre in diesem Kontext ohne das Projekt nicht realisierbar.

Durch eine ständige aktualisierte Gesamt-Finanzplanung des TKÜ-Zentrums bis zum Jahr 2018 wird ein verlässlicher Rahmen für die Investitions- und Haushaltsplanung des LKA BW, des Präsidiums Technik/Logistik/Service der Polizei und des Innenministeriums geschaffen.

#### FISBW

Um die Entwicklungen der Mobilfunknetze und deren Ausbreitung zukünftig noch benutzerfreundlicher abbilden zu können, wurde die Datenbank umstrukturiert. Das Neusystem ist deutlich schneller und bietet verbesserte Funktionalitäten. Der Rollout des sog. FIS 2.0 wurde zum 1. Oktober 2014 vollzogen.

Die im Rahmen des Projektes FISBW anfallenden geografischen Daten stehen nun dem Einsatzleitsystem VIADUX zur Verfügung. Ziel ist eine automatisierte graphische Darstellung der Ausbreitung der Funkzellen im Einsatzleitsystem auf Basis von notrufbegleitenden Standortinformationen. Dies stellt für den Einsatzdisponenten eine wesentliche Arbeitshilfe bei der Identifizierung des Standorts eines Notrufenden und der schnelleren und zielgerichteten Entscheidung hinsichtlich Vorgehensweise und Einsatzmittel dar.

# MASSNAHMEN

### PRÄVENTION

Die Polizei und ihre Kooperationspartner aus Wirtschaft und Forschung gewährleisten ein ständig aktualisiertes Informationsangebot rund um die Nutzung der IT-Technik und die damit verbundenen Risiken. Die Informationen sind allgemeinverständlich verfasst und bieten dem Bürger hilfreiche Tipps, die er je nach Interessenlage vertiefen kann.

#### ONLINE-ANGEBOTE DER PRÄVENTION

Allgemeine Sicherheitsempfehlungen für PC und Internet:
http://www.polizei-beratung.de/themen-und-tipps/gefahren-im-internet.html

Sicherheitskompass von Polizei und Bundesamt für Sicherheit in der Informationstechnik (BSI):
http://www.polizei-beratung.de/themen-und-tipps/gefahren-im-internet/sicherheitskompass.html

Allgemeine Handlungsempfehlungen für Eltern, um ihren Kindern den richtigen Umgang mit den Medien zu vermitteln:
http://www.polizei-beratung.de/themen-und-tipps/medienkompetenz.html

„Kinder sicher im Netz", eine Initiative für Eltern und Kinder zum richtigen Umgang mit dem Internet und zur Förderung der Medienkompetenz:
http://www.kinder-sicher-im-netz.de

Gemeinsame Initiative des Online-Marktplatzes eBay, dem Bundesverband des Deutschen Versandhandels (bvh) und ProPK mit dem Ziel, vor Betrug bei Onlinekäufen zu schützen und den Wissensstand über sicheren Online-Handel zu erhöhen:
http://www.kaufenmitverstand.de

Die Initiative „Sicherer Autokauf im Internet" gibt Ratschläge zum Schutz gegen Online-Betrüger beim Kauf von Kraftfahrzeugen und ist eine Kooperation von AutoScout24, mobile.de, ADAC und ProPK:
http://www.sicherer-autokauf.de

Kooperation mit der Landesanstalt für Medien und Kommunikation Rheinland-Pfalz, welche die Förderung der Medienkompetenz im Umgang mit dem Internet und den neuen Medien im Auftrag der Europäischen Kommission zum Ziel hat:
http://klicksafe.de

Kooperation mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI), welches eine umfangreiche Auswahl an Faltblättern und CD-ROMs zum Thema Sicherheit in der Informationstechnik bietet:
http://www.bsi-fuer-buerger.de

# ANLAGEN

## 3 ANLAGEN

### DATENGRUNDLAGE DES JAHRESBERICHTS

Grundlage des Jahresberichts sind die Daten aus der Polizeilichen Kriminalstatistik (PKS) und dem kriminalpolizeilichen Nachrichtenaustausch.

### FACHBEGRIFFE UND BEGRIFFSBESTIMMUNGEN

Kriminalität, die mittels Internet oder anderen informationstechnischen Diensten begangen wird oder die sich gegen diese Systeme richtet, hat meistens eine globale Komponente, die weltweite Vernetzung. Häufig finden sich in diesem Deliktsbereich deswegen englische Begriffe und Kunstwörter (wie z. B. Phishing, das sich aus den Begriffen password und fishing zusammensetzt). Fachbegriffe, die im Text verwendet werden oder die im Zusammenhang mit Cybercrime – ein weiteres Fachwort – häufig auftauchen, sind deswegen in Form von Begrifssbestimmungen erklärt.

### DEFINITION CYBERCRIME

Cybercrime umfasst nach bundesweit gültiger Definition alle Straftaten, die sich gegen

- das Internet,
- weitere Datennetze, sowie
- informationstechnische Systeme

oder deren Daten richten. Cybercrime umfasst auch solche Straftaten, die mittels dieser Informationstechnik begangen werden.

In der PKS werden die bisher verwendeten Begriffe „Computerkriminalität“ und „Internetkriminalität“ zunächst weiter verwendet. Computerkriminalität entspricht dabei Cybercrime im engeren Sinne (Variante 1, bzw. erster Satz/Aufzählung der Definition). Internetkriminalität entspricht dabei Cybercrime Tatmittel (Variante 2, bzw. 2. Satz der Definition). Die Delikte werden in der PKS-Tabelle 05 dargestellt.

### COMPUTERKRIMINALITÄT – CYBERCRIME IM ENGEREN SINNE

Die Delikte der Computerkriminalität werden im PKS-Summenschlüssel 897000 zusammengefasst und in der PKS-Grundtabelle (Tabelle 01) dargestellt.

Der Summenschlüssel „897000 Computerkriminalität“ umfasst die folgenden Straftatenschlüssel:

- 516300 Betrug mittels rechtswidrig erlangter Debitkarten mit PIN
- 517500 Computerbetrug – soweit nicht unter den Schlüsseln 516300 bzw. 517900 zu erfassen
- 517900 Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten
- 543000 Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung

- 674200 Datenveränderung, Computersabotage
- 678000 Ausspähen, Abfangen von Daten einschließlich Vorbereitungshandlungen
- 715100 Softwarepiraterie (private Anwendung z. B. Computerspiele)
- 715200 Softwarepiraterie in Form gewerbsmäßigen Handelns

Diese Schlüssel spiegeln folgende Straftatbestände wieder: §§ 202a, 202b, 202c, 263, 263a, 269, 270, 303a, 303b StGB sowie Softwarepiraterie gem. UrhG.

#### SONDERMELDEDIENST CYBERCRIME

Die verbindliche Umsetzung des neuen SMD Cybercrime (Stand 24. Februar 2012) in den Ländern und dem Bund wurde von allen Gremien empfohlen und zum 10. Dezember 2012 in Baden-Württemberg realisiert.

Der Meldedienst umfasst folgende Delikte:

| | | |
|---|---|---|
| - | Ausspähen von Daten | (§ 202a StGB) |
| - | Abfangen von Daten | (§ 202b StGB) |
| - | Vorbereitung des Ausspähens und Abfangen von Daten | (§ 202c StGB) |
| - | Computerbetrug | (§ 263a StGB) |
| - | Fälschung beweiserheblicher Daten | (§ 269 StGB) |
| - | Täuschung im Rechtsverkehr bei Datenverarbeitung | (§§ 269, 270 StGB) |
| - | Falschbeurkundung/Urkundenunterdrückung | (§§ 271, 274, 348 StGB) |
| - | Datenveränderung, Computersabotage | (§§ 303a + b StGB) |

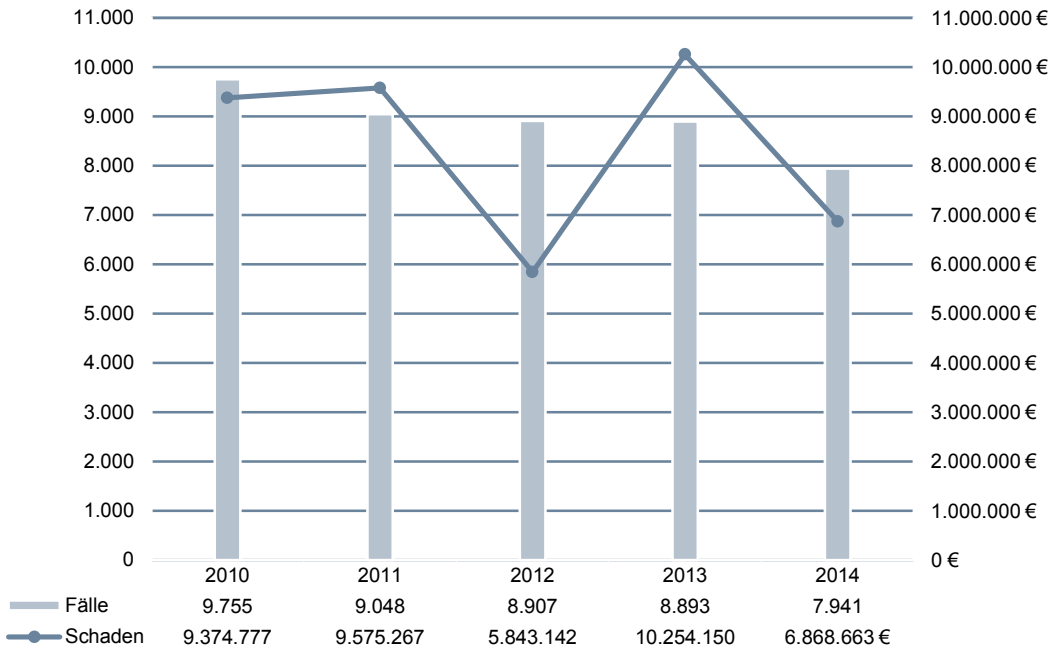
#### CYBERCRIME TATMITTEL – INTERNETKRIMINALITÄT

Straftaten sind gemäß PKS-Richtlinien dann als Internetkriminalität in der PKS zu erfassen, wenn das Internet als Tatmittel eingesetzt wird, auf besondere Fähigkeiten und Fertigkeiten des Täters oder die Tatbegehungsweise kommt es dabei nicht an. Erfasst werden grundsätzlich alle Delikte, zu deren Tatbestandsverwirklichung das Medium Internet als Tatmittel verwendet wird. Die Verwendung eines PC/Notebook etc. allein reicht nicht aus. Hier kommen sowohl Straftaten in Betracht, bei denen das bloße Einstellen von Informationen in das Internet bereits Tatbestände erfüllen (sog. Äußerungs- bzw. Verbreitungsdelikte) als auch solche Delikte, bei denen das Internet als Kommunikationsmedium bei der Tatbestandsverwirklichung eingesetzt wird.

## 1 | PKS-BAROMETER CYBERCRIME IM ENGEREN SINNE (2013-2014)

| | PKS-Schlüssel | 2013 | 2014 | in % | Tendenz |
|---|---|---|---|---|---|
| **Computerbetrug (§ 263a StGB)** | 5175 | 3.539 | 3.182 | -10,1 | ↘ |
| **Fälschung beweiserheblicher Daten (§ 269 StGB)/Täuschung im Rechtsverkehr (§ 270 StGB)** | 5430 | 692 | 534 | -22,8 | ↘ |
| **Datenveränderung (§ 303a StGB)/ Computersabotage (§ 303b StGB)** | 6742 | 392 | 213 | -45,7 | ↘ |
| **Ausspähen von Daten (§ 202a StGB)** | 6780 | 1.334 | 1.160 | -13,0 | ↘ |
| **Computerkriminalität** | 8970 | 8.893 | 7.941 | -10,7 | ↘ |

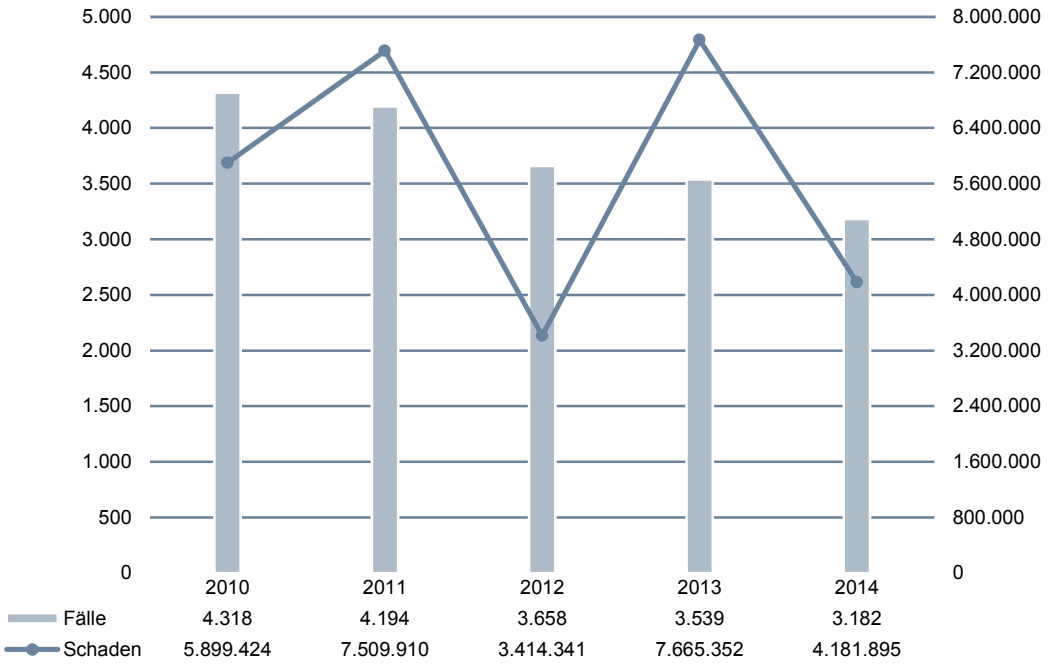
## 2 | CYBERCRIME IM ENGEREN SINNE FÜNFJAHRESVERGLEICH (2010-2014)



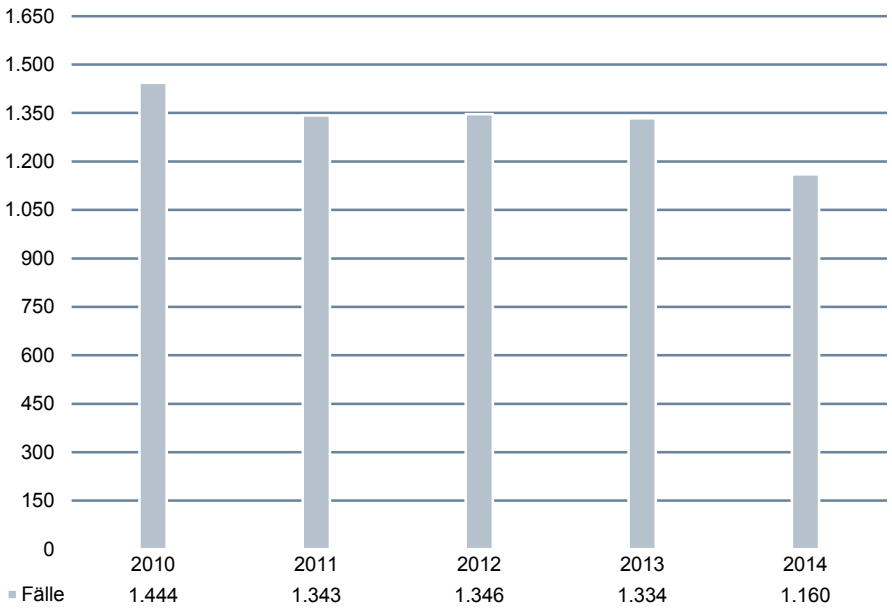
## 3 | CYBERCRIME IM ENGEREN SINNE (TABELLE) FÜNFJAHRESVERGLEICH (2010-2014)

| Berichtsjahr | 2010 | 2011 | 2012 | 2013 | 2014 |
|---|---|---|---|---|---|
| **Computerbetrug** | 4.318 | 4.194 | 3.658 | 3.539 | 3.182 |
| Computerbetrug Schadenssumme in € | 5.899.424 | 7.509.910 | 3.414.341 | 7.665.352 | 4.181.895 |
| **Fälschung beweiserheblicher Daten/Täuschung im Rechtsverkehr** | 638 | 618 | 649 | 692 | 534 |
| **Datenveränderung/ Computersabotage** | 194 | 236 | 292 | 392 | 213 |
| **Ausspähen von Daten** | 1.444 | 1.343 | 1.346 | 1.334 | 1.160 |
| **Computerkriminalität gesamt** | 9.755 | 9.048 | 8.907 | 8.893 | 7.941 |
| Computerkriminalität gesamt Schadenssumme in € | 9.374.777 | 9.575.267 | 5.843.142 | 10.254.150 | 6.868.663 |

## 4 | COMPUTERBETRUG FÜNFJAHRESVERGLEICH (2010-2014)



## 5 | AUSSPÄHEN VON DATEN FÜNFJAHRESVERGLEICH (2010-2014)




## 6 | CYBERCRIME TATMITTEL FÜNFJAHRESVERGLEICH (2010-2014)

| | 2010 | 2011 | 2012 | 2013 | 2014 |
|---|---|---|---|---|---|
| **Erfasste Fälle** | 22.494 | 20.988 | 16.912 | 18.804 | 17.949 |
| Erfasste Fälle Differenz | +989 | -1.506 | -4.076 | +1.892 | -855 |
| Erfasste Fälle Diff. in % | +4,6 | -6,7 | -19,4 | +11,2 | -4,5 |
| **Versuch** | 1.859 | 1.756 | 1.578 | 2.211 | 1.205 |
| **Aufgeklärte Fälle** | 16.247 | 14.667 | 11.028 | 12.631 | 13.396 |
| Aufgeklärte Fälle Differenz | -868 | -1.580 | -3.639 | +1.603 | +765 |
| Aufgeklärte Fälle Diff. in % | -5,1 | -9,7 | -24,8 | +14,5 | +6,1 |
| **AQ in %** | 72,2 | 69,9 | 65,2 | 67,2 | 74,6 |
| AQ Differenz in % | -7,4 | -2,3 | -4,7 | +2,0 | +7,4 |
| **Schaden in €** | 19.161.021 | 14.137.128 | 8.764.879 | 11.096.543 | 9.271.984 |
| Schaden Differenz | +5.653.983 | -5.023.893 | -5.372.249 | +2.331.664 | -1.824.559 |

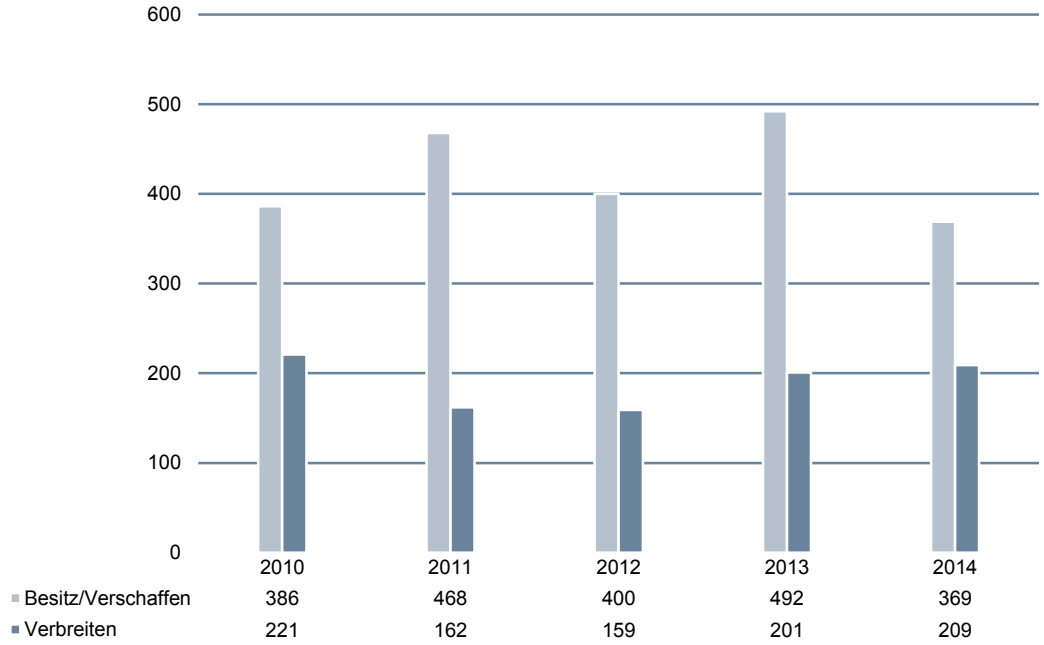
## 7 | PKS-BAROMETER CYBERCRIME TATMITTEL (2013 / 2014)

| PKS-Hauptschlüssel | 2013 | 2014 | +/- absolut | +/- in % | Barometer |
|---|---|---|---|---|---|
| **Internetkriminalität gesamt** | 18.804 | 17.949 | -855 | -4,5 | ↘ |
| **0000** (Straftaten gegen das Leben)** | 0 | 0 | 0 | 0 | → |
| **1000** (Straftaten gegen die sex. Selbstbestimmung)** | 851 | 792 | -59 | -6,9 | ↘ |
| **2000** (Rohheitsdelikte, Straft. gg. die pers. Freiheit)** | 354 | 463 | +109 | +30,8 | ↗ |
| **3*****, 4***** (Diebstahl mit und ohne erschw. Umstände)** | 1 | 2 | +1 | +100,0 | ↗ |
| **5000** (Vermögens- und Fälschungsdelikte)** | 13.593 | 12.936 | -657 | -4,8 | ↘ |
| **6000** (Sonst. Straftat-bestände gem. StGB)** | 3.341 | 3.069 | -272 | -8,1 | ↘ |
| **7000** (Strafrechtliche Nebengesetze)** | 664 | 687 | 23 | +3,5 | ↗ |

## 8 | PKS-BAROMETER KINDERPORNOGRAFIE (2013 / 2014)

| | PKS-Schlüssel | 2013 | 2014 | in % | Tendenz |
|---|---|---|---|---|---|
| **Besitz/Verschaffen von Kinder-pornografie (§ 184b StGB)** | 1433** | 492 | 369 | -25,0 | ↘ |
| **Verbreitung von Kinderporno-grafie (§ 184b StGB)** | 1434** | 201 | 209 | +4,0 | ↗ |

9 | **BESITZ/VERSCHAFFEN UND VERBREITEN VON KINDERPORNOGRAFIE FÜNFJAHRESVERGLEICH (2010-2014)**




10 | **DATENMENGEN KINDERPORNOGRAFIE AST KIPO FÜNFJAHRESVERGLEICH (2010-2014)**

| | 2010 | 2011 | 2012 | 2013 | 2014 |
|---|---|---|---|---|---|
| **Anlieferungen** | 7 | 9 | 22 | 35 | 48 |
| **Bilder** | 5.092 | 753 | 25.137 | 1.346.194 | 2.058.907 |
| **Videos** | 32 | 77 | 704 | 30.041 | 424.834 |

### ARBEITSBEREICH INTERNETRECHERCHE (AIR)

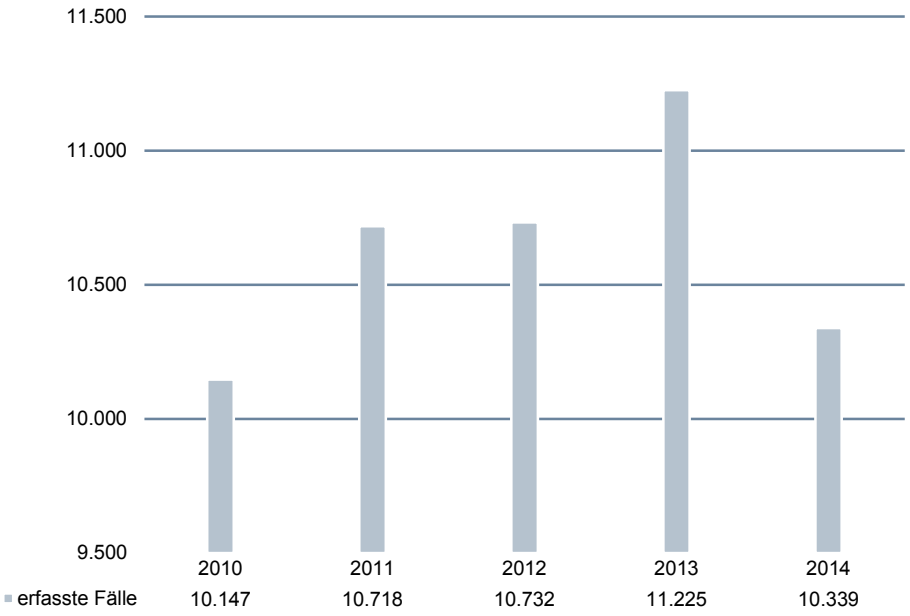
Der AIR hat die Aufgabe der brennpunktorientierten, nicht extern initiierten Suche nach Inhalten im Internet zum Zwecke der Gefahrenabwehr und der Weiterverfolgung von festgestellten, strafrechtlich relevanten Sachverhalten einschließlich der Beweissicherung bis hin zur Feststellung der Verantwortlichen und der örtlichen Zuständigkeiten von Polizei und Justiz.

Die Anzahl der generierten Strafverfahren ist stark abhängig von der Inanspruchnahme des AIR in Form von Einsatz- und Ermittlungsunterstützung für andere Abteilungen des LKA BW oder den Dienststellen des Landes.

## 11 | STRAFVERFAHRENINITIIERUNGEN AIR FÜNFJAHRESVERGLEICH (2010-2014)

| Berichtsjahr | 2010 | 2011 | 2012 | 2013 | 2014 |
|---|---|---|---|---|---|
| Deutschland | 66 | 420 | 40 | 297 | 731 |
| davon Baden-Württemberg | 3 | 24 | 4 | 25 | 69 |
| International | 1.045 | 7.720 | 636 | 5.419 | 9.656 |
| **Gesamt** | **1.111** | **8.164** | **676** | **5.716** | **10.387** |

## 12 | IT-BEWEISSICHERUNG – ENTWICKLUNG NEUER AUFTRÄGE (LANDESWEITE ÜBERSICHT 2010-2014)



# ANLAGEN

## BEGRIFFSBESTIMMUNGEN

| ***Begriff*** | ***Erläuterung*** |
|---|---|
| *Antivirenprogramm und Firewall* | *Schutzmaßnahmen zur Absicherung des eigenen Rechners. Antivirenprogramme enthalten Virenscanner, spüren bekannte Malware auf und identifizieren unbekannte Malware beispielsweise anhand ihres Verhaltens im System. Antivirenprogramme blockieren und beseitigen Malware. Firewalls sichern Datenverbindungen im Netzwerk ab. Sie können mittels Regeln durch den Anwender justiert werden und helfen, unerwünschten Datenverkehr zu blockieren.* |
| *App, Application* | *Software für mobile Endgeräte wie Tablets und Smartphones.* |
| *(Web-)Browser* | *Software, mit der Internetseiten und Dokumente aufgerufen werden können.* |
| *Brute Force Attack* | *Brute force steht für rohe Gewalt und bezeichnet eine Methode, bei der Rechenleistung und Wiederholungen eingesetzt werden, um beispielsweise den Zugang zu einer passwortgeschützten Datenbank zu erlangen oder einen Verschlüsselungscode zu knacken.* |
| *Bots, Botnetze/Botnet, Command & Control-Server, Zombie-PC* | *Unter einem Bot (vom englischen Begriff robot abgeleitet) versteht man ein Computerprogramm, das weitgehend selbständig sich wiederholende Aufgaben abarbeitet, ohne dabei auf eine Interaktion mit einem menschlichen Benutzer angewiesen zu sein. Der Rechner, auf dem die Bot-Software aktiv ist, wird dadurch Teil eines Netzwerks – eines sogenannten Botnet. Dieses Botnet kann im Weiteren gesteuert werden (durch den sog. Command & Control-Server/CC-Server), um z. B. Spam- oder Phishing-E-Mails zu versenden oder andere Rechner oder Server mittels einer DDoS-Attacke (Distributed Denial of Service) zu stören. Der infizierte Rechner wird häufig auch als Zombie-PC bezeichnet.* |
| *Chat* | *Chat steht für Unterhaltung, plaudern. Die Kommunikation findet in Echtzeit statt. Meist werden hierzu Chatrooms, also besondere Portale und Seiten im Internet benutzt, in denen sich Leute beispielsweise zu verschiedenen Themen treffen und austauschen. Die Kommunikation findet häufig mit mehreren Personen gleichzeitig statt. Es gibt verschiedene Techniken wie den (älteren) Internet Relay Chat (IRC), der Zusatzsoftware benötigt oder den Webchat, der im Browser ablaufen kann. Im Chat (aber auch in Foren) wird üblicherweise eine Netiquette (Network-Etiquette) eingefordert, dies sind Benimmregeln im gegenseitigen Umgang.* |
| *Cloud Computing* | *Cloud Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle.*<br>*Die Spannbreite, der im Rahmen von Cloud Computing angebotenen Dienstleistungen, umfasst das komplette Spektrum der Informationstechnik und beinhaltet unter anderem Infrastruktur (z. B. Rechenleistung, Speicherplatz), Plattformen und Software (Definition des BSI).* |

| | |
|---|---|
| *Cyberwar* | *Cyberwar ist aus den Wörtern Cyberspace und War zusammengesetzt und bedeutet zum einen die kriegerische Auseinandersetzung im und um den virtuellen Raum mit Mitteln vorwiegend aus dem Bereich der Informationstechnik. Zum anderen sind damit die hochtechnisierten Formen des Krieges im Informationszeitalter gemeint, die auf einer weitgehenden Computerisierung, Elektronisierung und Vernetzung fast aller militärischer Bereiche und Belange basieren. Übliche Zielrichtungen des Cyberwars sind Spionage, Sabotage und Manipulation.* |
| *Datenarten (Bestandsdaten, Verkehrsdaten und Inhaltsdaten)* | ***Bestandsdaten***<br>*Daten eines Teilnehmers, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden (§ 3 Nr. 3 TKG). Daten, die Anwender bei Vertragsabschluss oder -änderung beim Provider hinterlegen (zum Beispiel Adresse, Kontoverbindungen, Kopien, Personalausweisdaten etc.). Welche Auskünfte der Provider geben muss, ist in § 11 TKG geregelt.*<br>***Verkehrsdaten***<br>*Daten nach § 3 Nr. 30 TKG, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden (zum Beispiel Telefonnummern und Verbindungszeiten, Standortdaten von Mobiltelefonen, IP-Adressen und Zeitraum der Zuweisung zu einem Anschluss bei der Nutzung von Rechnern). Welche Verkehrsdaten durch den Verpflichteten gespeichert werden dürfen, ergibt sich aus § 96 TKG.*<br>***Inhaltsdaten***<br>*Alle tatsächlich übertragenen Daten, die nicht lediglich reine Verbindungs- und Steuerungsfunktion haben, zum Beispiel der Inhalt von Telefongesprächen.* |
| *Datengrößen/ Digitale Maßeinheiten* | *Ausgangsgröße ist das Byte. Größere Mengen werden mittels einer Zehnerpotenz dargestellt:*<br>*- 1 Kilobyte (KB) sind $10^3$ Byte = 1.000 Byte*<br>*- 1 Megabyte (MB) sind $10^6$ Byte = 1.000.000 Byte*<br>*- 1 Gigabyte (GB) sind $10^9$ Byte = 1.000.000.000 Byte*<br>*- 1 Terabyte (TB) sind $10^{12}$ Byte = 1.000.000.000.000 Byte*<br>*- 1 Petabyte (PB) sind $10^{15}$ Byte = 1.000.000.000.000.000 Byte*<br>*- 1 Exabyte (EB) sind $10^{18}$ Byte = 1.000.000.000.000.000.000 Byte* |
| *Digitale Identität, Identitätsdiebstahl bzw. Manipulation* | *Der Begriff „Identitätsdiebstahl" ist ein weit gefasster Begriff, der die missbräuchliche Nutzung personenbezogener Daten einer natürlichen Person durch Dritte bezeichnet. Identitätsdiebstahl im Kontext Cybercrime kann in vielerlei Ausprägungen stattfinden. Strafrechtlich relevant ist vor allem das „Ausspähen von Daten" (§ 202a StGB).* |
| *Domain, Top-Level-Domain* | *Eine Domain ist eine weltweit gültige und eindeutige Kennung, die bestimmten Regeln unterliegt. Ein Beispiel ist www.polizei-bw.de. Die sogenannte Top-Level-Domain oder auch Länderkürzel genannt, kennzeichnet in der Regel das Land (.de steht zum Beispiel für Deutschland), wobei es auch Top-Level-Domains gibt, die thematisch sind wie .com für commercial.* |

| | |
|---|---|
| *Domain Name Service (DNS)* | *Der DNS-Server wandelt die eindeutige IP-Adresse (numerisch) in den gewählten Domainnamen (zum Beispiel polizei-bw.de) um (auch Namensauflösung). Es handelt sich um einen zentralen Dienst im Internetverkehr. Deswegen ist er auch potentielles Ziel für Angriffe und Manipulationen.* |
| *DoS- und DDoS-Attacken* | *Als Denial of Service (kurz DoS, englisch für: Dienstverweigerung) wird in der digitalen Datenverarbeitung die Nichtverfügbarkeit eines Dienstes bezeichnet, der eigentlich verfügbar sein sollte. Obwohl es verschiedene Gründe für die Nichtverfügbarkeit geben kann, spricht man von DoS in der Regel als die Folge einer Überlastung von Infrastruktursystemen. Dies kann durch unbeabsichtigte Überlastungen verursacht werden oder durch einen mutwilligen Angriff auf einen Server, einen Rechner oder sonstige Komponenten in einem Datennetz.*<br>*Wird die Überlastung von einer größeren Anzahl anderer Systeme verursacht, so wird auch von einer verteilten Dienstblockade oder englisch Distributed Denial of Service (DDoS) gesprochen.* |
| *Download, Upload* | *Download bedeutet das Herunterladen einer Datei auf den lokalen Rechner. Im Gegenteil dazu bezeichnet der Upload das Hochladen von Daten, zum Beispiel in eine über das Internet zugängliche Datenbank oder Anwendung.* |
| *(Internet-)Forum/ Message Board* | *Internetforen bieten die Möglichkeiten, Fragen und Antworten sowie Gedanken und Anregungen auszutauschen. Die Kommunikation läuft hier asynchron, d. h. zeitversetzt und unterscheidet sich damit von Chats. Bereits kommentierte, d. h. fortgeschriebene, beantwortete Einträge werden Threads (englisch: Faden, Strang) genannt.* |
| *FTP* | *FTP bedeutet File Transfer Protocol (Datenübertragungsverfahren) und ist ein Netzwerkprotokoll zur Übertragung von Dateien über IP-Netzwerke.* |
| *Hacker* | *Sammelbegriff für IT-Spezialisten, im Regelfall negativ belegt. Zur weiteren Unterscheidung gibt es die Bezeichnungen „White-Hat", „Grey-Hat" oder „Black-Hat", welche die jeweilige Motivation und Loyalität zu Gesetzen und strafbaren Handlungen aufzeigt. „Black Hats" begehen Straftaten, um ihre meist kriminellen Ziele zu erreichen, sie stehen demnach auch im Fokus der Ermittlungsbehörden. „White Hats" hingegen führen z. B. Penetrationstests im Auftrag durch und besprechen mit dem Auftraggeber anschließend erkannte Schwachstellen sowie Lösungsmöglichkeiten.* |
| *Hashwerte* | *Bei Hashwerten handelt es sich um Prüfsummen zu elektronischen Daten/Dateien, die nach bestimmten Algorithmen errechnet werden. Umgangssprachlich können sie auch als „digitaler Fingerabdruck" bezeichnet werden.* |

| | |
|---|---|
| *HTML* | *HTML steht für Hypertext Markup Language. Mittels HTML können Dokumente und Webseiten aufgebaut werden. Mittels Webbrowser können diese Seiten dargestellt werden.* |
| *HTTP* | *HTTP bedeutet Hypertext Transfer Protocol. Es handelt sich um ein Hypertext-Übertragungsprotokoll und stellt ein nachrichtenorientiertes Kommunikationsprotokoll für Netzwerke dar. HTTP wird zur Übertragung von HTML-Webseiten und Daten in Netzwerken verwendet.* |
| *Hyperlink, Link* | *Sprungmarken, die zu einer bestimmten Textstelle, Datei oder im Internet zu einer Seite führen.* |
| *IMEI* | *IMEI steht für International Mobile Station Equipment Identity und ist die 15-stellige individuelle Seriennummer eines Mobiltelefons.* |
| *IMSI* | *IMSI steht für International Mobile Subscriber Identity. Mittels der IMSI können Geräte in GSM- und UMTS-Mobilfunknetzen eindeutig identifiziert werden. Die IMSI wird auf der SIM-Karte (Subscriber Identity Module) gespeichert. Sie werden durch die Mobilfunknetzbetreiber jeweils nur einmalig vergeben.* |
| *Internet Protocol Versionen – IPv4 und IPv6* | *Der Standard IPv4 benutzt 32-Bit-Adressen, wodurch, „nur" etwa 4,3 Milliarden eindeutige Adressen möglich sind. Dieser Bedarf ist zwischenzeitlich überschritten, die letzten freien Adressen wurden vergeben. Der neue Standard IPv6 besteht hingegen aus 128-Bit-Adressen. Dadurch gibt es zukünftig etwa 340 Sextillionen (eine Sextillion hat 36 Nullen) eindeutige Adressen.* |
| *IP-Adresse* | *IP steht für Internetprotokoll. In Computernetzwerken wird einzelnen Geräten auf Basis des Internetprotokolls eine Adresse zugewiesen. Durch die Adressierung können Geräte im Netzwerk erkannt und angesprochen werden (z. B. für den Datentransport). Meist werden Geräte automatisch konfiguriert und erhalten eine sogenannte dynamische IP-Adresse. Dynamisch bedeutet dabei, dass sie nicht dauerhaft durch das gleiche Gerät genutzt. Das Gegenteil sind statische IP-Adressen, die beispielsweise für Server oder Netzwerkdrucker üblich sind. Der aktuelle Standard zur Adressierung ist IPv4.* |
| *LAN und WLAN* | *LAN steht für Local Area Network. Durch solche lokalen Netzwerke werden meist Rechner in Privathäusern oder kleineren Firmen vernetzt. Erfolgt die Vernetzung kabellos mittels Funk, spricht man von Wireless (englisch: kabellos) LAN (WLAN).* |
| *Messenger, Instant Messaging* | *Messaging ist eine Form der modernen Unterhaltung unter Einsatz eines Messenger-Programms zwischen zwei oder mehr Personen. Die (Kurz-)Nachrichten werden dabei ohne Verzögerung an den Empfänger weitergeleitet. Diese Kommunikationsmethode ähnelt dem Chatten. Neben den eigentlichen Texten können je nach Software auch Links sowie Audio- und Videodaten übertragen werden.* |

| | |
|---|---|
| *Mobilfunkstandards (GSM, UMTS und LTE)* | *GSM (Global System for Mobile Communications)*<br>*GSM ist ein Standard für Mobilfunknetze. Er wird hauptsächlich für Telefonie genutzt. Zudem ermöglicht er die Übertragung von Kurzmitteilungen.*<br>*UMTS (Universal Mobile Telecommunations System)*<br>*UMTS ist ein Standard für Mobilfunk der dritten Generation (3G). Im Vergleich zu GSM sind deutlich höhere Datenübertragungsraten möglich.*<br>*LTE (Long Term Evolution)*<br>*Mobilfunkstandard der vierten Generation, der beispielsweise eine Downloadrate von bis zu 300 MBit/Sekunde erlaubt und damit UMTS nochmals übertrifft.* |
| *MTAN* | *(siehe TAN)* |
| *NAPT-Technik* | *Mit der Verwendung der Network-Adress-Port-Translation-Technik (NAPT) wird einer IP-Adresse eine Vielzahl von Nutzern zugeordnet. Damit soll erreicht werden, dass nicht zu viele IP-Adressen verbraucht werden.* |
| *Newsgroups* | *Nachrichtengruppen, die nach Themenbereichen geordnet sind und in der Regel von einem sogenannten Newsserver heruntergeladen werden. Neben der reinen Darstellung von Informationen werden Newsgroups für den Informationsaustausch genutzt. Die Kommunikation läuft dabei in der Regel asynchron, also zeitversetzt (anders als bei Chats, bei denen die Kommunikationspartner sich zur gleichen Zeit in einem Chatraum befinden und sprechen (schreiben)). Newsgroups ähneln damit eher Foren.* |
| *Operation/ Umfangsverfahren* | *Bei diesen Verfahren handelt sich um dezentral strafprozessual selbstständige Ermittlungsverfahren gegen eine Mehrzahl miteinander bekannter, intensiv in Verbindung stehender Tatverdächtiger mit Ermittlungserfordernissen in mindestens zwei Bundesländern oder Nationen.*<br>*Da bei länderübergreifenden Verfahren häufig auch Bezüge ins Ausland bestehen, sind sie unter dem aus dem internationalen Sprachgebrauch übernommenen Begriff „Operationen" zu führen. (Quelle: BLPG „Länderübergreifende Umfangsverfahren")* |
| *Peer-to-Peer/P2P, Client-Server-Modell* | *Peer-to-Peer (P2P)-Verbindungen sind dezentrale Rechner-Rechner-Verbindungen. Im Netzwerk sind bei dieser Verbindungsart alle Computer gleichberechtigt. Sie können Dienste in Anspruch nehmen und zur Verfügung stellen. Der Gegensatz zum Peer-to-Peer-Modell ist das Client-Server-Modell, in dessen Mittelpunkt ein zentraler Server steht. Dieser Server bietet Dienste an, die von den Clients genutzt werden.* |
| *Phishing* | *Phishing bedeutet übersetzt das „Fischen nach persönlichen Daten des Internetnutzers". Der Phisher schickt seinem Opfer in der Regel offiziell wirkende E-Mails, wie Rechnungen, Sicherheitshinweise oder Benutzerinformationen, die es verleiten sollen, dem Täter vertrauliche Informationen, vor allem Benutzernamen und Passwörter oder PIN und TAN von Online-Banking-Zugängen, preiszugeben. Mit den gestohlenen Zugangsdaten kann der Phisher die Identität* |

| | |
|---|---|
| | *seines Opfers übernehmen und in dessen Namen Handlungen ausführen. Im Internet werden so gestohlene Daten in ganzen Paketen zum Kauf angeboten.* |
| *Pop-up-Fenster* | *Pop up bedeutet im Englischen etwa plötzlich auftauchen und bezieht sich insbesondere auf Fenster, die gewünscht (zum Beispiel Kontextmenü, das mittels rechter Maustaste in vielen Programmen aufgerufen werden kann) oder unerwünscht (zum Beispiel Werbung im Internet beim Aufrufen einer Webseite) erscheinen. Viele Browser bieten inzwischen Pop-up-Blocker an, die diesen Vorgang beim Internetsurfen verhindern.* |
| *Provider* | *Provider bedeutet Anbieter und wird meist nur verkürzt benutzt. Übliche Langbegriffe sind Mobilfunkprovider, Telekommunikationsdienstprovider oder Internet-Service-Provider. Provider (auch Access-Provider genannt) bieten beispielsweise einen Zugang zum Internet gegen eine monatliche Gebühr an.* |
| *Proxy* | *Ein Proxyprogramm ist eine Kommunikationsschnittstelle in einem Netzwerk und steht als Mittelsmann zwischen anfragendem Rechner und Zielrechner. Proxys können zu verschiedenen Zwecken eingesetzt werden, zum Beispiel zur Anonymisierung oder zur Filterung.* |
| *Ransomware, Digitale Erpressung* | *Als Ransomware werden Schadprogramme bezeichnet, mit deren Hilfe ein Eindringling eine Zugriffs- oder Nutzungsverhinderung der Daten sowie des gesamten Computersystems erwirkt. Dabei werden private Daten auf einem fremden Computer verschlüsselt oder der Zugriff auf diese wird verhindert, um für die Entschlüsselung oder Freigabe ein Lösegeld zu fordern. Es handelt sich folglich um eine digitale Form einer Erpressung. Die Bezeichnung „Ransomware" setzt sich aus der Zugehörigkeit zur Klasse der Malware sowie der englischen Bezeichnung für Lösegeld (= „ransom") zusammen.* |
| *Scareware* | *Bei Scareware, alternativ auch „Fake-AV" (AV steht für Antivirus) genannt, handelt es sich um Software, die darauf ausgelegt ist, Computernutzer zu verunsichern (scare bedeutet Schrecken). Dies erfolgt durch ein kostenlos zur Verfügung gestelltes angebliches Antivirenprogramm oder aber durch Anzeigen bzw. Animationen über Webseiten im Internet. Der Schaden für den Nutzer kann darin bestehen, dass er aus Angst ein nutzloses Programm erwirbt oder dass er erst durch das Aufspielen der Software Schadsoftware auf seinen Rechner bringt.* |
| *Schadprogramme, Schadsoftware, Malware* | *Sammelbegriff für Computerprogramme, die unerwünschte, schädliche oder zerstörende Funktionen haben. Der Begriff Malware ist dabei eine Wortschöpfung aus den englischen Begriffen malicious (boshaft) und Software. Der Sammelbegriff umfasst insbesondere Viren, Würmer, Trojanische Pferde, Scareware, Spyware und Ransomware.* |
| *Smartphones* | *Smartphones sind Mobiltelefone, die den Fokus auf die Nutzung des Internets und dessen Dienste legen, während klassische Mobiltelefone den Schwerpunkt auf Telefonie und Dienste zur einfachen Nachrichtenübermittlung (zum Beispiel SMS) legen.* |

| | |
|---|---|
| *Social Engineering* | *Methode, um mit zwischenmenschlichen Kontakten (unmittelbar oder mittelbar) bestimmte Verhaltensweisen auszulösen, zum Beispiel Herausgabe von vertraulichen Informationen oder Passwörtern. Erfolgreiches Social Engineering basiert häufig auf falschem Vertrauen und greift im Bereich Cybercrime nicht die technische Komponente, sondern die menschliche Komponente an. Beispiele sind der gefälschte Anruf eines Technikers aus der Firma, der den Passwortzugang zur Wartung benötigt, oder die Nutzung einer gefälschten E-Mail-Adresse oder falscher Identitäten (zum Beispiel in sozialen Netzwerken).* |
| *Spam* | *Als Spam-Mail werden unerwünscht übertragene Nachrichten bezeichnet. Der Inhalt reicht von lästiger Werbung über Phishing-Mails bis hin zur direkten Übersendung von Malware (häufig in Anlagen integriert, die beim absichtlichen oder versehentlichem Öffnen Schadsoftware auf den Rechner übertragen).* |
| *Spoofing* | *Spoofing umfasst Manipulation, Verschleierung und Vortäuschung und kann in der IT zur Täuschung des Gegenübers eingesetzt werden. Möglichkeiten gibt es viele, man kann zum Beispiel angezeigte Telefonnummern verändern (Call-ID-Spoofing), IP-Adressen ändern (IP-Spoofing), oder die Umwandlung von IP-Adressen in Domain Names fingieren (DNS-Spoofing).* |
| *Tablet(-Computer)* | *Tablets sind mobile Computer, die anders als Note- und Netbooks in der Regel nicht einklappbar sind und keine eigene Tastatur haben, sondern mittels Touchscreen gesteuert werden. Übliche Bildschirmgrößen sind zehn, acht und sieben Zoll. Tablets werden von unterschiedlichen Herstellern produziert und verbreiten sich derzeit neben Smartphones insbesondere wegen der hohen Mobilität sehr stark.* |
| *TAN, mTAN, ChipTAN* | *TAN ist die Abkürzung für Transaktionsnummer. TAN werden im Onlinebanking verwendet und funktionieren wie Einmalpasswörter. Der Kunde erhält von seiner Bank in der Regel einen Bogen mit etwa 50 TAN, die er bei Onlinebanking-Vorgängen nach Abfrage eingeben muss. Inzwischen gibt es mehrere Varianten des Verfahrens. Das mTAN-Verfahren (m steht für mobile) bindet Mobiltelefone in den Onlinebanking-Vorgang ein. Per SMS wird dem Bankkunden eine TAN gesendet, die er in den Rechner übertragen muss. Beim ChipTAN-Verfahren erwirbt der Bankkunde ein Zusatzgerät (Kartenlesegerät) und bindet seine persönliche Bankkarte in den Onlinebanking-Vorgang ein.* |
| *Spam* | *Als Spam-Mail werden unerwünscht übertragene Nachrichten bezeichnet. Der Inhalt reicht von lästiger Werbung über Phishing-Mails bis hin zur direkten Übersendung von Malware (häufig in Anlagen integriert, die beim absichtlichen oder versehentlichem Öffnen Schadsoftware auf den Rechner übertragen).* |

| | |
|---|---|
| *Spear-Phishing* | *Neue bzw. Sonderform des Phishing, bei dem die Opfer (in der Regel eine bestimmte Gruppe, z. B. alle Mitarbeiter eine Firma) gezielt ausgewählt und angegriffen werden. Die Informationen, die das Ziel zu einer bestimmten Aktion verleiten sollen, sind auf das Ziel bzw. die Zielgruppe abgestimmt bzw. weisen zum Beispiel einen örtlichen/persönlichen Bezug auf. Spear-Phishing ist deutlich erfolgreicher als klassisches Phishing.* |
| *Spoofing* | *Spoofing umfasst Manipulation, Verschleierung und Vortäuschung und kann in der IT zur Täuschung des Gegenübers eingesetzt werden. Möglichkeiten gibt es viele, man kann zum Beispiel angezeigte Telefonnummern verändern (Call-ID-Spoofing), IP-Adressen ändern (IP-Spoofing), oder die Umwandlung von IP-Adressen in Domain Names fingieren (DNS-Spoofing).* |
| *Spyware* | *Diese Art von Software forscht bzw. spioniert (englisch to spy) den Computer und das Nutzerverhalten aus. Die Daten werden an Dritte (oder den Urheber selbst) weitergeleitet. Die Informationen können für unterschiedliche Zwecke weiterverwendet werden – von unerwünschter Werbung bis hin zu Datenmissbrauch zur Begehung von Straftaten.* |
| *SSL bzw. TLS* | *SSL steht für Secure Sockets Layer. SSL wurde inzwischen durch den Nachfolger TLS (Transport Layer Security) abgelöst. Es handelt sich um Verschlüsselungsprotokolle, die einen sicheren Datentransport gewährleisten. Eine typische Anwendung ist HTTPS (Hypertext Transfer Protocol Secure).* |
| *Tablet(-Computer)* | *Tablets sind mobile Computer, die anders als Note- und Netbooks in der Regel nicht einklappbar sind und keine eigene Tastatur haben, sondern mittels Touchscreen gesteuert werden. Übliche Bildschirmgrößen sind zehn, acht und sieben Zoll. Tablets werden von unterschiedlichen Herstellern produziert und verbreiten sich derzeit neben Smartphones insbesondere wegen der hohen Mobilität sehr stark.* |
| *TAN, mTAN, ChipTAN* | *TAN ist die Abkürzung für Transaktionsnummer. TAN werden im Onlinebanking verwendet und funktionieren wie Einmalpasswörter. Der Kunde erhält von seiner Bank in der Regel einen Bogen mit etwa 50 TAN, die er bei Onlinebanking-Vorgängen nach Abfrage eingeben muss. Inzwischen gibt es mehrere Varianten des Verfahrens. Das mTAN-Verfahren (m steht für mobile) bindet Mobiltelefone in den Onlinebanking-Vorgang ein. Per SMS wird dem Bankkunden eine TAN gesendet, die er in den Rechner übertragen muss. Beim ChipTAN-Verfahren erwirbt der Bankkunde ein Zusatzgerät (Kartenlesegerät) und bindet seine persönliche Bankkarte in den Onlinebanking-Vorgang ein.* |
| *TOR* | *TOR (The Onion Routing) ist ein Netzwerk zur Anonymisierung von Verbindungsdaten, das seine Nutzer vor der Analyse des Datenverkehrs schützt. Die dabei angewendete Technik ist die kaskadierte Verschlüsselung. Als Kaskadierung wird das Hintereinanderschalten mehrerer Systeme bezeichnet (deswegen auch der Bezug zu einer Zwiebel, englisch onion).* |

| | |
|---|---|
| *Trojanische Pferde (kurz Trojaner)* | *Ein Trojanisches Pferd besteht aus zwei Bestandteilen, einem in der Regel nützlichen Programmteil, das einen Zweck erfüllt, den der Nutzer erzielen möchte und einem versteckten Programmteil, der im Hintergrund arbeitet und unerwünschte Software aufspielt oder Veränderungen am Computersystem vornimmt. Häufig wird Spyware oder eine sogenannte Backdoor (eine „Hintertür", durch die der Täter später ungesehen in das System eindringen kann) aufgespielt, mit deren Hilfe der Täter Daten erlangt oder Veränderungen vornehmen kann.* |
| *URL* | *URL steht für Uniform Resource Locator und bedeutet einheitlicher Quellenanzeiger. Mit URL werden Adressen beschrieben, die eine bestimmte Ressource in einem Netzwerk lokalisieren. Dazu werden das verwendete Netzwerkprotokoll (z. B. HTTP, FTP et cetera) und der Ort der Ressource angegeben.* |
| *(Computer)Virus* | *Computerviren sind die älteste Art der Malware. Sie verbreiten sich, indem sie Kopien von sich selbst in Programme, Dokumente, Datenträger oder den Bootbereich schreiben. Dabei finden Manipulationen statt, die der Benutzer nicht kontrollieren kann. Die Folgen reichen dabei von einfachen Manipulationen bis hin zum kompletten Systemabsturz.*<br>*Eine besonders heimtückische Art von Viren sind polymorphe Viren. Sie verändern selbständig ihren eigenen Programmcode, tarnen sich dadurch und werden deshalb besonders schwer von Antivirenprogrammen entdeckt.* |
| *Webseite (engl. Website) und Homepage* | *Eine Webseite bezeichnet die Gesamtheit aller Dokumente (die gesamte Webpräsenz), die über eine Adresse im Internet erreichbar ist.*<br>*Der Begriff Homepage wird häufig gleichbedeutend mit Webseite benutzt. Streng genommen ist die Homepage jedoch nur das Begrüßungsportal, das zu den weiteren Inhalten der Webseite führt.* |
| *(Computer-)Wurm* | *Würmer ähneln Viren und verbreiten sich direkt über Netzwerke wie das Internet, Firmenintranets, Peer-to-Peer-Netzwerken aber auch Wechselmedien. Zielrichtung eines Wurms ist dabei die schnelle (weltweite) Verbreitung.* |

# ANSPRECHPARTNER


**ANSPRECHPARTNER**

**ÖFFENTLICHKEITSARBEIT**

Telefon 0711 5401-2012 und -3012

Fax 0711 5401-1012

E-Mail stuttgart.lka.oe@polizei.bwl.de

# IMPRESSUM

**CYBERCRIME / DIGITALE SPUREN**

**JAHRESBERICHT 2014**


**HERAUSGEBER**

Landeskriminalamt Baden-Württemberg
Taubenheimstraße 85
70372 Stuttgart

Telefon 0711 5401-0
Fax 0711 5401-3355
E-Mail stuttgart.lka@polizei.bwl.de
Internet www.lka-bw.de

**GESTALTUNG**

Liane Köhnlein, LKA BW

**DRUCK**

e. kurz + co, Stuttgart





**BILDQUELLEN**

LKA BW, fotolia.com

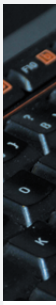



*Diese Informationsschrift wird im Auftrag der Landesregierung Baden-Württemberg im Rahmen ihrer verfassungsrechtlichen Verpflichtung zur Unterrichtung der Öffentlichkeit herausgegeben.*
*Sie darf weder von Parteien noch von deren Kandidaten oder Helfern während eines Wahlkampfs zum Zwecke der Wahlwerbung verwendet werden. Dies gilt für alle Wahlen.*

*Missbräuchlich sind insbesondere die Verteilung auf Wahlveranstaltungen und an Informationsständen der Parteien sowie das Einlegen, Aufdrucken oder Aufkleben parteipolitischer Informationen oder Werbemittel.*

*Untersagt ist auch die Weitergabe an Dritte zum Zwecke der Wahlwerbung.*
*Auch ohne zeitlichen Bezug zu einer Wahl darf die vorliegende Druckschrift nicht so verwendet werden, dass dies als Parteinahme des Herausgebers zugunsten einzelner politischer Gruppen verstanden werden könnte.*
*Diese Beschränkungen gelten unabhängig vom Vertriebsweg, also unabhängig davon, auf welchem Wege und in welcher Anzahl diese Informationsschrift dem Empfänger zugegangen ist.*

*Erlaubt ist jedoch den Parteien, die Informationsschrift zur Unterrichtung ihrer Mitglieder zu verwenden.*



# 2014