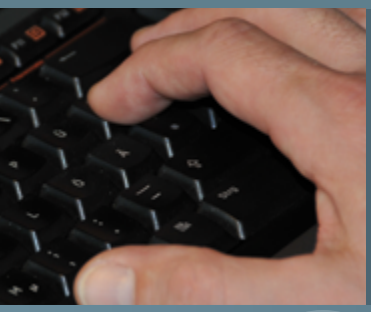



2012

LKA BW

Cyberkriminalität/ Digitale Spuren

JAHRESBERICHT 2012

Baden-Württemberg

LANDESKRIMINALAMT

IMPRESSUM

CYBERKRIMINALITÄT / DIGITALE SPUREN

JAHRESBERICHT 2012

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

Übelmesser Druck Eberhard Poth, Stuttgart

© LKA BW, 2013

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, Aufdrukken 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 der Herausgeberin 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.

CYBERKRIMINALITÄT / DIGITALE SPUREN

	2011	2012	
GESAMT[1]	**24.848**	**20.913**	↘ - 15,8 %
COMPUTERKRIMINALITÄT	9.048	8.907	→
INTERNETKRIMINALITÄT	20.988	16.912	↘

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

INHALT

1 ANALYSEDARSTELLUNG

Neue Technologien bereichern das Leben. Es gibt aber auch Schattenseiten. Kriminelle nutzen das Internet oder andere Dienste zur Begehung von Straftaten bzw. greifen die Datenverarbeitungs-Systeme direkt an. Die Fallzahlen sind im Mehrjahresvergleich deutlich angestiegen. Aktuell werden Millionen von Computern ohne Wissen der Besitzer fremdgesteuert und zur Verteilung von *Schadsoftware*[2] aber auch zur Begehung schwerer Straftaten genutzt. *Botnetze*, *Schadsoftware* und sich ständig ändernde Tatbegehungsweisen verursachen bei betroffenen Bürgern, Behörden und Wirtschaftsunternehmen einen hohen materiellen und immateriellen Schaden. Straftaten werden den Sicherheitsbehörden nicht mehr gemeldet, um einen Imageschaden zu vermeiden. Das Dunkelfeld vergrößert sich dadurch noch weiter. Im virtuellen Raum entsteht eine digitale Schattenwirtschaft, die sich der im Internet zur Verfügung gestellten Tatwerkzeuge bedient, um Straftaten zu begehen. Es wird mit Waffen, Rauschgift und Kinderpornografie gehandelt. Dabei ist das Internet nur Mittel zum Zweck. Die Organisierte Kriminalität erschließt sich den virtuellen Raum als zusätzliche Einnahmequelle. Diesen Herausforderungen stellt sich die Polizei Baden-Württemberg mit einer flächendeckenden Organisationsstruktur, mit der Erarbeitung von Standards und Geschäftsprozessen sowie einer weiteren Qualifizierung und Professionalisierung polizeilicher Arbeit.

EINRICHTUNG DER ABTEILUNG „CYBERKRIMINALITÄT / DIGITALE SPUREN“ UND AKTUELLE ENTWICKLUNGEN

Am 1. Januar 2012 wurde die Abteilung „Cyberkriminalität/Digitale Spuren“ beim Landeskriminalamt Baden-Württemberg (LKA BW) eingerichtet. Die Neuorganisation und das Zusammenführen von Spezialisten aus verschiedenen Abteilungen des LKA BW sowie die eindeutige Schwerpunktsetzung haben sich bewährt, soviel kann nach einem Jahr bereits gesagt werden. Schnittstellen wurden minimiert und Kompetenzen gebündelt.

Im Rahmen der baden-württembergischen Polizeireform werden im Jahr 2014 auf Ebene der regionalen Polizeipräsidien eigene Kriminalinspektionen (K5) eingerichtet. Diese sind spiegelbildlich zur neuen Abteilung des LKA BW aufgebaut (ausgenommen sind zentrale Servicefunktionen sowie das Kompetenzzentrum Telekommunikationsüberwachung). Neben Auswertung und Ermittlungen werden dort zukünftig auch Aufgaben der IT-Beweissicherung sowie der Analyse strukturierter Massendaten zentral wahrgenommen.

BEDEUTUNG DES INTERNETS

ARD und ZDF erstellen seit dem Jahr 1997 die sogenannte ARD/ZDF-Onlinestudie zur Entwicklung der Internetnutzung in Deutschland sowie dem Umgang der Nutzer mit den Angeboten.
Die Befragungen sind repräsentativ und umfassen alle bundesdeutschen Erwachsenen ab 14 Jahre.

[2] *Fachbegriffe, die im Text verwendet werden oder im Zusammenhang mit Cyberkriminalität und dem Themenkomplex digitale Spuren häufig auftauchen, sind kursiv dargestellt und in den Anlagen unter „Begriffsbestimmungen“ erklärt.*

Im Jahr 2012 gaben 75,9 % der Befragten an, dass sie online sind. Damit gibt es in Deutschland rund 53 Millionen Internetnutzer ab 14 Jahre, etwa 1,7 Millionen Nutzer mehr als im Jahr 2011. Gegenüber dem Jahr 2000 mit 18,4 Millionen Nutzern hat sich die Zahl nahezu verdreifacht. Die stärksten Zuwachsraten verzeichnen dabei Nutzer über 50 Jahre. Bei den untersuchten Altersgruppen zeigen sich dennoch erhebliche Unterschiede. Bis zum Alter von 49 Jahren sind zwischen 90 und 100 % der Befragten online, während es bei den 50- bis 59-Jährigen 76,8 % und bei den ab 60-Jährigen 39,2 % sind. Die mobile Internetnutzung mittels *Smartphones* und *Tablets* nimmt zu und ergänzt den Zugang ins Netz mit stationären Rechnern. Hier haben sich die Zahlen in den letzten drei Jahren mehr als verdoppelt (Anstieg von elf auf 23 %). Die Befragung ergibt weiterhin, dass die Befragten durchschnittlich 133 Minuten pro Tag im Netz verbringen.

DUNKELFELDSTUDIEN

Die Polizeiliche Kriminalstatistik (PKS) ist die wichtigste Quelle zu Aussagen zum sogenannten Hellfeld, der bekannt gewordenen registrierten Kriminalität. Davon abzugrenzen ist das sogenannte Dunkelfeld, das die Summe aller Straftaten umfasst, die der Polizei nicht bekannt werden und deshalb auch in keine Statistik einfließen. Im Bereich Cyberkriminalität ist ein besonders hohes Dunkelfeld zu prognostizieren. Umfassende wissenschaftliche Dunkelfeldstudien gibt es derzeit jedoch noch nicht.

Tendenzielle Aussagen aus repräsentativen Befragungen, die durch verschiedene Unternehmen und Berufsverbände veröffentlicht werden, enthalten wertvolle Hinweise für die Polizei. Eine repräsentative Umfrage des Branchenverbands BITKOM im Jahr 2012[3] ergab beispielsweise, dass sich drei Viertel aller deutschen Internetuser im Web bedroht fühlen. Jeder zweite Internetnutzer gab an, bereits persönliche Erfahrungen mit Internetkriminalität gemacht zu haben. Das entspricht hochgerechnet 28 Millionen Menschen in Deutschland! Genannt wurden in diesem Zusammenhang beispielsweise Vorfälle mit Schadprogrammen (36 %), das Ausspähen von Zugangsdaten (16 %), Betrug im Zusammenhang mit Online-Shopping oder sexueller Belästigung (jeweils 12 %).

Diese Tendenzen müssen von der Polizei im Umgang mit der zunehmenden Verlagerung von Kriminalität in das Internet berücksichtigt werden, denn das polizeiliche Hellfeld spiegelt nur einen Bruchteil dieser repräsentativ erhobenen Ergebnisse wider.

DEFINITION CYBERCRIME UND CYBERKRIMINALITÄT

Die Internationalität war ein wesentlicher Grund dafür, den bereits verwendeten Begriff „Cybercrime“ bundeseinheitlich und verbindlich zu definieren.

„Cybercrime umfasst die Straftaten, die sich gegen

- das Internet,
- weitere Datennetze,
- informationstechnische Systeme

[3] *repräsentative BITKOM-Umfrage 2012 (u. a. Presseinformation BITKOM vom 16. März 2012)*

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

In Baden-Württemberg wird der Begriff Cybercrime synonym zu Cyberkriminalität verwendet. Wir unterscheiden zwischen Cyberkriminalität im weiteren Sinne (PKS-Begriff Internetkriminalität) und Cyberkriminalität im engeren Sinne (PKS-Begriff Computerkriminalität). Der PKS-Begriff Internetkriminalität umfasst alle Straftaten, die mit dem Tatmittel Internet begangen werden und der PKS-Begriff Computerkriminalität umfasst Straftaten, bei denen Elektronische Datenverarbeitung (EDV) in den Tatbestandsmerkmalen der Strafnorm genannt ist (z. B. die Datenveränderung gem. § 303a Strafgesetzbuch (StGB)).

LAGE DER CYBERKRIMINALITÄT 2012

„Analoges Verbrechen lohnt sich nicht" – so könnte die Überschrift einer aktuellen Pressemitteilung zur Gesamtentwicklung der Kriminalität lauten. Der digitale Wandel macht auch vor den klassischen Kriminalitätsformen keinen Halt. Das Risiko, das mit dem Überfall einer Bank einhergeht, ist mit dem eines digitalen Verbrechens in der Anonymität der Online-Welt nicht gleichzusetzen. Der Versuchung, mittels virtueller Strumpfmaske und digitalem Waffenarsenal auf Beutezug zu gehen, können viele Täter nicht widerstehen. Wie einschlägige Strafverfahren der Internetkriminalität zeigen, werden dort heute schon Summen erlangt, die die klassischen „analogen" Modi Operandi der allgemeinen und Organisierten Kriminalität in den Schatten stellen.
Die Schlüssel dazu liefern Schwachstellen in der Software der Betriebssysteme und der Anwendungen. Laut eines Artikels der „Wirtschaftswoche"[4] meldeten im Dezember 2012 IT-Sicherheitsdienste, dass allein die Betrugssoftware „Eurograbber" in Online-Banking-Vorgänge von rund 30.000 europäischen Bankkunden eingegriffen hat und die Kunden um hochgerechnet 36 Millionen Euro geschädigt wurden.

Anlagen | 1-2

INTERNETKRIMINALITÄT (CYBERKRIMINALITÄT IM WEITEREN SINNE)

Nahezu alle Delikte, die in der realen Welt verübt werden, können auch im virtuellen Raum begangen werden. Im Jahr 2012 wurden 16.912 Straftaten der Internetkriminalität erfasst. Dies stellt einen Rückgang um 4.076 Fälle oder 19,4 % dar. Im Vergleich der letzten fünf Jahre stellt dieser Wert eine deutliche Abnahme dar, da in den Vorjahren jeweils etwa 20.000 Fälle registriert wurden. Sie wird fast ausschließlich durch den Rückgang der Vermögens- und Fälschungsdelikte verursacht. Die in diesem Deliktsfeld erfassten Fälle sind mit einem Rückgang um 24,7 % auf 12.219 Fälle (16.220 Fälle)[6] deutlich rückläufig. Ausschlaggebend sind Rückgänge im Bereich des Waren-/Warenkreditbetrugs um 26,8 % auf 5.729 Fälle (7.829 Fälle), des „sonstigen Betrugs"[5] um 23,3 % auf 5.367 Fälle

4 *„IT-Sicherheit. Wie Online-Betrüger und Cyber-Spione zu Werke gehen", Thomas Kuhn, 12. Januar 2013*
5 *Vorjahreszahlen in Klammern*
6 *PKS-Schlüssel 5170***

(6.999 Fälle) – darunter Computerbetrug um - 17,0 % auf 2.896 Fälle (3.489 Fälle) und Rückgänge bei den weiteren Betrugsarten um 32,3 % auf 2.004 Fälle (2.960 Fälle).

Im Bereich des Warenbetrugs sind die Fallzahlen bereits seit dem Jahr 2010 rückläufig. Warenbetrug im Internet wird über Online-Shops und Auktionsplattformen – oftmals über mehrere Jahre hinweg – begangen. Der Rückgang des Deliktsaufkommens resultiert u. a. aus Abschlüssen mehrerer Großverfahren mit hohen Fallzahlen im Regierungsbezirk Tübingen im Jahr 2011, während 2012 keine vergleichbaren Verfahren in die Statistik eingeflossen sind.
Bei den strafrechtlichen Nebengesetzen ist entgegen den Vorjahren erstmals wieder ein leichter Anstieg um 17,7 % auf 691 Fälle (587 Fälle) zu verzeichnen. Dieser Anstieg ist auf die Entwicklung bei den Urheberrechtsverstößen als Teilbereich der strafrechtlichen Nebengesetze zurückzuführen.
Im Jahr 2012 stiegen Urheberrechtsverstöße um 36,5 % auf 572 Fälle (419 Fälle). Im Jahr 2008 wurden in diesem Bereich jedoch noch 1.812 Fälle registriert. Der Rückgang im Mehrjahresvergleich resultiert aus einer Vereinfachung bei der zivilrechtlichen Verfolgung von Urheberrechtsverstößen, bei denen Geschädigte und Rechteverwerter ohne Strafanzeige Daten über den mutmaßlichen Täter erlangen können.

Die Straftaten gegen die sexuelle Selbstbestimmung sind um 10,4 % auf 637 Fälle (711 Fälle) gesunken und erreichen damit einen ähnlichen Wert wie im Jahr 2010 (657 Fälle). Ein Einflussfaktor ist der Rückgang der Delikte Besitz/Verschaffen von Kinderpornografie (mit Tatmittel Internet) um 16,8 % auf 272 Fälle (327 Fälle), der im nächsten Abschnitt näher betrachtet wird.

Die Bearbeitung der Internetkriminalität findet im LKA BW in allen Ermittlungsabteilungen und bei den örtlichen Dienststellen auf Ebene der Schutz- und Kriminalpolizei statt. Die polizeiliche Bearbeitungszuständigkeit richtet sich nach dem Grunddelikt. Die Nutzung des Tatmittels Internet stellt dabei keine strafrechtliche Qualifizierung dar, sondern ist als Sonderform oder Variante der Deliktsbegehung anzusehen. Deshalb sind in verschiedenen Jahresberichten weitere Informationen zur Internetkriminalität zu finden. Beispielsweise werden die Zusammenhänge und Bezüge der Organisierten Kriminalität und der Bandenkriminalität zur Cyberkriminalität im Jahresbericht „Organisierte Kriminalität“ dargestellt. Politisch motivierte Täter nutzen das Internet zur Radikalisierung (z. B. *Webseiten* mit Propagandamaterial, Verbreitung von Ideologien), Rekrutierung und Mobilisierung (z. B. über *Soziale Netzwerke*, Foren) und nicht zuletzt auch zur Begehung von Straftaten (z. B. das Outing von ideologischen Gegnern, dem regelmäßig Straftaten wie das Ausspähen von Daten vorangehen). Weitere Informationen sind im LKA-Jahresbericht „Politisch motivierte Kriminalität“ zu finden. Eine ausführliche Betrachtung der Vermögensdelikte und der Wirtschaftskriminalität sowie deren Bezüge zur Cyberkriminalität ist im Jahresbericht „Wirtschaftskriminalität“.

KINDERPORNOGRAFIE

ANSPRECHSTELLE KINDERPORNOGRAFIE

Die Ansprechstelle Kinderpornografie (ASt Kipo) ist der Inspektion 710 des LKA BW angegliedert. Sie ist die zentrale Ansprechstelle des Landes für den Komplex Besitz/Verschaffen und Verbreitung von Kinderpornografie.

Anlagen | 3-4

BESITZ / VERSCHAFFEN KINDERPORNOGRAFISCHER SCHRIFTEN

Im Deliktsbereich Besitz/Verschaffen kinderpornografischer Schriften ist für das Jahr 2012 ein Rückgang der Fallzahlen um 14,5 % auf 400 Fälle (468 Fälle) zu verzeichnen. Diese Deliktsform wird vorwiegend über das Internet begangen. Die Fallzahlen mit dem Tatmittel „Internet" verringerten sich korrespondierend um 16,8 % auf 272 Fälle (327 Fälle). Die Aufklärungsquote betrug 95,6 % (90,2 %). Die Anzahl der polizeilich registrierten Straftaten der Verbreitung von Kinderpornografie blieb mit 159 Fällen hingegen annähernd auf dem Stand des Vorjahres mit 162 Fällen. Der Anteil der Straftaten mit Tatmittel Internet ist dabei jedoch um 27,7 % auf 120 Fälle (94 Fälle) gestiegen. Im Fünfjahresvergleich relativiert sich diese Feststellung, da im Jahr 2011 deutlich weniger Fälle als in den Vorjahren festgestellt wurden.

Die Fallzahlen der beiden Deliktsformen Besitz/Verschaffen und Verbreitung von kinderpornografischen Inhalten ergeben insgesamt 559 Fälle und liegen damit unter dem Niveau der Vorjahre (2011: 630, 2010: 607).

OPERATIONEN / UMFANGSVERFAHREN

Die ASt Kipo bearbeitete im Jahr 2012 52 Operationen (OP)/Umfangsverfahren mit 277 Tatverdächtigen (TV) in Baden-Württemberg. Damit ist im Vergleichszeitraum die Anzahl der OP zwar gefallen, jedoch die Zahl der TV im Gegensatz zur Entwicklung der PKS-Zahlen gestiegen (2011: 63 OP mit 214 TV in Baden-Württemberg).

HERAUSRAGENDE ERMITTLUNGSVERFAHREN

OP „FIRST"

Mitte des Jahres 2012 ging bei der ASt Kipo ein Hinweis auf eine Webseite i. Z. m. der Verbreitung von Kinderpornografie ein. Bei der Überprüfung dieser Webseite wurden kinder- bzw. jugendpornografische Bild- und Videodateien festgestellt. Nach Unterrichtung des deutschen Serverbetreibers wurden die strafrechtlich relevanten Inhalte aus dem Netz entfernt und die notwendigen Daten gesichert.
Bei der Überprüfung des bereits sichergestellten Access-Log (Logdatei) konnte festgestellt werden, dass es innerhalb von vier Tagen zu 1.382 Zugriffen durch 120 unterschiedliche IP-Adressen aus 16 Nationen auf die als kinderpornografisch eingestuften Dateien kam.

Nach Auswertung dieser Zugriffe konnten gegen 28 Inhaber deutscher IP-Adressen Ermittlungsverfahren eingeleitet werden. Bei 14 weiteren deutschen IP-Adressen konnte aufgrund der fehlenden Rechtsgrundlage zur Vorratsdatenspeicherung der Inhaber nicht mehr ermittelt werden.

ERMITTLUNGSVERFAHREN „STRAWBERRY"

In einem von der ASt Kipo bearbeiteten Ermittlungsverfahren, bei dem miteinander verknüpfte Webseiten mit kinderpornografischen Inhalten festgestellt wurden, trat bei der Beweissicherung die Besonderheit auf, dass die verknüpften *Webseiten* teilweise nur dann kinder-, jugend-, gewalt- und tierpornografisches Material anzeigten, wenn der Aufruf von der Ursprungswebseite erfolgte. Wurde die *Webseite* ohne Bezug zur Ursprungswebseite geöffnet, waren lediglich pornografische Inhalte feststellbar. Die Überprüfung der nahezu 1.000 miteinander verbundenen *Webseiten* ergab 37 eindeutige Webseiten mit kinder-, jugend-, tier- oder pornografischen Inhalten, die ohne Altersverifikation zugänglich waren (strafbar nach § 184 StGB).

ERMITTLUNGSGRUPPE „CHAT"

In einem Ermittlungsverfahren der Polizeidirektion Heidenheim wurde von Juli bis November 2012 gegen einen Beschuldigten ermittelt, der mit zwei weiteren Beschuldigten im Internet plante, seine ehemalige Lebensgefährtin, deren sieben Jahre alte Tochter und eine Nachbarin in seine Gewalt zu bringen. Die weitere Planung der Tat sah die gemeinsame Vergewaltigung, Tötung und Beseitigung der Leichname vor. Gegen die Beschuldigten wurden Haftbefehle wegen Verdachts der Verabredung zu gemeinschaftlichem Mord und Vergewaltigung sowie des schweren sexuellen Missbrauchs eines Kindes erlassen. Allen drei Beschuldigten konnten der Besitz und zum Teil auch das Verbreiten von zahlreichen kinder- und jugendpornografischen Schriften nachgewiesen werden. Im Dezember 2012 wurde der Haupttäter zu einer Freiheitsstrafe von drei Jahren und vier Monaten verurteilt.
Die beiden Mittäter wurden jeweils zu Bewährungsstrafen von sieben bzw. acht Monaten verurteilt.
Aus dem Ermittlungsverfahren resultierten durch die Auswertung der digitalen Beweismittel zwölf Folgeverfahren (wegen Verbrechensverabredungen, schwerem sexuellen Missbrauch eines Kindes sowie Besitz und Verbreitung kinderpornografischer Schriften u. a).

SEXUELLER MISSBRAUCH VON KINDERN ÜBER CHATFORUM

Im Juni 2012 ging bei der Kriminalaußenstelle Albstadt der Polizeidirektion Balingen ein Hinweis auf eine pädophile Person in einem *Chatforum* ein. Im Zuge der Ermittlungen konnte der geständige Beschuldigte, der zumindest im Zeitraum von Juni bis November 2012 über verschiedene E-Mail-Accounts hunderttausende kinderpornografische Bild- und Videodateien bezogen und teilweise auch verbreitet hatte, festgestellt werden. Er verwendete in mehreren *Chats und Newsgroups* zahlreiche Falsch- und Nicknamen. Der Beschuldigte war geständig und übergab der Polizei mehrere Datenträger, auf denen einige hunderttausend kinderpornografische Bild- und Video-dateien gespeichert sind.

LÖSCHUNG VON INTERNETSEITEN MIT KINDERPORNOGRAFISCHEM INHALT

Durch die nationale und internationale Zusammenarbeit innerhalb der Polizei konnte das Entfernen von kinderpornografischen Internetseiten intensiviert und dadurch die Onlineverfügbarkeit der zu beanstandenden Inhalte verringert werden. Kooperationen und Sondervereinbarungen mit Dienste-anbietern bzw. Providern trugen maßgeblich dazu bei, Angebote mit entsprechenden Inhalten weiter zu reduzieren. Die Dauer der Umsetzung bei Inhalten auf deutschen Servern beträgt mittlerweile etwa einen Tag. Das BKA ist zuständig für die Überwachung des Löschens von ausländischen Internetseiten mit kinderpornografischen Inhalten. Laut einer Statistik des BKA wurden im Jahre 2011 insgesamt 3.828 *Webseiten* weltweit gelöscht. Im Jahr 2012 stieg die Zahl auf weltweit 5.467 gelöschte *Webseiten*.

ABLAGE KINDERPORNOGRAFISCHER SCHRIFTEN BEI FILEHOSTERN UND VERBREITUNG ÜBER TAUSCHBÖRSEN

Der Trend des Vorjahres, kinder- oder jugendpornografische Inhalte bei *Filehostern* sowie in dezentralen Netzwerken zu speichern, setzte sich im Jahr 2012 fort. Dabei stieg weiterhin die Nutzung einer bestimmten Tauschbörse, die schon im Vorjahr hinsichtlich der Verbreitung kinderpornografischer Dateien innerhalb geschlossener Benutzerkreise im Fokus stand.

CYBERGROOMING

Neben den im sozialen Nahraum begangenen Sexualdelikten an Kindern und Jugendlichen kommt es auch immer wieder nach Kontaktanbahnungen über das Internet zu sexuellen Übergriffen.
Für das gezielte Ansprechen von Kindern und Jugendlichen im Internet mit der Zielrichtung der Anbahnung von sexuellen Kontakten hat sich zwischenzeitlich der Begriff „Cybergrooming" etabliert. Viele pädosexuelle Täter halten sich vorwiegend in *Chats* auf, die für Kinder und Jugendliche konzipiert sind. Durch gefälschte Profile wird den Kindern und Jugendlichen ein gleichaltriger Gesprächspartner vorgetäuscht. Durch eine geschickte Gesprächsführung wird dann auf die sexuell meist unerfahrenen *Chatter* so eingewirkt, dass bspw. Kinder im *Chat* aufgefordert werden, sexuelle Handlungen an sich vorzunehmen. Auch nehmen die Täter sexuelle Handlungen an sich selbst vor, die Kindern dann per Webcam oder durch die Übermittlungen von Lichtbildern zugänglich gemacht werden. Im Rahmen einer repräsentativen Umfrage unter Minderjährigen unter 14 Jahren wurde bereits im Jahr 2007 festgestellt, dass annähernd 38 % aller Befragten zu ungewollter Kommunikation mit sexuellem Inhalt im Internet gedrängt wurden. 25 % wurden zur Beschreibung von sexuellen Handlungen aufgefordert und an fast 10 % wurde pornografisches Material gesandt[7].
Die Straftäter verwirklichen zumeist den Straftatbestand des § 176 Abs. 4 StGB in den Varianten Nr. 3 und Nr. 4. Die Straftaten des Cybergroomings werden unter dem PKS-Straftatenschlüssel 13140000 in der Statistik (Tabelle Internetkriminalität) ausgewiesen, weshalb die Polizei über verlässliche Daten zum Hellfeld verfügt. Im Jahr 2012 wurden 80 Fälle erfasst, 17 Fälle mehr als im Vorjahr.

[7] *Dr. Catarina Katzer zitiert in: „Deutsche Polizei", Ausgabe 02-2012, „Cybergrooming in virtuellen Welten – Chancen für Sexualtäter."*

Vor fünf Jahren waren es noch zwölf Fälle. Die Aufklärungsquote liegt bei 92,5 %. Von einem hohen Dunkelfeld muss ausgegangen werden.

OPERATION „DONAU"

Umfangreiche Erkenntnisse und Erfahrungen im Deliktsbereich „Cybergrooming" konnten im Jahr 2012 durch die OP „Donau" erlangt werden. Die Polizeidirektion (PD) Tuttlingen führte im Januar 2012 elf Tage lang Initiativermittlungen im Internet wegen Verdachts des sexuellen Missbrauchs von Kindern in einem *Chat-Portal* durch. Hinsichtlich organisatorischer und technischer Fragestellungen erfolgte im Vorfeld die Unterstützung durch den Arbeitsbereich Internetrecherche (AIR) und die ASt Kipo des LKA BW. Innerhalb der elf Tage konnten insgesamt 19 Ermittlungsverfahren wegen Verdachts des sexuellen Missbrauchs von Kindern eingeleitet werden. Von den ermittelten Beschuldigten waren bereits drei als Sexualstraftäter in Erscheinung getreten. In 92 Fällen blieb es bei sexuellen Anbahnungsgesprächen im Versuchsstadium. Durch die OP „Donau" bestätigte sich das vermutete hohe Dunkelfeld in diesem Deliktsbereich für das ausgewählte *Chat-Portal*, das sich nach kriminalistischer Erfahrung auch auf andere *Chatforen*, *Newsgroups* oder *Social Media-Dienste* erstreckt.

Anlagen | 5

ARBEITSBEREICH INTERNETRECHERCHE

Der im Jahr 2005 eingerichtete AIR des LKA BW hat die Aufgabe der brennpunktorientierten, nicht extern initiierten Suche nach Inhalten im Internet zum Zwecke der Gefahrenabwehr sowie der Weiterverfolgung von festgestellten strafrechtlich relevanten Sachverhalten. Ebenso fallen Maßnahmen der Beweissicherung bis zur Feststellung der Verantwortlichen und der örtlichen Zuständigkeiten von Polizei und Justiz in den Zuständigkeitsbereich des AIR. Der AIR führte bisher OP in den Deliktsbereichen Gewaltverherrlichung, Volksverhetzung und Kinderpornografie durch, wobei der Schwerpunkt bei der Bekämpfung der Verbreitung von Kinderpornografie liegt.
Im Rahmen der OP „Infans" wegen Verdachts der Verbreitung von Kinderpornografie in einem Filesharing-Netzwerk wurden durch den AIR im Zeitraum vom 29. Oktober bis 3. Dezember 2012 weltweit 676 Strafverfahren initiiert, davon 40 in Deutschland. Durch den Rücklauf der damit verbundenen Erkenntnisanfragen wurde festgestellt, dass zwei Anschlussinhaber bereits Vorstrafen im Bereich der schweren sexuellen Missbrauchshandlungen zum Nachteil von Kindern aufwiesen. Gegen einen der Anschlussinhaber war in der Vergangenheit bereits wegen Vergewaltigung, gegen einige andere wegen Verdachts der Verbreitung von Kinderpornografie ermittelt worden.
Im Rahmen der Durchsuchungsmaßnahmen eines durch die OP „Infans" initiierten Ermittlungsverfahrens in Baden-Württemberg konnten bei einem als Heilerziehungspfleger arbeitenden TV eine große Anzahl kinderpornografischer Dateien aufgefunden werden. Hierunter befanden sich Bilddateien mit Missbrauchshandlungen an Kleinkindern und Säuglingen.

Immer wieder wird durch Mitteilungen von Polizeidienststellen im In- und Ausland deutlich, dass durch derartige OP des AIR nicht nur Straftaten in Form der Verbreitung kinderpornografischer

Schriften unterbunden und verfolgt werden können. Vielmehr werden auch noch andauernde Missbrauchshandlungen auf diesem Weg bekannt und durch die einschreitenden Beamten beendet.

Aufgrund der fehlenden gesetzlichen Verpflichtung zur Vorratsdatenspeicherung konnten in vier Fällen trotz unverzüglicher Anfrage beim *Provider* die Anschlussinhaber nicht ermittelt werden. In einem weiteren Fall lag eine statische *IP-Adresse* vor, zu der vom zuständigen Provider keine Beauskunftung des Bestandsdateninhabers erfolgte. Durch Internetrecherchen des AIR wurde festgestellt, dass es sich hierbei um den Anschluss einer Firma handelte. Eine Kontaktaufnahme mit Verantwortlichen der Firma führte nicht zur Identifikation des TV. Jedoch überarbeitete die Firma daraufhin das Sicherheitskonzept für ihren Internetzugang und schloss eine Sicherheitslücke, auf die der AIR aufmerksam machen konnte.

VORRATSDATENSPEICHERUNG

Mit dem Urteil des Bundesverfassungsgerichtes (BVerfG) vom 2. März 2010 wurde die bestehende rechtliche Ausgestaltung der sogenannten Vorratsdatenspeicherung (§§ 113a und 113b Telekommunikationsgesetz (TKG) sowie § 100g Abs. 1 Satz 1 Strafprozessordnung (StPO), soweit danach Verkehrsdaten gemäß 113a TKG erhoben werden dürfen) für nichtig erklärt. Eine verfassungskonforme Neuregelung durch den Gesetzgeber hat das BVerfG jedoch nicht ausgeschlossen.
Durch die bestehende gesetzliche Lücke ist nur noch der Zugriff auf Verkehrsdaten möglich, die von den Verpflichteten im eigenen Interesse (Rechnungsstellung und/oder Dokumentation) gespeichert und noch nicht anonymisiert wurden. Aufgrund der Freiwilligkeit obliegt die Dauer der Speicherung der Verkehrsdaten dem Ermessen der Verpflichteten. Aus diesem Grund unterscheiden sich der Umfang der gespeicherten Daten und die Dauer der Speicherung zwischen den Verpflichteten zum Teil erheblich. Das Urteil wirkt sich sowohl auf die repressiven als auch auf die präventiven Aufgabenfelder eindeutig negativ aus.
Die Deutschland von der Europäischen Union (EU) gesetzten Fristen zur Umsetzung der Richtlinie 2006/24/EG vom 15. März 2006 (Amtsblatt der EU vom 13. April 2006) „über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden“ sind abgelaufen. Mit Pressemitteilung vom 31. Mai 2012 teilte die EU-Kommission mit, dass sie an diesem Tag Klage vor dem Europäischen Gerichtshof gegen Deutschland erhoben und als Strafe ein tägliches Zwangsgeld in Höhe von ca. 315.000 Euro vorgeschlagen habe[8].

Die Wiedereinführung einer verfassungsmäßigen Regelung der Vorratsdatenspeicherung unter Einhaltung der durch das BVerfG aufgestellten Voraussetzung ist zwingend erforderlich. Die Not-wendigkeit der Vorratsdatenspeicherung zur Bekämpfung von schweren Straftaten zeigen auch die Ermittlungsergebnisse des AIR und der ASt Kipo bei der Durchführung von OP. In allen Fällen

[8] *http://europa.eu/rapid/press-release_IP-12-530_de.htm?locale=en*

des Besitzes oder der Verbreitung von Kinderpornografie werden durch den AIR unverzüglich, d. h. nach Bekanntwerden der Informationen, Bestandsdatenanfragen durchgeführt. Im Rahmen der OP „Infans“ wurden 10 % der Fälle nicht beauskunftet, bei denen die tatverdächtigen Anschlussinhaber zum Anfragezeitpunkt sogar noch „online“ waren.
Aufgrund der fehlenden gesetzlichen Verpflichtung zur Speicherung der Verbindungsdaten durch die Provider ist festzustellen, dass in 53,2 % aller Fälle von Recherchen der ASt KiPo im Rahmen der OP „First“ die Feststellung des Anschlussinhabers und weitere folgende Ermittlungen nicht mehr möglich waren. Somit konnte hier jeder zweite Anschlussinhaber in Deutschland, dessen Anschluss wegen des Besitzes oder der Verbreitung von Kinderpornografie ermittelt wurde, aufgrund der fehlenden Vorratsdatenspeicherung nicht identifiziert und ermittelt werden.
Erschwerend kommt hinzu, dass zwischen dem Zeitpunkt der Tat und der Kenntniserlangung durch die Polizei zum Teil ein erheblicher zeitlicher Verzug besteht.

SOZIALE NETZWERKE – FACEBOOK-PARTYS

Zu Beginn des Sommers 2012 musste die Polizei Baden-Württemberg zahlreiche Einsatzlagen bewältigen, die aus Verabredungen von Bürgern zu öffentlichen Veranstaltungen in *Sozialen Netzwerken* (z. B. zu sogenannten „Project-X-Partys“) resultierten. Diese waren durch die Anonymität der Anmelder und die nicht bestimmbare Anzahl von Teilnehmern sowie eine oftmals kurze Vorlaufzeit für die Einsatzvorbereitungen und die Überbetonung des Eventcharakters geprägt. Neben zahlreichen Beratungsleistungen für Landesdienststellen war der AIR in die Einsätze der PD Waiblingen und der PD Ulm eingebunden und erhob einsatzrelevante Informationen, die über die entsprechenden Facebook-Veranstaltungsseiten veröffentlicht wurden. Die frühzeitige und dauerhafte Aufklärung sowie die beweiskräftige Sicherung von relevanten Online-Inhalten durch die Mitarbeiter des AIR und die Sachbearbeiter Cyberkriminalität der örtlichen Dienststellen waren dabei wichtige Komponenten, um die Verantwortlichen zu identifizieren.
Auffällig an diesem Phänomen ist, dass sich die Zahl der Zusagen für die sogenannten Project-X-Partys je Veranstaltung im drei- bis vierstelligen, die der Einladungen im bis zu fünfstelligen Bereich bewegte und diese bis zum Beginn der Veranstaltung kontinuierlich weiter anstieg. Als mögliche Ursache für die hohe Anzahl der Teilnehmer konnte ermittelt werden, dass auf einschlägigen Facebookseiten eine Anleitung veröffentlicht worden war, die erklärte, wie mittels einfacher Einstellungen der Nutzer eines Facebook-Accounts seinen gesamten eigenen Facebook-Freundeskreis automatisiert einladen kann. Diese Einladungen konnten sich dann im Schneeballsystem verbreiten, da eine dreistellige Anzahl von Facebookfreunden bei vielen Nutzern durchaus üblich ist.

Anlagen | 6-12

COMPUTERKRIMINALITÄT (CYBERKRIMINALITÄT IM ENGEREN SINNE)

Die in der PKS registrierten Fälle der Computerkriminalität erreichen im Jahr 2012 annähernd den Wert des Vorjahres. Statistisch ist ein leichter Rückgang um 1,6 % auf 8.907 Fälle (9.048 Fälle) zu verzeichnen. Ursächlich hierfür ist die Anzahl der Delikte des Computerbetrugs (§ 263a StGB), die um 12,8 % auf 3.658 Fälle (4.194 Fälle) gesunken sind. Mit Ausnahme des Tatbestandes des Computerbetrugs ist bei allen Delikten eine geringe Zunahme zu verzeichnen. Der Tatbestand des Ausspähens von Daten (§ 202a StGB) ist nahezu unverändert geblieben. Im Jahr 2012 sind mit 1.346 erfassten Fällen drei mehr als im Vorjahr (1.343) zu verzeichnen, was einer Zunahme um 0,2 % entspricht.

Die rückläufige Entwicklung der Fallzahlen des Computerbetrugs ist zum einen auf einige Großverfahren bei Dienststellen aus dem Jahr 2011 zurückzuführen. Zum anderen wurden auch generell weniger Strafverfahren im Deliktsbereich Phishing bearbeitet. Teilweise kann diese Entwicklung den im Jahr 2012 von weiteren Kreditinstituten eingeführten modernen Sicherheitsstandards wie dem mTAN- oder auch ChipTAN-Verfahren zugeschrieben werden. Durch diese Sicherheitsvorkehrungen der Banken für ihre Kunden dürfte die Verwertung der erlangten Daten zusätzlich erschwert worden sein.

Daneben ist festzustellen, dass die Dienststellen der Landespolizei verstärkt auf eine den PKS-Richtlinien entsprechende Erfassung achten. Dieses Verhalten führte dazu, dass weniger Fehlerfassungen beispielsweise von Auslandsstraftaten ihren Eingang in die PKS fanden als im Vorjahr. Darüber hinaus sind die bearbeiteten Straftaten im Zuge ihrer Erfassung besser auf zutreffende Spezialnormen hin geprüft und daher weniger Delikte ausschließlich auf den Computerbetrug als Führungsdelikt reduziert worden. Diese Entwicklung dürfte bei einigen Dienststellen mit der dort veränderten Organisationsstruktur in Zusammenhang stehen. Teilweise wurde die Sachbearbeitung von Delikten der Computerkriminalität auf spezialisierte Organisationseinheiten für den Bereich Cyberkriminalität verlagert.

Der registrierte Schaden ist deutlich um 39,0 % von 9.575.267 Euro auf 5.843.142 Euro gesunken. Die größte Veränderung der Schadenshöhe ist für den Tatbestand des Computerbetrugs mit einem Rückgang um 54,5 % von 7.509.910 Euro auf 3.414.341 Euro zu verzeichnen. Die Entwicklung der Schadenshöhe ist zu einem großen Teil auf ein von der Landespolizeidirektion Karlsruhe im Jahre 2011 abgeschlossenes Ermittlungsverfahren mit Führungsdelikt Computerbetrug und einem Schaden von 2.500.000 Euro zurückzuführen, welches in die Statistik desselben Jahres mit einfloss. Grundlage dieses Verfahrens war ein Fall, in dem Kundendaten eines großen Internetproviders ausgespäht und für das Einrichten von VoIP-Rufnummern in bereits angelegten Kundenaccounts verwendet worden waren. Über diese wurden anschließend kostenpflichtige Mehrwertdienste angerufen, die entsprechende Kosten generierten. Darüber hinaus hatten im Jahr 2011 mehrere Dienststellen Verfahren mit hohen Schadenssummen zu bearbeiten, welche die Gesamtsumme für das betreffende Jahr in die Höhe steigen ließ und die hohe Differenz zum Berichtsjahr erklären.

ANALYSEDARSTELLUNG

ARBEITSBEREICH ERMITTLUNGEN CYBERKRIMINALITÄT

Die Erfahrungen aus den im Jahr 2012 beim LKA BW bearbeiteten Ermittlungsverfahren zeigen, dass die Cyberkriminellen ihre Techniken zur Verschleierung ihrer Identität zunehmend weiterentwickeln. Fast sämtliche bei der Abteilung „Cyberkriminalität/Digitale Spuren" des LKA BW bearbeiteten Ermittlungsverfahren ließen Bezüge ins Ausland erkennen. Die deshalb erforderlichen, zum Teil langwierigen Rechtshilfeersuchen erschwerten die polizeilichen Ermittlungen zusätzlich. Im Rahmen der internationalen Rechtshilfe mit in- und ausländischen Strafverfolgungsbehörden war es jedoch in Kooperation mit Internet-Service-Providern in einem Ermittlungsverfahren möglich, mehrere Domains zu beschlagnahmen. Diese standen im Zusammenhang mit einem *Botnetz*, das von den Tätern für *DDoS-Angriffe* auf mehrere hundert *Webseiten* im In- und Ausland verwendet wurde. Durch die Beschlagnahme wurde den Tätern der Zugriff auf ihre für die Begehung der Straftaten eingesetzte IT-Infrastruktur entzogen. Dadurch konnten weitere Angriffe verhindert werden.

ERMITTLUNGSVERFAHREN „KNOCKDOWN"

Im März 2012 wurde das LKA BW über das BKA von US-amerikanischen Strafverfolgungsbehörden um Vollstreckung eines Internationalen Fahndungsersuchens zur Festnahme eines serbischen Staatsangehörigen und der Durchführung entsprechender Durchsuchungsmaßnahmen ersucht.
Der Tatverdächtige, gegen den amerikanische Behörden wegen Straftaten aus dem Bereich der Cyberkriminalität seit mehreren Jahren ermittelt hatten und der seit geraumer Zeit auf der Fahndungsliste von Interpol stand, hatte sich zu dieser Zeit bei seiner Ehefrau in einer Stadt im nördlichen Teil von Baden-Württemberg illegal aufgehalten und plante seine unmittelbar bevorstehende Ausreise ins Ausland. Nach Erkenntnissen der amerikanischen Behörden war der 24-jährige Tatverdächtige ein herausragendes Mitglied eines internationalen *Online-Forums*, in dem vor allem mit gestohlenen Kreditkartendaten gehandelt wurde. Gegen den Betreiber und weitere Mitglieder wurde seit dem Jahr 2004 wegen Ausspähens von Daten, Computerbetrugs und anderer Delikte ermittelt. Den Mitgliedern des Forums werden mehr als 1,5 Millionen gestohlene Kreditkartensätze und ein durch missbräuchliche Verwendung eingetretener Gesamtschaden von mehr als vier Millionen US Dollar zugerechnet. Die Aufenthaltsfeststellung und Identifizierung sowie die Festnahme des Hackers innerhalb weniger Tage erfolgte aufgrund seiner illegalen Internetaktivitäten, die er auch von seinem Aufenthaltsort in Baden-Württemberg durchführte. Die parallel zur Festnahme durchgeführten *Live-Forensic-Maßnahmen* der IT-Beweissicherung des LKA BW führten zur Sicherstellung beweiserheblicher digitaler Spuren. Nach Abschluss des Auslieferungsverfahrens erfolgte im Dezember 2012 die Überstellung an die US-amerikanischen Behörden.

ERPRESSUNGEN IM ZUSAMMENHANG MIT VIDEO(CHAT)PLATTFORMEN

Mit Stand 11. Januar 2013 wurden seit Dezember 2012 in Baden-Württemberg sieben Strafanzeigen zu Sachverhalten bekannt, die sich zu einem neuen Internetphänomen entwickeln könnten.
Auf einer Videoplattform wird der erste Kontakt zwischen Opfer und Täter(in) hergestellt. Über *Chat* und Webcam erfolgt ein sog. Anbahnungsgespräch, in deren Verlauf sich eine weibliche

Person entkleidet und das Opfer dazu überredet, Kontaktdaten aus anderen Internetdiensten wie beispielsweise *Sozialen Netzwerken* auszutauschen. Entweder auf der Ursprungsplattform bzw. in einem anderen *Sozialen Netzwerk* oder auf einem *Messenger* wird das Opfer aufgefordert, sich ebenfalls vor der Webcam zu entkleiden und sexuelle Handlungen an sich vorzunehmen. Diese Opferhandlung wird vom Täter aufgezeichnet.
Unmittelbar danach erhält das Opfer eine erpresserische Nachricht des Täters, in welcher es zur Zahlung mehreren hundert Euro über Western Union aufgefordert wird. Ferner wird dem Opfer ein Link auf eine öffentliche Videoplattform übermittelt, unter welchem der Videomitschnitt seiner sexuellen Handlung kurzfristig aufrufbar ist. Ergänzend dazu werden die über Internetdienste bekannt gewordenen Freundeskontakte des Opfers übermittelt. Die Täter drohen damit im Fall des Nichtzahlens an diese Freunde die öffentliche Erreichbarkeit des Videomitschnittes zu übermitteln.

RANSOMWARE – EINE VARIANTE DER DIGITALEN SCHUTZGELDERPRESSUNG

Im Vergleich zum Vorjahr ist weiterhin ein hohes Fallzahlenaufkommen festzustellen. Die INPOL Fall-Anwendung IuK, in der alle Straftaten des Sondermeldedienstes (SMD) Cybercrime erfasst werden, enthält für Baden-Württemberg im Jahr 2012 insgesamt 3.153 Fälle (2.994 Fälle) der Erpressung. Die mit der Bezeichnung *„Ransomware"* erfassten Delikte haben daran einen Anteil von 3.038 Fällen (2.799 Fälle). Dies entspricht einer Steigerung um 8,5 % der Straftaten, die mit diesem Modus Operandi begangen wurden.
Das Jahr 2012 war geprägt von vielen verschiedenen Varianten der ursprünglich verbreiteten Version mit angeblichem Bezug zur Bundespolizei bzw. dem BKA. Die Ergebnisse bundesweiter Ermittlungen ergaben, dass sich offenbar unterschiedliche Tätergruppierungen des seit Ende des Jahres 2011 in diversen Internetforen verfügbaren Quellcodes der *Schadsoftware* bedienen. Die im Jahr 2012 verbreiteten Arten haben alle gemeinsam, dass dem Geschädigten eine behördliche Mitteilung suggeriert wird. Diese ist als *Pop-Up-Fenster* eingeblendet und unterbindet mit ihrem Erscheinen den weiteren Zugriff auf die Benutzeroberfläche des infizierten Systems. Durch die angezeigten behördlichen Symbole der angeblichen Absender soll die Ernsthaftigkeit der Nachricht untermauert werden.
Je nach Variante wird zur Verstärkung dieses Eindrucks auch das Übertragungsbild einer Webcam eingeblendet. Dort ist der Geschädigte, sofern er die Webcam aktiviert hat, in einem Fenster sichtbar. Eine weitere, wenn auch nur selten verbreitete Version mit in schlechtem Deutsch zu hörender Sprachausgabe sollte der Einschüchterung der Nutzer dienen. Im Text der Meldung wird dem Nutzer häufig das Aufrufen von pornografischen, kinderpornografischen und gewaltverherrlichenden Inhalten vorgeworfen. Bei den im Jahr 2012 stark verbreiteten Varianten mit GEMA-, GVU- oder BSI-Logo wird der Geschädigte des Verstoßes gegen die Schutzrechte der jeweiligen Gesellschaft durch illegales Herunterladen von Medien bezichtigt.
Seit Dezember 2012 kursiert eine Variante, die in der Mitteilung die Fotografie einer jungen weiblichen Person beinhaltet, bei welcher es sich nach Einschätzung des BKA um eine strafbewehrte jugendpornografische Darstellung handelt. Im Text der Bildschirmmitteilung wird dazu behauptet, dass die Wiedergabe von pornografischen Inhalten mit Minderjährigen auf dem Rechner des Nutzers

festgestellt worden sei. In einer gemeinsamen Pressemitteilung des BKA und des BSI wurde deshalb auf diese *Schadsoftwarevariante* hingewiesen und vorsorglich mitgeteilt, dass die Sicherung der in der *Ransomware* enthaltenen jugendpornografischen Darstellung auch ein strafbares Verschaffen bzw. einen Besitz von Jugendpornografie darstellen könnte. Weitere Hinweise und einen Auszug aus der Pressemitteilung siehe unter Ziff. 2/Maßnahmen/Ransomware.

NEUES PHÄNOMEN: ANRUFE ANGEBLICHER MICROSOFT-MITARBEITER

Im Laufe des Jahres 2012 kam es bundesweit immer wieder zu Fällen von Anrufen eines angeblichen Mitarbeiters der Fa. Microsoft. Baden-Württemberg ist bislang mit vereinzelten Fällen betroffen. Eine Auswertung im Lagebildinformationssystem Land ergibt für das Jahr 2012 in Baden-Württemberg fünf Fälle. Es ist jedoch damit zu rechnen, dass dieser Modus Operandi weiterhin genutzt wird. Bis zum 6. Februar 2013 wurden in Baden-Württemberg bereits fünf Fälle erfasst bzw. bearbeitet. Die Anrufe erfolgten in der Regel mit unterdrückter Rufnummer auf den Festnetzanschluss des Geschädigten. In englischer Sprache teilt der Anrufer mit, dass es angeblich ein Problem mit dem Rechner des angerufenen Geschädigten gebe und man nun versuchen wolle, dies gemeinsam zu beheben. Anschließend werden die Geschädigten telefonisch dazu aufgefordert, an ihrem Rechner eine Verbindung zum Internet aufzubauen und dann weitere Schritte gemäß genauer telefonischer Weisung durch den unbekannten Anrufer vorzunehmen. Damit gelingt es dem Täter, mittels der im Betriebssystem vorhandenen Fernwartungsfunktion, der sogenannten „Remote-Desktop-Verbindung", Zugriff auf den Rechner des Geschädigten zu erlangen. Teilweise versuchen die Täter, über das Internet weitere Schad- oder Fernwartungssoftware auf dem Rechner des Angerufenen zu installieren. Schließlich wird vom Täter behauptet, dass auf dem Rechner des Geschädigten angeblich eine Lizenz abgelaufen sei und dieser nun für einen gewissen Betrag eine neue erwerben müsse. Teilweise wurden die Opfer aber auch zum Abschluss eines kostenpflichtigen Wartungsvertrages oder zum Herunterladen einer vermeintlichen „Sicherheitssoftware" aufgefordert. Sollte der Geschädigte dem nicht zustimmen, würde der Rechner entweder gesperrt werden oder aber künftig nicht mehr ordnungsgemäß funktionieren. Der Angerufene solle deshalb entweder seine Kreditkartendaten angeben oder aber eine Bargeldüberweisung mittels Western Union tätigen. Alle Varianten dieser Methode zielen letztlich darauf ab, unbeschränkten Zugriff auf den Rechner des Geschädigten zu erlangen. Gibt der Angerufene darüber hinaus seine Kreditkartendaten an, besteht die Gefahr, dass diese im Nachhinein der mehrfachen missbräuchlichen Verwendung dienen. Alle bisherigen Geschädigten geben an, dass der unbekannte Anrufer während des gesamten Telefonats nur Englisch gesprochen habe, teilweise mit asiatischem Akzent. Im Hintergrund seien Geräusche ähnlich einem Callcenter zu hören gewesen. Die Telefonnummern der Geschädigten dürften die Täter vermutlich dem öffentlichen Telefonbuch entnommen haben. In den bislang bekannten Fällen hat sich aufgrund weiterer Ermitt-

lungen gezeigt, dass diese Anrufe offensichtlich aus dem Ausland kamen. Aufgrund der Verschiedenartigkeit der vermeintlichen Herkunftsländer ist aber von einer Verschleierung über das Internet auszugehen. Laut Internetrecherchen und dem nationalen Informationsaustausch trat das Phänomen in dieser Art erstmals bereits im September 2011 in der Schweiz auf. Darüber hinaus existieren einige aktuelle Warnmeldungen gängiger Online-Magazine.

DIGITALE FORENSIK

Anlagen | 13

IT-BEWEISSICHERUNG

Innerhalb der Polizei Baden-Württemberg wird die Sicherung und Untersuchung digitaler Spuren durch die Arbeitsbereiche IT-Beweissicherung (ITB) wahrgenommen.
Diese seit dem Jahr 2001 landesweit in jedem Polizeipräsidium bzw. jeder Polizeidirektion vorhandenen Spezialisten unterstützen die Kriminalitätsbekämpfung in allen Deliktsbereichen professionell durch die Sicherung von Daten und Untersuchung von Asservaten. In vielen Fällen bildet diese Arbeit das Fundament für die spätere Beweisführung vor Gericht.
Die Sicherung und Untersuchung digitaler Spuren wird durch die ständig voranschreitende Vernetzung und digitale Durchdringung unserer Alltagswelt immer wichtiger und ist in vielen Fällen die einzige Möglichkeit, um Straftaten aufzuklären.

AUFTRAGSAUFKOMMEN ITB

Das landesweite Auftragsaufkommen wird seit dem Jahr 2006 statistisch erfasst. Im Jahr 2006 wurden insgesamt 7.324 Aufträge registriert. In den folgenden Jahren kam es zu einem kontinuierlichen Anstieg. Im Jahr 2010 wurden erstmals über 10.000 Aufträge (10.149) erfasst. Ein Rückgang ist derzeit nicht erkennbar. Im Jahr 2012 wurden 10.732 neue Aufträge registriert, 14 Aufträge mehr als im Vorjahr.

MOBILE GERÄTE

Laut einer repräsentativen Umfrage des Branchenverbands BITKOM im Jahr 2012 gibt es rund 115 Millionen Mobilfunkverträge in Deutschland. Das entspricht fast 1,4 Verträgen (und etwa so vielen Geräten) pro Einwohner[9]. Hinzu kommen mobile *Tablets* sowie Net- und Laptops, die Kommunikation, Datenübermittlung und Internetsurfen fast überall ermöglichen. Diese Vorgänge generieren digitale Daten und damit digitale Spuren. Durch die flächendeckende Verfügbarkeit des Internets unabhängig vom Standort (Internet-Cafés, Hotels, Fahrzeuge etc.) und der genutzten technischen Einrichtung (PC, Notebook, Mobiltelefon, *Smartphone* etc.) wird im Falle der Begehung von Straftaten die Anzahl potentieller digitaler Spuren immer größer. Damit einhergehend wird auch die Spurenlage bzw. der polizeiliche Zugriff auf diese Tat- bzw. Täterspuren zunehmend komplexer und unübersichtlicher.

[9] *http://www.bitkom.org/de/markt_statistik/64046_72960.aspx, aufgerufen am 11. Februar 2013*

ANALYSEDARSTELLUNG

Neben der Kommunikations- und Unterhaltungselektronik werden Rechnersysteme zunehmend in anderen Geräten verbaut. So finden sich elektronische Systeme in Kraftfahrzeugen und Haushaltsgeräten wie Waschmaschinen oder Kühlschränken. Diese Geräte zeichnen meist für den Benutzer unsichtbar Daten auf und können beweiserhebliche digitale Spuren enthalten, die eine professionelle und verfahrenssichere Auswertung und Analyse durch Spezialisten erforderlich machen.

STEIGENDE DATENMENGEN

Einhergehend mit der Verbreitung von Geräten steigen die Datenspeicher und Datenmengen kontinuierlich an. Ein Desktoprechner verfügt heute über Festplatten in der Größenordnung von 500 *Gigabyte* bis zwei *Terabyte*. Ein *Gigabyte* ermöglicht das Speichern von etwa 250.000 DIN A4-Seiten. Eine Standardfestplatte mit einem *Terabyte* Speicher (etwa 1.000 *Gigabyte*) kann rund 200.000 qualitativ gute Bilder (à 5 *Megabyte*) speichern. Vor zehn oder 20 Jahren stand dem Nutzer nur ein Bruchteil dieser gigantischen Speicherkapazitäten zur Verfügung. Hinzu kommen Angebote für Online-Speicher, die dem Nutzer kostenlos mehrere Gigabyte *Cloudspeicher* zur Verfügung stellen. Die hohen Datenmengen bedingen höhere Rechnerleistung bei der Auswertung und Verarbeitung der Daten, steigende Bearbeitungszeiten und enormen Speicherbedarf bei der polizeilichen Beweissicherung.

VERSCHLÜSSELUNG

Der technische Wandel und die damit einhergehende einfache, teilweise standardisierte Verwendung von Verschlüsselungsmethoden bereiten der Polizei in zunehmenden Maße Schwierigkeiten bei der Aufklärung von Straftaten. In vielen Fällen werden bereits heute Softwareprodukte verwendet, die über eine automatische Verschlüsselung und/oder Anonymisierung verfügen. Insoweit folgen auch Straftäter der allgemeinen technischen Entwicklung und nutzen gezielt die spezifischen Vorteile, die sich dabei insbesondere für ihre Tatplanungen und -ausführungen ergeben. Kinderpornografisches Material, Lagepläne, Bombenbauanleitungen oder ideologisches Propagandamaterial werden verschlüsselt und weiterverbreitet bzw. anderen Tätern zur Verfügung gestellt.

ANALYSE STRUKTURIERTER MASSENDATEN / ARBEITSBEREICH STRUKTURIERTE MASSENDATEN

Mit Einrichtung der Abteilung „Cyberkriminalität/Digitale Spuren“ im LKA BW und der damit einhergehenden Einrichtung eines Arbeitsbereichs „Massendaten“ in der Inspektion 720 wurde der stetig wachsenden Bedeutung der spezifischen Tätigkeit der Analyse strukturierter Massendaten Rechnung getragen. Die mit der Polizeireform geplante flächendeckende Einrichtung von Sachbearbeitern für Datenanalyse in der K5 der künftigen Regionalpräsidien führt diese Entwicklung fort.
Nach Feststellung der unter Leitung des LKA BW arbeitenden Projektgruppe „Analyse und Auswertung strukturierter Massendaten“ ist die Datenanalyse keine Teildisziplin der Operativen Auswertung, sondern stellt die polizeiliche Verarbeitung eines eigenständigen, speziellen Beweisthemas dar, deren Ergebnis neben anderen Beweisthemen in den analytischen Prozess innerhalb eines Ermittlungsverfahrens oder einer Operativen Auswertung einfließt.
Bislang konzentrierten sich Analyse und Auswertung dieser speziellen digitalen Spurenart insbesondere auf Funkzellendaten. Sie sind jedoch nicht darauf beschränkt. Gemäß der Arbeitsdefinition der Projektgruppe sind strukturierte Massendaten „Daten oder Datensätze, die eine gleichartige Struktur aufweisen und deren Inhalte in einem Bedeutungskontext stehen, wobei deren Anzahl unerheblich ist“. Hieraus wird deutlich, dass der Schwerpunkt dieser Definition nicht auf die Anzahl der Datensätze abhebt, sondern vielmehr eine Konzentration auf den Analyseprozess vornimmt. Bei den zu analysierenden Daten müssen unterschiedliche Strukturen vergleichbar gemacht werden können, d. h. Feldbeschreibungen müssen vorhanden sein und herausgearbeitet werden.

KOMPETENZZENTRUM TELEKOMMUNIKATIONSÜBERWACHUNG

Der moderne Kommunikationsmarkt ist von rasanten Entwicklungen geprägt. Übertragungsgeschwindigkeiten, Bandbreiten und Datenmengen nehmen stark zu. Darüber hinaus zeichnet er sich aus durch zunehmende Verschlüsselung der Kommunikationsinhalte, technisch bedingte oder absichtlich erzeugte Anonymisierung von Teilnehmeranschlüssen, Internationalisierung und die Einführung neuer technischer Standards.
Herkömmliche Kommunikationsdienste und Internet verschmelzen miteinander und gehen mit einer steigenden Anzahl an Kommunikationsmöglichkeiten und vielfältigen Nutzungsmöglichkeiten einher. Die Nutzerzahlen von interaktiven Informations- und Kommunikationsplattformen und mobilen Endgeräten wachsen rasant. Begleitet wird dies durch immer kürzere Entwicklungszyklen mit umfassenden Neuerungen.
Diesen Herausforderungen mit unmittelbaren Auswirkungen auf die Telekommunikationsüberwachung (TKÜ) muss begegnet werden. Weitere Herausforderungen ergeben sich aus einer Zunahme an Beratungstätigkeit, Schulungen und Projektarbeiten.

Kernstück der technischen Plattform für die TKÜ ist die leistungsfähige TKÜ-Anlage des LKA BW. Die Administration wird durch den Systemanbieter zusammen mit vier Ingenieuren, einer Programmiererin und einem Techniker des LKA BW realisiert. Damit wird der Betrieb des Rechenzentrums, die Systemsoftware, die Umsetzung und Einhaltung der technischen Richtlinien, die Ausleitung und der Import der TKÜ-Daten sowie die Entwicklung von Datenbanken und Dekodiermodulen gewährleistet.

Dem Landtag Baden-Württemberg wird jährlich ein Bericht über Umfang und Erfolg von Telefonüberwachungsmaßnahmen 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

Beim TKÜ-Zentrum wird durch spezialisierte Polizeivollzugsbeamte eine TKÜ-Hotline betrieben, die 24 Stunden an sieben Tagen in der Woche über einen Bereitschaftsdienst erreichbar ist.
Die Mitarbeiter beraten in allen Fragen zur TKÜ in den Bereichen der Gefahrenabwehr und Strafverfolgung (§ 23a Polizeigesetz Baden-Württemberg (PolG BW) bzw. §§ 100a und 100g StPO) und sind zentraler Ansprechpartner für die Netzbetreiber. Die TKÜ-Hotline begleitet den Gesamtprozess der Telekommunikationsüberwachung von der Einrichtung, Verlängerung bis zur Löschung der jeweiligen Maßnahme. Die begleitende Beratung ist hierbei ein wichtiges Element.

Zur Entlastung und Unterstützung der polizeilichen Sachbearbeiter gewährleistet die Elektronische Schnittstelle Behörden (ESB) eine schnelle und sichere Beschaffung von Verkehrsdaten nach § 100g StPO. Sie werden bei Straftaten von erheblicher Bedeutung (insbesondere bei Katalogtaten gem. § 100a StPO) und bei Straftaten, die mittels Telekommunikation begangen wurden, nach Vorliegen eines richterlichen Beschlusses erhoben.

Durch das Erheben von TKÜ- und Verkehrsdaten werden Kosten verursacht, die durch die *Provider* in Rechnung gestellt werden. Durch eine zentrale Rechnungsbearbeitung im TKÜ-Zentrum werden erhebliche Kosten landesweit eingespart.

Anlagen | 14

PROJEKT FISBW (FUNKZELLENINFORMATIONSSYSTEM BADEN-WÜRTTEMBERG)

Das Mobilfunknetz basiert auf Standards wie *GSM* oder *UMTS*, der hauptsächlich für Telefonie, aber auch für Datenübertragung sowie Kurzmitteilungen genutzt wird. Mobilfunk ist gekennzeichnet durch die funktechnische Übertragung von einem stationären zu einem mobilen Empfänger. Beim Sender spricht man von der Basisstation, beim Empfänger von der Mobilstation. Das Sendegebiet ist eine Funkzelle. Die Größe der Funkzelle ist direkt abhängig von der Anzahl der Teilnehmer innerhalb eines bestimmten Gebietes und wird im Wesentlichen durch das Mobilfunkkonzept des Betreibers definiert. Durch die Aneinanderreihung der einzelnen Sendegebiete entsteht die zellulare Struktur des Mobilfunknetzes.
Die Ausdehnung der Funkzelle wird durch verschiedene Faktoren wie Landbeschaffenheit, Bebauung oder andere technische Einflussgrößen beeinflusst. In ländlichen Gebieten stehen die Basisstationen oft weit auseinander. Die ungefähren Radien der Funkzellen können hier bis zu 35 km betragen. In Ballungsräumen und anderen dicht besiedelten bzw. bebauten Gebieten sind die Funkzellen sehr klein, teilweise zwischen 100 bis 300 m.
Bei jedem Einschalten und Einbuchen eines Mobiltelefons werden aus technischen Gründen Informationen über die Identität des Nutzers (u. a. *IMSI*, *IMEI*) an den Netzbetreiber übermittelt. Damit ist ein Netzbetreiber in der Lage festzustellen, wann und wo ein bestimmtes Mobiltelefon eingeschaltet bzw. benutzt wurde.

Das Funkzelleninformationssystem Baden-Württemberg (FISBW) enthält Informationen über die tatsächliche Funkausbreitung von *GSM-/UMTS-Mobilfunkzellen*. Die von den Betreibern übermittelten Funkzellendaten können in ihrer tatsächlichen Ausbreitung dargestellt werden. Die kartografische Darstellung und Nutzung der auf eigener Vermessung beruhenden Daten bedeutet insbesondere im Bereich der Gefahrenabwehr, z. B. bei der Lokalisierung von Mobiltelefonen und der Auswertung von Standortdaten bei einer Vermisstenfahndung, einen hohen Einsatzwert.
Als besonders hilfreich hat sich dies für die Planung und Durchführung von Suchmaßnahmen unter Einsatz von Polizeihubschraubern erwiesen.

Anlagen | 14

Im Jahr 2012 gab es 5.318 Abfragen der FIS-Datenbank. Die Daten werden durch eine landesweite Vermessung mittels Zellvermessungssystemen bereitgestellt. Die in der Anlage 14 blau dargestellten Polizeipräsidien und -direktionen sind bereits vermessen. Die Vermessung der noch ausstehenden Polizeidirektionen ist bereits in Arbeit bzw. befindet sich in der Vorbereitung.

Das Projekt FISBW wird in enger Abstimmung mit den zu vermessenden Dienststellen umgesetzt. Die Bereitschaftspolizei unterstützt das LKA BW bei zentralen Aufgaben. Durch das Projekt FISBW wird die Vermessungstechnik bereitgestellt und das Routing, die Qualitätsprüfung der Messdaten, der Betrieb der FISBW-Datenbank sowie das Einweisen der Ansprechpartner der Polizeidirektionen gewährleistet.

OPERATIVE IT / NETZWERKFORENSIK

Die Polizeivollzugsbeamten und IT-Spezialisten (Diplom-Informatiker) des Arbeitsbereichs Operative IT/Netzwerkforensik (OIT) führen TKÜ-Maßnahmen durch, die von standardisierten Maßnahmen der klassischen Überwachung der Telekommunikation abweichen.

Die ermittlungsführenden Dienststellen des Landes werden unterstützt bei der/den

- Durchführung von Maßnahmen zur Überwachung von kryptierter Kommunikation über das Internet,
- Durchführung von Identifizierungs- und Lokalisierungsmaßnahmen von EDV-Systemen in IT-Netzwerken durch EDV-technische Maßnahmen,
- technischen Durchführung der Überwachung von Servern- und LAN-Anschlüssen im Internet,
- Überwachungen nach §§ 100a, g StPO, die mit Standardmaßnahmen nicht durchführbar sind.

Ein wesentlicher Baustein ist die Beratung von Ermittlungsbeamten, Polizeiführern in polizeilichen Sonderlagen, Staatsanwaltschaften und Richtern hinsichtlich technischer Möglichkeiten. Die beratenden und unterstützenden Maßnahmen der OIT müssen für jedes Verfahren individuell angepasst werden.

Die OIT war 2012 in 29 Verfahren beratend bzw. unterstützend tätig, hiervon in fünf Verfahren für das LKA BW und in 23 Verfahren für Landesdienststellen. In einem Verfahren wurde ein anderes Landeskriminalamt technisch unterstützt. Der Schwerpunkt lag auf Server-Überwachungsmaßnahmen, der Identifizierung und Lokalisierung von Tätern im Internet. Maßnahmen zur Gewinnung von unverschlüsselten Daten (Dekryptierung) wurden durchgeführt. Die von der OIT geleisteten Unterstützungshandlungen erstreckten sich in einzelnen Ermittlungsverfahren über einen Zeitraum von bis zu sechs Monaten.

IMSI- / WLAN-CATCHER

Dieser Arbeitsbereich führt IMSI-Catcher- bzw. WLAN-Catcher-Einsätze sowie Funkzellenbestimmungen und -vermessungen (gem. § 23a PolG BW oder § 100i bzw. § 100a StPO) durch. Die Funkzellenbestimmung erfolgt zur Vorbereitung einer Funkzellenabfrage gem. § 100g StPO. 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.

2 MASSNAHMEN / HANDLUNGSEMPFEHLUNGEN

EVALUATION ABTEILUNG „CYBERKRIMINALITÄT / DIGITALE SPUREN" BEIM LKA BW

Die Erfahrungen im Zusammenhang mit der Einrichtung der Abteilung Cyberkriminalität/ Digitale Spuren werden derzeit evaluiert. Ein Bericht wird im 1. Quartal 2013 erstellt.

SICHERHEITSOFFENSIVE POLIZEITECHNIK 2012

Im Rahmen des Programms „Sicherheitsoffensive Polizeitechnik 2012" wurden für die technische Ausstattung im Bereich Cyberkriminalität/Digitale Spuren finanzielle Mittel in Höhe von ca. 1,4 Millionen Euro zur Verfügung gestellt. Hiermit wurde insbesondere dem erforderlichen Technikbedarf bei den örtlichen Dienststellen zur Bekämpfung von Cyberkriminalität Rechnung getragen. Das LKA BW hatte Mitte des Jahres 2012 mit der Landespolizei und der Akademie der Polizei Baden-Württemberg (AkadPol BW) ein abgestimmtes Beschaffungs- und Verteilkonzept unter Berücksichtigung der anstehenden Polizeireform erarbeitet und anschließend gemeinsam mit dem Innenministerium Baden-Württemberg -Landespolizeipräsidium- (IM BW -LPP-) die notwendigen Beschaffungsmaßnahmen durchgeführt. Zielgruppen der Beschaffungsmaßnahmen waren die Sachbearbeiter Cyberkriminalität, Sachbearbeiter IT-Beweissicherung und Sachbearbeiter Datenanalyse. Wesentlicher Bestandteil der Beschaffungsmaßnahmen waren 556 Auswerte-PC zur inhaltlichen Auswertung von digitalen Spuren in polizeilichen Ermittlungsverfahren. Für die Auswerte-PC wurde durch die IT-Experten der Inspektion 710 des LKA BW eine Installations-DVD mit zur Fallbearbeitung bei Delikten der Cyberkriminalität benötigten Programmen inklusive Handlungsanleitung erstellt.

Durch den AIR wurde eine „Live DVD" entwickelt, die dem Sachbearbeiter Cyberkriminalität die notwendige Software zur gerichtsfesten Sicherung beweiserheblicher Feststellungen im Internet zur Verfügung stellt. Die Software entspricht den Richtlinien der BSI-Zertifizierung.

Für Ermittlungs- und Sicherungsmaßnahmen im Internet wurden 100 Internet-PC beschafft.

26 Analyse-PC wurden für Mitarbeiter beschafft, die im Bereich der Analyse strukturierter Massendaten eingesetzt sind (z. B. Analyse von Funkzellendaten etc.). Für den Bereich der IT-Beweissicherung wurde in Direct Attached Storage-Speichersysteme, Mobilfunkauswertesysteme und Apple Macintoshsysteme investiert.

Darüber hinaus konnten 380 Drucker sowie diverse Kleingeräte (Kopfhörer, externe USB-Festplatten, Kartenleser, Festplatten für den Datenaustausch zwischen Internet- und Auswerte-PC) beschafft werden. Die Gesamtzahl ist an der bislang an der AkadPol BW fortgebildeten Sachbearbeiter Cyberkriminalität orientiert.

BEKÄMPFUNG DER KINDERPORNOGRAFIE

Die Straftatbestände Besitz/Verschaffen sowie Verbreitung kinderpornografischer Inhalte sind gemeinsam zu betrachten und im Rahmen der Bearbeitung von Ermittlungsverfahren im Zusammenhang zu bewerten. Ein Großteil der Fälle kann erst nach Auswertung der vorliegenden Beweismittel strafrechtlich zugeordnet werden. Ist es nicht möglich, hinreichend zu beweisen, dass eine Verbreitung kinderpornografischer Schriften vorliegt, wird der Vorgang der Staatsanwaltschaft nur wegen Besitzes von kinderpornografischen Schriften vorgelegt.

Im Bereich der Auswertung von Bild- und Videomaterial stellt die Verwendung sogenannter *Hashwerte* eine verlässliche Methode zur automatisierten Datenselektion dar.
Seit April 2012 steht das bisher bundesweit eingesetzte Programm PERKEO[10] nicht mehr zur Verfügung, weshalb vor Lizenzablauf ein Konzept für die bundesweite Hash-Datenbank Pornografische Schriften (Hash-DB PS) durch eine Projektgruppe unter Beteiligung des BKA und einzelner Landeskriminalämter erarbeitet wurde. Die erforderlichen technischen und konzeptionellen Vorarbeiten dazu sind aktuell noch nicht abgeschlossen.
Die bei der ASt Kipo landesweit geführte Hash-DB PS wird die polizeilichen Sachbearbeiter bei der Bearbeitung von Ermittlungsverfahren wegen sexuellen Missbrauchs von Kindern und des Verdachts des Besitzes oder des Verbreitens von Kinderpornografie bei der Auswertung entsprechender Bild- und Videodateien wesentlich entlasten. Eine Sichtung wird nur noch einmalig zu leisten sein. Durch die bundesweite Vernetzung steht die Hash-DB PS anschließend allen Polizeibeamten zur Verfügung. Die psychische Belastung der Mitarbeiter wird sich durch die Reduzierung der noch zu bewertenden bislang unbekannten Bild- und Videodateien und die daraus resultierende Minimierung der Auswertedauer deutlich verringern.
Bei einzelnen Landeskriminalämtern im Bundesgebiet bestehen bereits größere Datenbestände bewerteter Bild- und Videodateien, die in der Hash-DB PS eingebunden werden können. Dadurch würde sich bereits mit dem Tag der Einführung dieser Datenbank die Auswertedauer entsprechender Ermittlungsverfahren deutlich reduzieren. Aufgrund noch zu klärender technischer Fragestellungen i. Z. m. der Realisierung der Hash-DB PS ist jedoch mit einem Start des Wirkbetriebs nicht vor dem Jahr 2014 zu rechnen.

[10] *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 Kinderpornografie)*

MASSNAHMEN

SCHULFAHNDUNG

Schulfahndung umfasst Fahndungsmaßnahmen bei unbekannten Bilderserien i. Z. m. sexuellem Missbrauch an Schulen. Primäre Zielrichtung derartiger Schulfahndungen ist die Beendigung andauernder Missbrauchshandlungen.
Wenn durch Ermittlungen Kinder oder Jugendliche, bei denen aufgrund sichergestellter Bild- oder Videodateien der Verdacht des sexuellen Missbrauchs gegeben ist, nicht identifiziert werden können, besteht die Möglichkeit einer zielgruppenorientierten Öffentlichkeitsfahndung an Schulen. Dies stellt eine Mindermaßnahme zur sonst üblichen Öffentlichkeitsfahndung dar. Bilddateien, die für eine Identifizierung geeignet sind, werden hierbei den Lehrkräften an Schulen im Bundesgebiet zur Prüfung übermittelt, ob es sich bei der abgebildeten Person um eine (ehemalige) Schülerin oder einen Schüler handelt.
Die ASt Kipo hat in Zusammenarbeit mit dem Innen- und Kultusministerium des Landes Baden-Württemberg Anfang des Jahres 2012 ein Merkblatt gefertigt. Darin werden den Lehrkräften der Ablauf der sogenannten Schulfahndung und die von ihnen erbetenen Maßnahmen erläutert.

Im Zuge der Schulfahndung „Donner“ des BKA im April 2012 wurden die Fahndungsinformationen in Baden-Württemberg über das Innenministerium an das Ministerium für Kultus, Jugend und Sport weitergeleitet. Von dort wurden anschließend die Schulen mittels eines E-Mail-Verteilers angeschrieben. Diese Verfahrensweise ist vorläufig auch für künftige Fälle in Baden-Württemberg vorgesehen.
Im Nachgang zur o. g. Schulfahndung wurde durch das BKA eine Bund-Länder-Projektgruppe (BLPG) eingerichtet, die polizeiliche Standards für Fahndungen an Schulen zur Bekämpfung des sexuellen Missbrauchs an Kindern beschreiben soll. Ein Ergebnis der BLPG soll noch im Jahr 2013 vorliegen.

CYBERGROOMING

Ein zu erwartendes sehr gering ausgeprägtes Anzeigeverhalten und die im Analyseteil angeführte Studie weisen auf ein enormes Dunkelfeld in diesem Deliktsbereich hin. Zum Schutz von Kindern und Jugendlichen im Internet müssen insbesondere die Präventionsmaßnahmen im Bereich Neue Medien und Internetkompetenz fortgesetzt werden. Neben der Zielgruppe der Kinder und Jugendlichen selbst, müssen Eltern und Erziehungsberechtigte über die Gefahren des Cybergroomings aufgeklärt und informiert werden.

Die EU-Richtlinie 2011/92/EU (Richtlinie vom 13. Dezember 2011, Amtsblatt der Europäischen Union vom 17. Dezember 2011) zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie fordert die Mitgliedsstaaten auf, u. a. im Bereich der Strafbarkeit bezüglich der Kontaktaufnahme zu Kindern für sexuelle Zwecke mittels Informations- und Kommunikationstechnologie nachzubessern (Artikel 6 und 7).

Die Gesetzgebung ist aufgefordert, bestehende Gesetzeslücken zeitnah zu schließen. Die Notwendigkeit wird durch Erfahrungen der OP „Donau“ bestätigt.

OPERATION DONAU / ERMITTLUNGEN WEGEN CYBERGROOMING

Die Ergebnisse dieser OP sowie ein ähnliches Ergebnis aus einem anderen Bundesland belegen das Erfordernis vermehrt in diesem Bereich tätig zu werden. Die Durchführung der OP Donau zeigte, dass auch i. Z. m. Ermittlungen im Internet auf klassische Ermittlungstätigkeit (z. B. im Bereich der Identifizierung des Beschuldigten) nicht verzichtet werden kann.

VORRATSDATENSPEICHERUNG

Der Gesetzgeber ist weiterhin – auch im Hinblick auf das EU-Recht – aufgefordert, die Vorratsdatenspeicherung unter Beachtung der Grenzen und Vorgaben des Urteils des BVerfG zur Vorratsdatenspeicherung vom 2. März 2010 neu zu regeln, um die gesetzliche Lücke zu schließen.

SOZIALE NETZWERKE – FACEBOOK-PARTYS

Ende Juni 2012 wurde das LKA BW durch das IM BW -LPP- damit beauftragt, eine Handreichung für die Dienststellen in Baden-Württemberg zu erstellen, in dem die Besonderheiten des Phänomens Facebook-Partys und die Rechtsgrundlagen für die in Frage kommenden polizeilichen Maßnahmen dargestellt werden. Nahezu zeitgleich wurde durch die Teilnehmer der Tagung Polizeiliche Aufgaben der Beschluss gefasst, einen landesweiten Expertenworkshop unter Federführung der Landespolizeidirektion (LPD) Stuttgart durchzuführen. Das LKA BW hat die bis zum Workshop erarbeiteten Ergebnisse bzw. Erfahrungswerte aus Einsatzunterstützungen im Vorfeld durch seine Teilnehmer in den Informationsaustausch und die anschließende Erarbeitung einer Handreichung einfließen lassen[11].

Die Handlungsempfehlung enthält sowohl Hinweise zu tangierten Rechtsgrundlagen als auch mögliche Handlungsoptionen für (Polizei-)Behörden und den Polizeivollzugsdienst sowohl vor als auch während und nach der Veranstaltung. Daneben wurden Vorlagen sowie Hinweise für die Einsatzbewältigung und Musterverfügungen erarbeitet und den Dienststellen zur Verfügung gestellt.
Als Erfolgsfaktor für die Bewältigung von Facebook-Partys oder ähnliche Veranstaltungen wurde die frühzeitige Einbindung von speziell ausgebildeten Polizeibeamten in der Funktion der Sachbearbeiter Cyberkriminalität identifiziert. Diese werden mit der anlassbezogenen Internetrecherche und Datensicherung zur Ermittlung von Organisatoren und Teilnehmern in den genutzten *Sozialen Netzwerken* beauftragt. Reicht das vor Ort vorhandene Spezialwissen nicht aus, unterstützt das LKA BW mit seinen Spezialisten.

[11] *„Hinweise und Empfehlungen IM BW -LPP- zur Vorbereitung und Bewältigung von Einsätzen der Polizei im Zusammenhang mit Veranstaltungen nach Aufrufen in sozialen Netzwerken (u. a. „Facebook-Partys“) vom 25. Oktober 2012“, landesweit mit Schreiben vom 30. Oktober 2012 umgesetzt.*

MASSNAHMEN

Während des Einsatzes sind aufgrund der besonderen Phänomenausprägung bestimmte Maßnahmen, insbesondere in Zusammenhang mit der Öffentlichkeitsarbeit, zu berücksichtigen. Die taktische Kommunikation vor Ort sowie die parallele Präsenz in *Sozialen Netzwerken*, um negativen Entwicklungen der Veranstaltung schnell begegnen zu können, sind erfolgskritische Faktoren für einen derartigen Einsatz. Mit den Maßnahmen ist beabsichtigt, die Anzahl der Teilnehmer im Vorfeld abschätzen zu können.
Die Polizei und andere Behörden und Organisationen mit Sicherheitsaufgaben verfolgen bei Facebook-Partys das Ziel, Gewaltakte, Straftaten, Alkoholexzesse oder Verstöße gegen das Jugendschutzgesetz zu verhindern. Der Verfolgung von Straftaten und Ordnungswidrigkeiten in Zusammenhang mit Facebook-Partys kommt hierbei eine besondere generalpräventive Bedeutung zu. Öffentlichkeitswirksame Verbotsverfügungen, Auflagen sowie die Verhängung von Ordnungsgeldern gegen die Anmelder bzw. Verursacher und die Auferlegung der entstandenen Kosten im Nachgang zur Veranstaltung entfalten in der Regel eine präventive Wirkung auf Nachahmungstäter.

IT-EXPERTEN

Im April 2011 und den darauffolgenden Monaten wurden in der Polizei Baden-Württemberg 15 IT-Experten für die Bereiche Ermittlungen Cyberkriminalität/Arbeitsbereich Internetrecherche, IT-Beweissicherung (jetzt Forensische IuK), Operative IT sowie bei der AkadPol BW eingestellt.
Die Erfahrungen sind durchweg positiv. Erwartungen, die an eine Zusammenarbeit mit ausgebildeten Informatikern und dem bei den neuen Mitarbeitern vorhandenen IT-Fachwissen gerichtet wurden, haben sich erfüllt.
Beispielsweise wurde der Arbeitsbereich Ermittlungen der Inspektion 710 von den IT-Experten in Ermittlungsverfahren unterstützt, z. B. bei der Aufbereitung von Netzwerkdaten der Server-TKÜs oder der Serverauswertung (Analyse des Servers und Auswertung von *Logdateien*). Teilweise entwickelten sie hierzu eigene Auswertetools.

SONDERLAUFBAHN CYBERKRIMINALIST

Bei den technisch hochspezialisierten Aufgabenstellungen und kriminalistischen Vorgehensweisen im Zusammenhang mit Ermittlungsverfahren und Ermittlungsaufträgen der Cyberkriminalität kommen klassisch ausgebildete Polizeivollzugsbeamte zunehmend an ihre Grenzen. Notwendige Qualifikationen sind nur mit erheblichem Fortbildungsaufwand möglich.
Die bisherigen Erfahrungen mit IT-Experten belegen, dass diese technisches Know-how mitbringen, um auch bedeutende technische Schwierigkeiten zu bewältigen. Allerdings benötigen eingestellte IT-Experten polizeiliches Wissen, um polizeiliche Maßnahmen in einem Ermittlungsverfahren verknüpft mit hoheitlichen Befugnissen durchführen zu können. Strafrechtliches, strafprozessuales und insbesondere polizeitaktisches „Mit- und Vorausdenken“ sind für dieses Aufgabenfeld notwendig.
Eine Sonderlaufbahn Cyberkriminalität wird eingeführt. Die Sonderlaufbahn wird sich an die bereits bestehende Sonderlaufbahn Wirtschaftskriminalität anlehnen. Die notwendigen Vorbereitungsmaßnahmen werden derzeit umgesetzt.

RANSOMWARE

Ermittlungsansätze sind in aller Regel nicht nur über die Verbindungsdaten oder festgestellte Zielkonten vorhanden. Auch aus erlangten Vermögensvorteilen in digitalen Währungen, welche missbräuchlich zum Onlineeinkauf benutzt werden, ergeben sich Hinweise. Generell führen viele Erkenntnisse aus Ermittlungen im Bereich der Cyberkriminalität jedoch ins Ausland. Hier erweist es sich häufig als schwierig, über die Ländergrenzen hinweg aktiv zu werden. Deshalb kommt der engen und koordinierten nationalen und internationalen Zusammenarbeit im Bereich der Cyberkriminalität eine immer größere, häufig entscheidende Bedeutung zu.

Das BKA und das BSI haben die aktuelle Variante, bei denen eine strafbewehrte jugendpornografische Abbildung eingeblendet wird, am 29. Januar 2013 erneut zum Anlass genommen, vor Fällen der *Ransomware* zu warnen. In der gemeinsamen Presseerklärung heißt es: „Sollten Sie eine derartige Meldung erhalten, zahlen Sie den geforderten Betrag auf keinen Fall! Ihr Rechner ist bereits mit einer *Schadsoftware* infiziert, die wesentliche Teile des Betriebssystems verändert hat, um das Popup-Fenster zu generieren. Ein regulärer Zugriff auf Ihr Betriebssystem ist mit hoher Wahrscheinlichkeit auch nach Begleichung der geforderten Zahlung nicht möglich.
Vorsorglich wird darauf hingewiesen, dass die Sicherung der in der *Ransomware* enthaltenen jugendpornografischen Darstellung eine Besitzverschaffung bzw. einen strafbaren Besitz von Jugendpornografie darstellt.
Hilfreiche Hinweise zur Bereinigung Ihres Systems von *Schadsoftware* finden Sie auf den Internet-Seiten des Anti-Botnetz-Beratungszentrums unter www.botfrei.de.
BKA und BSI empfehlen, den Update-Status des Betriebssystems und der genutzten *Anti-Viren-Software* sowie aller installierten Programme auf dem aktuellen Stand zu halten. Dies erhöht die Chancen, dass es erst gar nicht zu einer Infektion mit der *Schadsoftware* kommt."

ERFASSUNG VON AUSLANDSSTRAFTATEN IN DER PKS

Die hohe Zahl an Auslandstraftaten bedingt eine nur unzureichende Aussagekraft der PKS für den Deliktsbereich Cyberkriminalität. Das Tatortprinzip der PKS-Richtlinien sieht vor, keine Auslandsstraftaten mit geklärtem oder ungeklärtem Tatort zu erfassen. Durch den hohen Anteil an Straftaten mit Auslandsbezug finden deshalb die meisten dieser Fälle keinen Eingang in die PKS.
Beispielsweise sind im Phänomenbereich *Ransomware* aus der PKS heraus keine verlässlichen Auskünfte zum polizeilichen Hellfeld möglich. Hier ist ein Rückgriff auf den SMD Cybercrime erforderlich. Ein Vergleich mit dem Polizeilichen Informationssystem Baden-Württemberg ergibt, dass bspw. 2.899 Fälle der Erpressung mit Sonderkennung Internet im Jahr 2012 nicht in die PKS eingingen. Die Geschädigten der infizierten Rechner befinden sich zwar in Baden-Württemberg, aufgrund bisheriger Erkenntnisse muss jedoch davon ausgegangen werden, dass die Angriffe vom Ausland aus durchgeführt werden.

MASSNAHMEN

ERPRESSUNGEN IM ZUSAMMENHANG MIT VIDEO(CHAT)PLATTFORMEN

Die Entwicklung dieses Phänomens wird durch das LKA BW beobachtet. Eine erste landesweite Anfrage zu Erkenntnissen wurde bereits gesteuert. Da sich eine Vielzahl der Opfer aus Scham nicht an die Polizei wenden dürfte, muss von einem hohen Dunkelfeld ausgegangen werden. Anlassbezogen wird das LKA BW medienwirksame Präventionshinweise erarbeiten.

DIGITALE FORENSIK

IT-BEWEISSICHERUNG

Die Fremdvergabe von Untersuchungsaufträgen entlastet die Polizei insbesondere dann, wenn sie sich im Verlauf des Verfahrens mit Spezialsoftware konfrontiert sieht und einschlägige Technik und Kenntnisse zur Datensicherung nicht vorhanden sind. Die Vergabe der Datenträgeruntersuchung an externe Sachverständige sollte auf die Verfahren beschränkt werden, die im Wesentlichen zu den Belastungsspitzen und langen Bearbeitungszeiten bei ITB beitragen. In jedem Einzelfall ist zu prüfen, ob sich das konkrete Verfahren für die Vergabe an einen externen Gutachter geeignet ist. Das LKA BW wird hierzu in Absprache mit der Staatsanwaltschaft eine entsprechende Handreichung erarbeiten.

ANALYSE STRUKTURIERTER MASSENDATEN / ARBEITSBEREICH STRUKTURIERTE MASSENDATEN

Die im Rahmen der Sicherheitsoffensive 2012 beschafften 26 Rechnereinheiten für die Sachbearbeiter Datenanalyse wurden zwischenzeitlich landesweit ausgeliefert. Erste Erfahrungen mit diesem für die Analysten neuen Werkzeug zeigen, dass Arbeitsprozesse weiter entwickelt bzw. angepasst werden müssen. Diese Anpassungen müssen stets auch mit Blick auf die Kostenentwicklung betrieben werden.

Neben den zur Verfügung stehenden finanziellen Mitteln ist der Bereich der Aus- und Fortbildung ein weiterer erfolgskritischer Faktor. Über das grundsätzliche Verständnis für Datenbanken und -strukturen als Basiswissen hinaus sollen dem künftigen Datenanalysten unter anderem der Umgang und die Verwendung zahlreicher Spezialprogramme vermittelt werden. Dieses ehrgeizige Ziel, flächendeckend eine Kompetenz für die Gewinnung neuer Ermittlungsansätze und Beweismittel aus strukturierten Massendaten zu generieren, stellt hohe Anforderungen an den Bereich der Aus- und Fortbildung.

Die immer schneller wachsenden Datenmengen und die steigende Vernetzung, sei es durch *Smartphones* und *Cloudtechnik*, stellen die IT-Forensiker laufend vor neue Herausforderungen. Diesen kann nur durch ständige Fortbildung und kontinuierliche Investitionen in PC-Hardware und Software begegnet werden.

KOMPETENZZENTRUM TELEKOMMUNIKATIONSÜBERWACHUNG

Der entstandene erhebliche rechtliche und technische Regelungsbedarf wurde in einer BLPG mit dem Bericht „Ergänzung der TKÜV“ zusammengefasst und liegt mit konkreten Änderungsvorschlägen der AG Kripo zur Umsetzung vor.
Seit dem Jahr 2010 besteht mit dem Bayerischen Landeskriminalamt eine Kooperation. Themen- und Kooperationsfelder sind die gegenseitige Unterstützung, das Zusammenwirken beim Aufbau der Funkzelleninformationssysteme sowie die Bereiche Fortbildung und Operative IT.

Neben der Beratung und Umsetzung von Beschlüssen finden durch die Mitarbeiterinnen und Mitarbeiter der TKÜ-Zentrale landesweit individuelle Einweisungen, Schulungen und Vorträge für Bedarfsträger statt.

Beim BKA wurde im Jahr 2012 ein Kompetenzzentrum eingerichtet, das sich mit der Fortentwicklung und Ausgestaltung der Quellen-TKÜ befasst.

BETRIEB DER TKÜ-ANLAGE

Die ständige Weiterentwicklung der Telekommunikationsüberwachungsanlage ist Grundvoraussetzung, um sich den ändernden Bedingungen anzupassen. Daher wurde im Jahr 2012 ein umfassendes Software-Update der TKÜ-Anlage durchgeführt. Dabei wurde die TKÜ-Anlage für den neuen *IPv6-Standard* ertüchtigt.
Der Betrieb und die Fortentwicklung werden in den nächsten Jahren erneut erhebliche finanzielle Aufwendungen erfordern. Die Investitionen garantieren den störungsfreien Betrieb der TKÜ-Anlage sowie einen rechtskonformen und fachgerechten Umgang mit den erhobenen Daten.
Der Schutz von Kommunikationsvorgängen mit Berufsgeheimnisträgern und Inhalte des *Kernbereichs privater Lebensführung* werden vollumfassend durch die eingesetzte Technik im LKA BW gewährleistet.

FISBW

Bis Jahresende 2013 soll die Landesfläche vermessen sein. Ein zeitgerechter Abschluss ist für den Betrieb der neuen Führungs- und Lagezentren der zukünftigen regionalen Polizeipräsidien ab dem Jahr 2014 relevant.
Zur Zielerreichung wurde Ende des Jahres 2012 in weitere Zellvermessungssysteme investiert. Ergänzend setzen die Polizeidirektionen, deren Zuständigkeitsbereich noch nicht vermessen ist, zusätzliches Personal ein. Um den betroffenen Dienststellen das zu Grunde liegende Vermessungskonzept vorzustellen, fand am 22. Januar 2013 im LKA BW eine zentrale Informationsveranstaltung für die Leiter der Führungs- und Einsatzstäbe der betroffenen Polizeidirektionen und Vertreter der Landespolizeidirektionen sowie des IM BW -LPP- statt. Die Dienststellen planen und koordinieren die Vermessung selbst und führen diese eigenständig durch.

MASSNAHMEN

Um die Mitarbeiter (sog. FISBW-Koordinatoren) auf ihre Aufgaben vorzubereiten, wurde vom Projekt FISBW eine Schulungskonzeption erarbeitet, die sowohl die Vermittlung von fachspezifischem Wissen als auch praktische Übungen beinhaltet. Die Schulungskonzeption ist Grundlage für entsprechende Schulungen für die FISBW-Koordinatoren an der AkadPol BW in Freiburg.
Die permanente Fortentwicklung der FISBW-Datenbank wird in enger Kooperation mit dem Bayerischen Landeskriminalamt sichergestellt.
Aktuell wird die FISBW-Datenbank gemeinsam durch die Landeskriminalämter Bayern und Baden-Württemberg modernisiert und grundlegend überarbeitet. Unter anderem sollen die Daten dem Sachbearbeiter benutzerfreundlicher und besser aufbereitet zur Verfügung gestellt werden.

OPERATIVE IT / NETZWERKFORENSIK

Die Umsetzung von Ausgleichsmaßnahmen wird zunehmend komplexer und setzt weiterhin den gemeinsamen Einsatz von IT-Spezialisten und Polizeivollzugsbeamten voraus. Nicht unerhebliche Finanzmittel sind nötig, um der Nutzung des Internets zur Begehung von schweren Straftaten begegnen zu können.

IMSI- / WLAN-CATCHER

Im Zusammenhang mit der rasch fortschreitenden Einführung von *LTE* sind mittelfristig Investitionen notwendig, um weiterhin im gesamten Mobilfunkspektrum einsatzfähig zu bleiben.
Um die steigenden Einsatzzahlen bewältigen zu können müssen Einsatzkriterien festgelegt, Personal verstärkt und Investitionen vorgenommen werden.

GESAMTKONZEPTION CYBERKRIMINALITÄT / DIGITALE SPUREN

Das LKA BW wurde durch das IM BW -LPP- damit beauftragt, eine landesweite Gesamtkonzeption „Cyberkriminalität/Digitale Spuren“ zu erstellen. Diese Konzeption wurde am 1. Februar 2013 an das IM BW -LPP- übersandt. Die Gesamtkonzeption wurde zuvor innerhalb der Projektstruktur zur Polizeireform mit Vertretern der Landespolizei und des IM BW -LPP- abgestimmt. Mit der Gesamtkonzeption sollen landesweit insbesondere folgende Bereiche geregelt werden: Aufgabenfelder und -abgrenzung bei der Bekämpfung und Bearbeitung von Delikten der Cyberkriminalität, Fachaufsicht, Personal und Personalausstattung, Aus- und Fortbildung, sachliche Ausstattung und deren Beschaffung, Raumbedarf sowie Gremienarbeit. Im Rahmen der Erarbeitung der Konzeption wurden 25 Handlungsempfehlungen erarbeitet. Nach Zustimmung der Polizeichefbesprechung am 13./14. Februar 2013 werden sie nach ihrer zeitlichen Priorisierung durch die festgelegten Stellen bearbeitet. Die Federführung für die Umsetzung haben das IM BW -LPP- und das LKA BW gemeinsam übernommen. Die meisten Handlungsempfehlungen sollen noch vor Umsetzung der Polizeireform abschließend bearbeitet werden, damit die Ergebnisse in der künftigen Struktur der Polizei bereits mit Umsetzung der Polizeireform ihre Wirkung erzielen.

SYMPOSIUM AM 23. OKTOBER 2012 IN STUTTGART

Im Rahmen der Feierlichkeiten zum 60-jährigen Bestehen des Landes und des Landeskriminalamts Baden-Württemberg richtete das LKW BW am 23. Oktober 2012 im Rathaus der Stadt Stuttgart ein Symposium mit dem Titel und Thema: „Virtuelle Welten. Reale Gefahren. Herausforderungen der Kriminalität 2.0“ aus.

Über 200 Gäste aus Politik, Wissenschaft, Wirtschaft, Justiz sowie Kolleginnen und Kollegen der Polizei aus Baden-Württemberg, dem Bundesgebiet und Österreich nahmen an der Veranstaltung teil und verfolgten die Reden, Vorträge und Podiumsdiskussionen. Hochkarätige Referenten aus verschiedenen Sicherheitsbehörden, der freien Wirtschaft sowie der Forschung und Lehre beleuchteten die aktuellen und zukünftigen Problemstellungen, die sich aus der zunehmenden Digitalisierung des Alltags ergeben. Neben der Darstellung aktueller Maßnahmen, Problemstellungen und Lösungsansätzen wurden Handlungsbedarfe erarbeitet, die sich an Politik, Sicherheitsbehörden und die Wirtschaft richten. Im Rahmen der Veranstaltung eröffnete Herr Innenminister Reinhold Gall (MdL) einen „Internetsicherheits-Parcours“ für die Bürgerinnen und Bürger, dessen Schirmherrschaft er auch übernahm. Der Parcours konnte im Anschluss an die Veranstaltung an mehreren Tagen im Stadtgebiet Stuttgart besichtigt und durchlaufen werden.

ZENTRALE ANSPRECHSTELLE CYBERCRIME

Auf Ebene der AG Kripo und der Innenministerkonferenz sowie dessen Arbeitskreis II wurden in den Jahren 2009/2010 Beschlüsse gefasst, die den Ländern empfehlen „Zentrale Ansprechstellen Cyberkriminalität“ (ZAC) einzurichten. Die Mitarbeiterinnen und Mitarbeiter der ZAC sollen die Aufgabe des zentralen Ansprechpartners für die Wirtschaft, öffentliche und nichtöffentliche Stellen auf Bundes- und Landesebene wahrnehmen.

Die organisatorischen Voraussetzungen für den wirkungsvollen Einsatz der ZAC sind in Baden-Württemberg durch die Einrichtung der neuen Abteilung Cyberkriminalität/Digitale Spuren geschaffen worden. Die Aufgabe wurde der Führungsgruppe der Abteilung übertragen. Diese erarbeitet derzeit ein Konzept für die zukünftige Aufgabenwahrnehmung der ZAC. Die Einrichtung der K5 bei den regionalen Polizeipräsidien ermöglicht es, ein effektives landesweites Netzwerk von fachlichen Ansprechpartnern einzurichten. Durch die Einrichtung einer ZAC werden Parallelprozesse innerhalb der Polizei des Landes vermieden und Informationslagen an einer Stelle gebündelt sowie zielgerichtet gesteuert.

KOOPERATIONEN

Die Abteilung Cyberkriminalität/Digitale Spuren hat im Jahr 2012 Gespräche mit unterschiedlichen Behörden, Institutionen und Organisationen aufgenommen. Nicht nur das Symposium am 23. Oktober 2012 hat deutlich aufgezeigt, dass zur Bekämpfung der Cyberkriminalität und zur Erhöhung der Cybersicherheit ein starkes Netzwerk aus Partnern erforderlich ist.

Im Berichtsjahr 2012 wurde eine Kooperation mit der Hochschule Albstadt-Sigmaringen beschlossen, die sich derzeit in der letzten Abstimmung befindet. Weiterhin wurde der Beitritt zu der bestehenden Kooperation zwischen dem Landeskriminalamt Nordrhein-Westfalen und dem BITKOM-Branchenverband entschieden. Die Unterzeichnung des Kooperationsvertrags hat am 7. März 2013 im Rahmen der CeBIT in Hannover stattgefunden.

PRÄVENTION

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

SAFER INTERNET DAY 2013

Die Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK), dessen Zentrale Geschäftsstelle beim LKA BW eingerichtet ist, hat in Zusammenarbeit mit dem BSI anlässlich des Safer Internet Days 2013 Tipps für sichere Passwörter herausgegeben. Ausgangslage war eine repräsentative Umfrage des Forschungsunternehmens TNS Emnid im Auftrag des BSI, die belegte, dass deutsche Internetnutzer bei Passwörtern zu bequem wären. Die Tipps sind auf der Internetseite http://www.polizei-beratung.de eingestellt[12].

ONLINE-ANGEBOTE DER PRÄVENTION

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

[12] *http://www.polizei-beratung.de/presse/782-umfrage-belegt-deutsche-internetnutzer-sind-bei-passwoertern-zu-bequem-.html*

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), welche eine umfangreiche Auswahl an Faltblättern und CD-ROMs zum Thema Sicherheit in der Informationstechnik bietet:
http://www.bsi-fuer-buerger.de

Statistische Daten zu Maßnahmen nach §§ 100a und 100g StPO: https://www.bundesjustizamt.de/de/themen/buergerdienste/justizstatistik/telekommunikation/telekommunikationsueberwachung.html

ANLAGEN

3 ANLAGEN

Grundlage des Jahresberichts sind die Daten aus der PKS, dem kriminalpolizeilichen Nachrichtenaustausch, (Sonder-)Meldediensten und eigenen Erhebungen.

DEFINITION CYBERCRIME

Mit Beschluss der Leitertagung Cybercrime am 28./29. September 2011 wurde der Vorschlag zur Einrichtung einer BLPG mit der Aufgabe der Evaluierung der Datenbasis und Erarbeitung von Optimierungsvorschlägen zur Beschreibung der Cybercrime als Grundlage strategischer Entscheidungen in die Kommission Kriminalitätsbekämpfung (KKB) eingebracht. Die KKB beschloss die Einrichtung der BLPG im Rahmen ihrer 26. Tagung im Oktober 2011. An ihr beteiligten sich unter Federführung des BKA die Länder Baden-Württemberg, Bremen, Hessen, Niedersachsen, Nordrhein-Westfalen und Thüringen. Ziel war die Erarbeitung einer zukunftsfähigen Definition des Begriffs „Cybercrime" unter Berücksichtigung von nationalen und internationalen Sicherheitsstrategien und Definitionen. Der Auftrag schloss Empfehlungen zur Überarbeitung des Meldedienstes „IuK-Kriminalität" in INPOL-Fall und der PKS mit ein. Die BLPG „Definition Cybercrime" erarbeitete nachfolgende Definition des Begriffes Cybercrime:

Cybercrime umfasst die Straftaten, die sich gegen

- das Internet,
- weitere Datennetze,
- informationstechnische Systeme

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

Während die neue Begriffsdefinition und die Empfehlungen zum SMD Cybercrime bereits umgesetzt wurden (siehe hierzu Absatz unten), wurde die PKS-Erfassung derzeit noch nicht angepasst. Bis auf Weiteres sind deshalb noch die alten Begrifflichkeiten und Definitionen (Internetkriminalität und Computerkriminalität) anzuwenden.

INTERNETKRIMINALITÄT (CYBERKRIMINALITÄT IM WEITEREN SINNE)

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.

COMPUTERKRIMINALITÄT (CYBERKRIMINALITÄT IM ENGEREN SINNE)

Straftaten, bei denen die EDV in den Tatbestandsmerkmalen der Strafnorm genannt ist.

Der Computerkriminalität werden in der PKS folgende Delikte zugeordnet:

-	Betrug mittels rechtswidrig erlangter Debitkarten mit PIN	(§ 263a StGB)
-	Computerbetrug	(§ 263a StGB)
-	Betrug mit Zugangsberechtigung zu Computerdiensten	(§ 263 StGB)
-	Fälschung beweiserheblicher Daten	(§ 269 StGB)
-	Täuschung im Rechtsverkehr bei Datenverarbeitung	(§§ 269, 270 StGB)
-	Datenveränderung, Computersabotage	(§§ 303a + b StGB)
-	Ausspähen von Daten	(§ 202a StGB)
-	Abfangen von Daten	(§ 202b StGB)
-	Vorbereitung des Ausspähens und Abfangen von Daten	(§ 202c StGB)
-	Softwarepiraterie, privat und gewerbsmäßig	(UrhG)

SONDERMELDEDIENST CYBERCRIME

Die bei der Computerkriminalität aufgeführten Straftaten waren mit Ausnahme der Straftaten nach dem Urheberrechtsgesetz im Rahmen des Meldedienstes „Kriminalität im Zusammenhang mit Informations- und Kommunikationstechnik (IuK-Kriminalität)“ meldepflichtig und wurden bislang in der INPOL Fall-Datei IuK erfasst.

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.

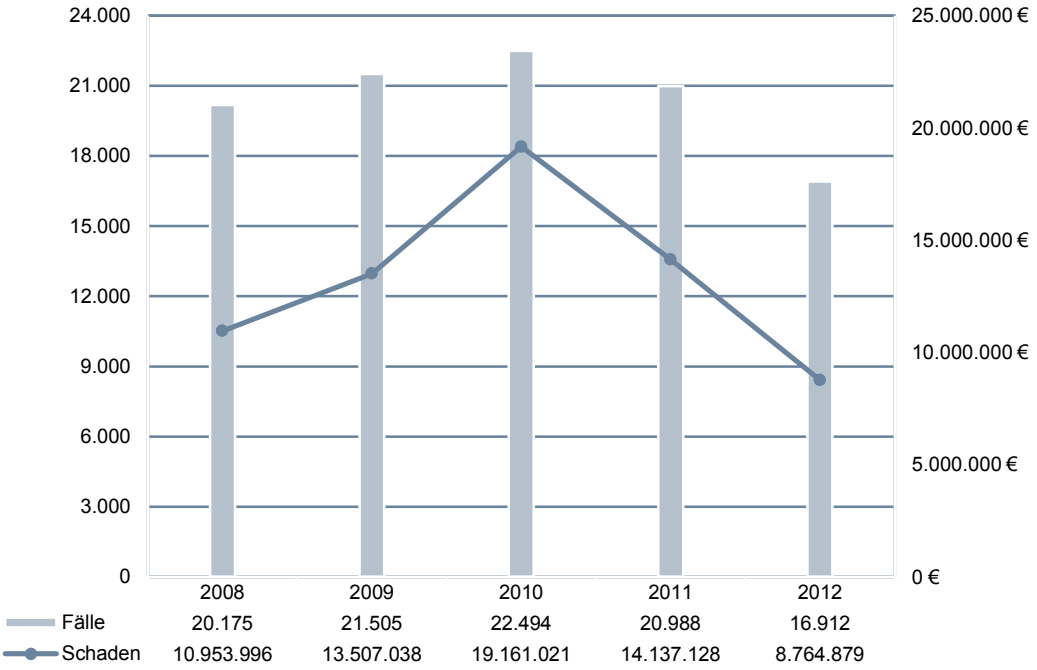
Der Meldedienst umfasst folgende Delikte:

-	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)

1 | PKS-BAROMETER INTERNETKRIMINALITÄT 2011/2012

	PKS-Schlüssel	2011	2012	in %	Tendenz
Internetkriminalität	Tabelle 05	20.988	16.912	-19,4	↘
Schadenssumme in €	Tabelle 05	14.137.128	8.764.879	-38,0	↘
Vermögens- und Fälschungsdelikte	Tabelle 05 5000**	16.220	12.219	-24,7	↘

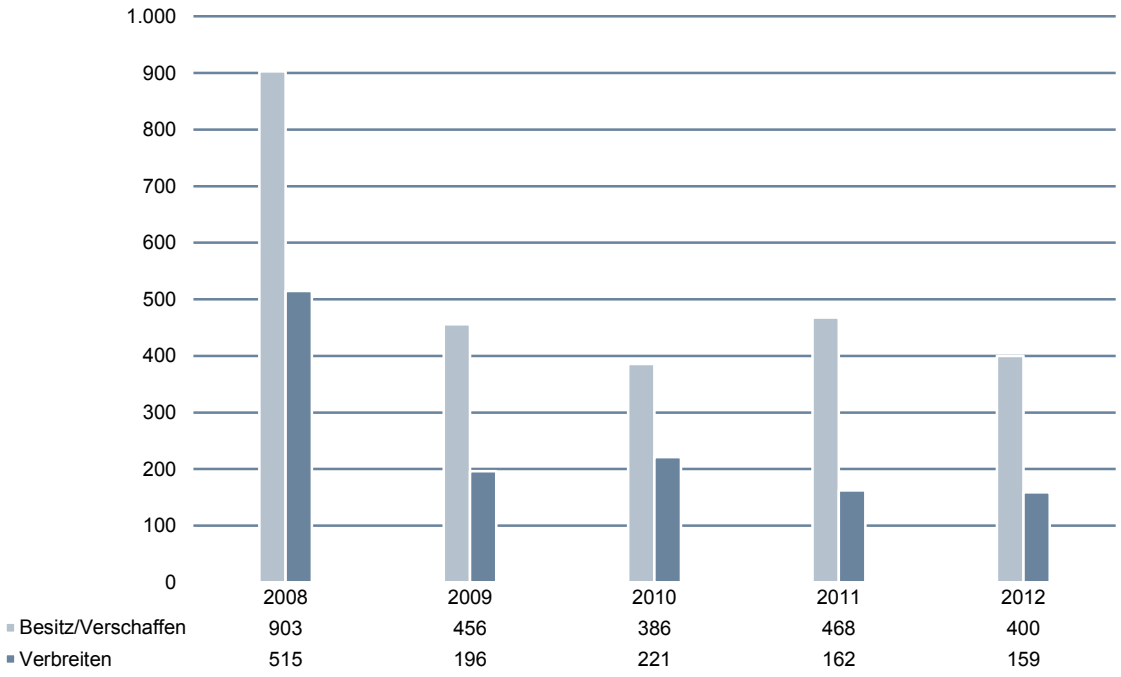
2 | INTERNETKRIMINALITÄT FÜNFJAHRESVERGLEICH (2008 BIS 2012)



3 | PKS-BAROMETER KINDERPORNOGRAFIE 2011/2012

	PKS-Schlüssel	2011	2012	in %	Tendenz
Besitz/Verschaffen von Kinderpornografie (§ 184b StGB)	1433	468	400	-14,5	↘
Verbreitung von Kinderpornografie (§ 184b StGB)	1434	162	159	-1,9	→

4 | BESITZ / VERSCHAFFEN UND VERBREITEN VON KINDERPORNOGRAFIE 2008 BIS 2012



5 | TABELLE STRAFVERFAHRENINITIIERUNGEN AIR 2008 BIS 2012

Berichtsjahr	2008	2009	2010	2011	2012
Deutschland	1.504	338	66	420	40
davon Baden-Württemberg	100	30	3	24	4
International	8.557	2.305	1.045	7.720	636
Gesamt	**10.061**	**2.643**	**1.111**	**8.164**	**676**

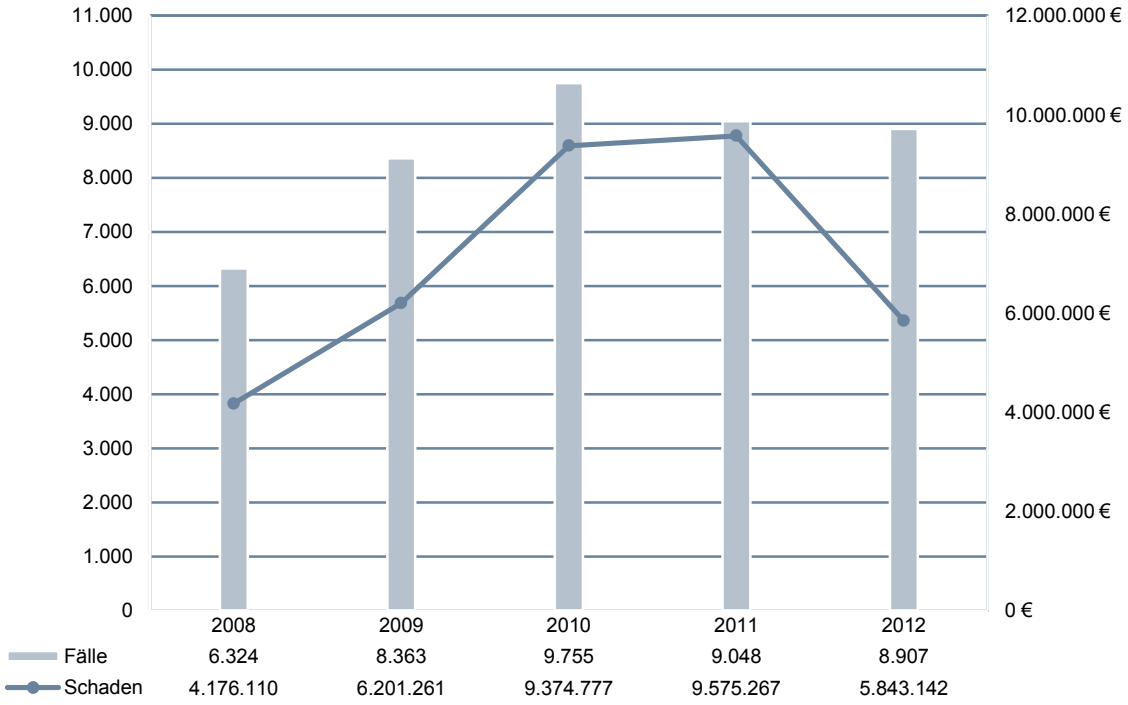
6 | PKS-BAROMETER COMPUTERKRIMINALITÄT 2011 / 2012

	PKS-Schlüssel	2011	2012	in %	Tendenz
Computerbetrug (§ 263a StGB)	5175	4.194	3.658	-12,8	↘
Fälschung beweiserheblicher Daten (§ 269 StGB)/Täuschung im Rechtsverkehr (§ 270 StGB)	5430	618	649	+5,0	↗
Datenveränderung (§ 303a StGB)/ Computersabotage (§ 303b StGB)	6742	236	292	+23,7	
Ausspähen von Daten (§ 202a StGB)	6780	1.343	1.346	+0,2	→
Computerkriminalität	8970	9.048	8.907	-1,6	↘

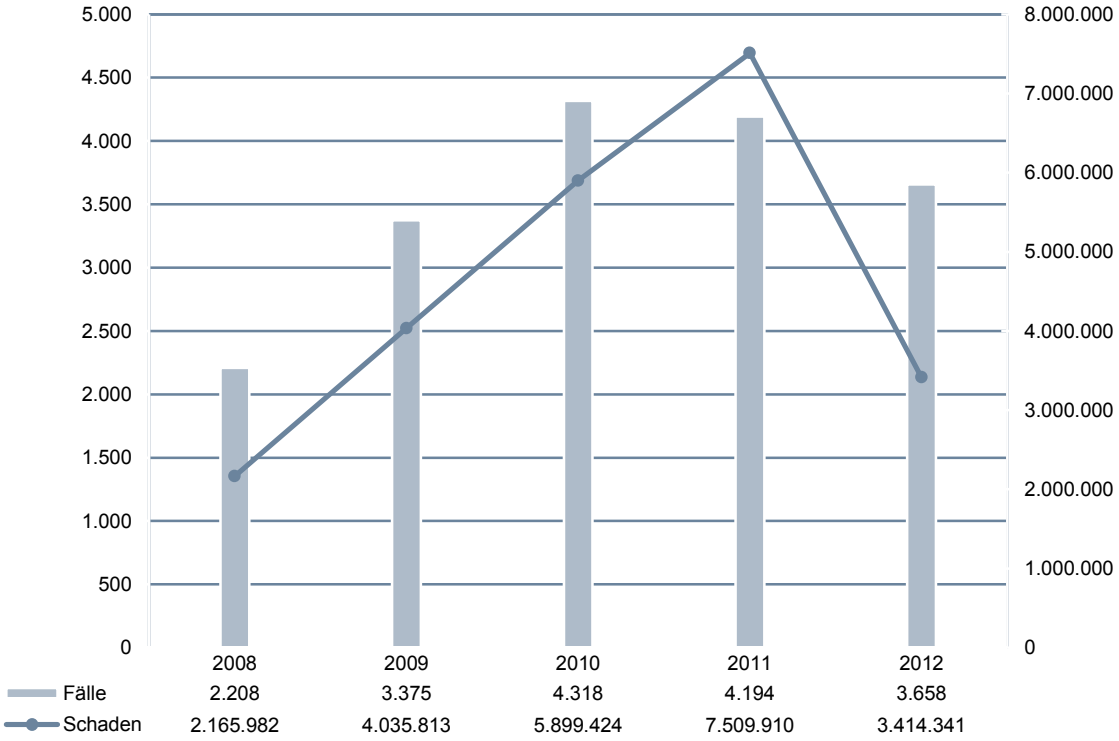
7 | TABELLE COMPUTERKRIMINALITÄT 2008 BIS 2012

Berichtsjahr	2008	2009	2010	2011	2012
Computerbetrug PKS 5175	2.208	3.375	4.318	4.194	3.658
Schadenssumme in € Computerbetrug	2.165.982	4.035.813	5.899.424	7.509.910	3.414.341
Fälschung beweiserheblicher Daten/Täuschung im Rechtsverkehr PKS 5430	342	672	638	618	649
Datenveränderung/ Computersabotage PKS 6742	212	141	194	236	292
Ausspähen von Daten PKS 6780	828	1.242	1.444	1.343	1.346
Computerkriminalität PKS 8970	6.324	8.363	9.755	9.048	8.907
Schadenssumme in € Computerkriminalität	4.176.110	6.201.261	9.374.777	9.575.267	5.843.142

8 | COMPUTERKRIMINALITÄT FÜNFJAHRESVERGLEICH (2008 BIS 2012)

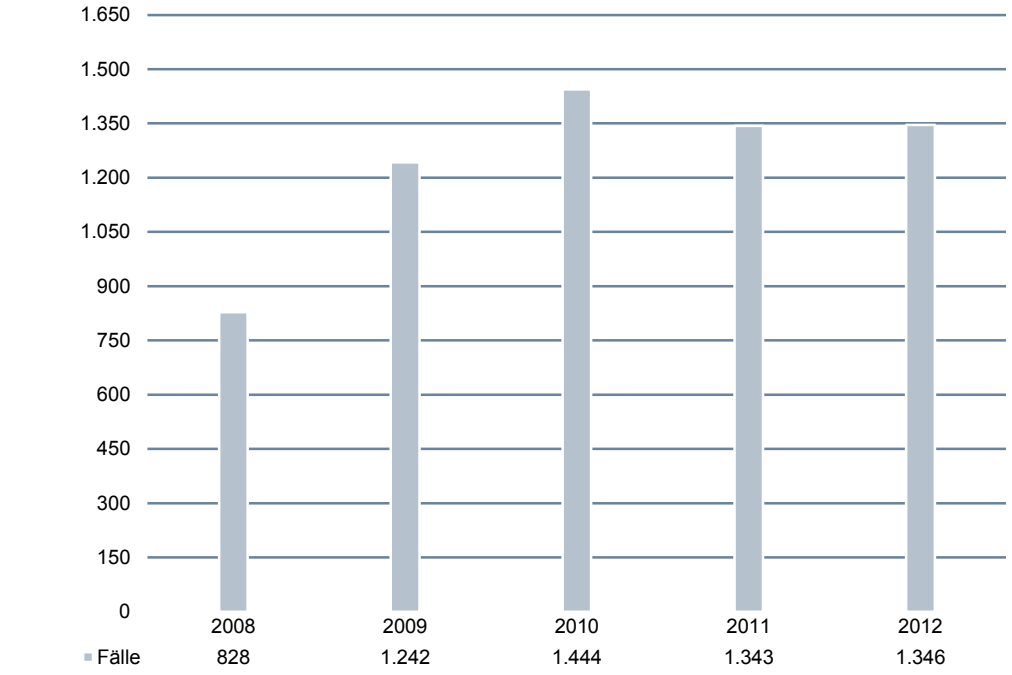


9 | COMPUTERBETRUG 2008 BIS 2012



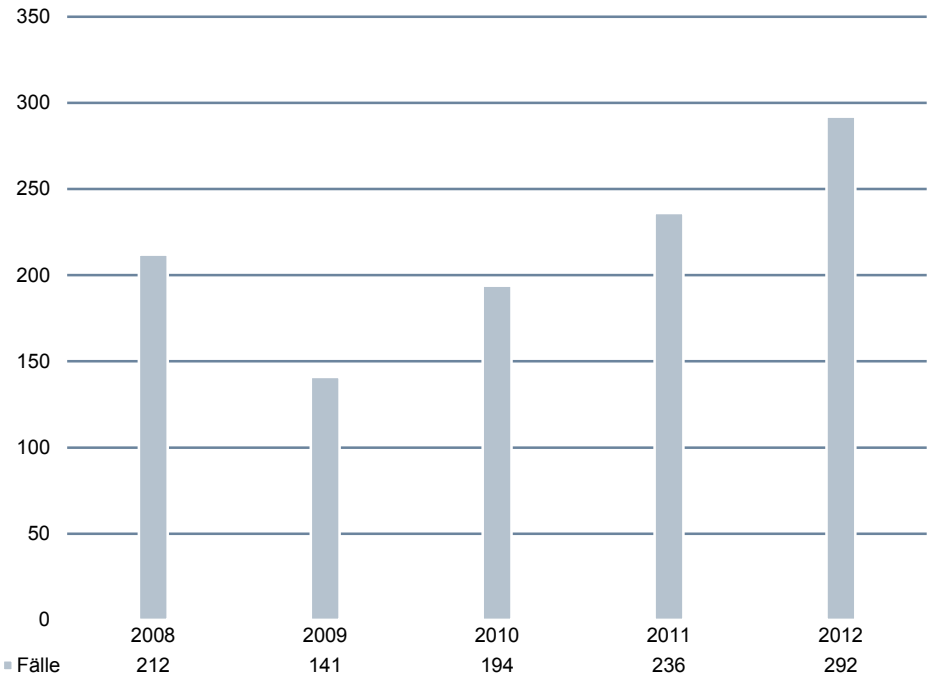
	2008	2009	2010	2011	2012
Fälle	2.208	3.375	4.318	4.194	3.658
Schaden	2.165.982	4.035.813	5.899.424	7.509.910	3.414.341

10 | AUSSPÄHEN VON DATEN 2008 BIS 2012

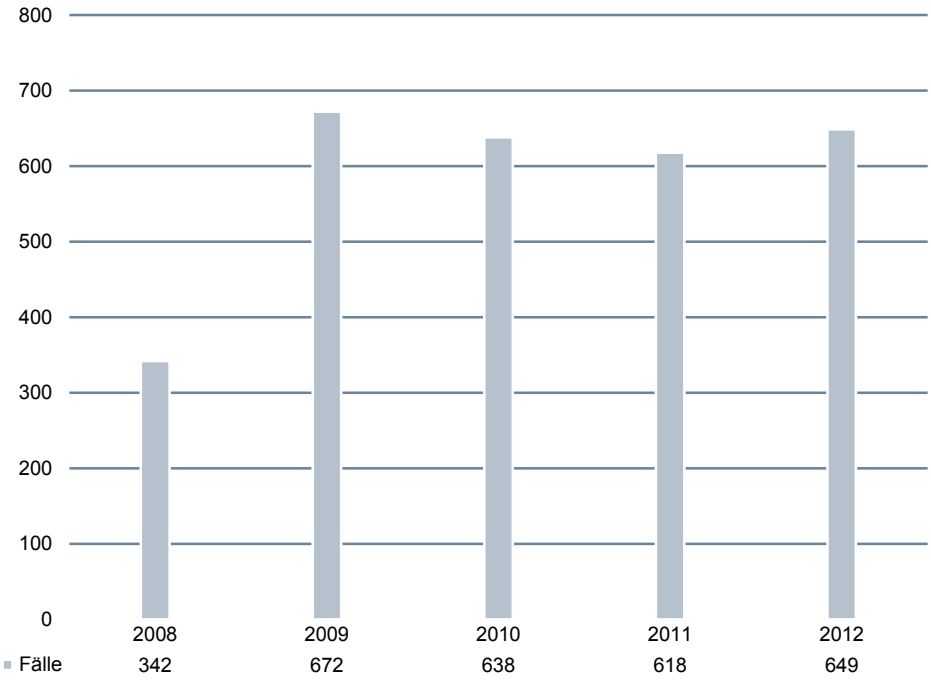


	2008	2009	2010	2011	2012
Fälle	828	1.242	1.444	1.343	1.346

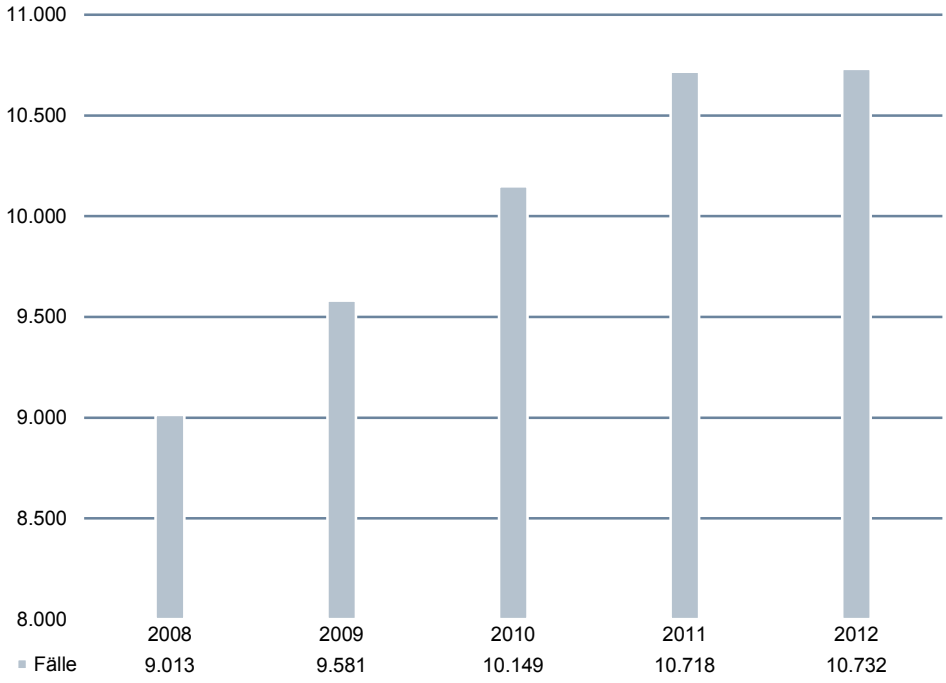
11 | **DATENVERÄNDERUNG – COMPUTERSABOTAGE 2008 BIS 2012**



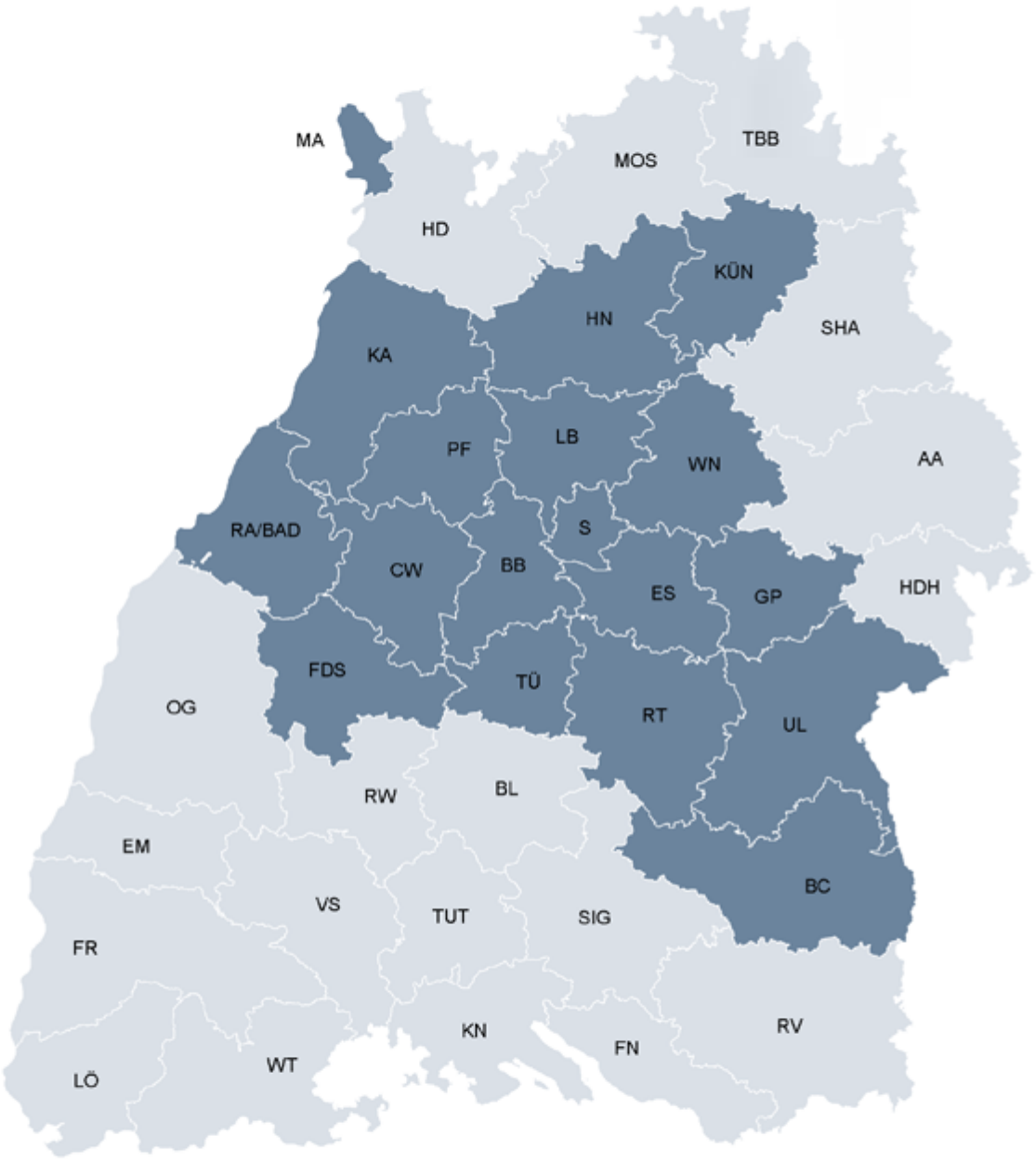
12 | **FÄLSCHUNG BEWEISERHERBLICHER DATEN – TÄUSCHUNG IM RECHTSVERKEHR 2008 BIS 2012**



13 | IT-BEWEISSICHERUNG – ENTWICKLUNG DER NEUEN AUFTRÄGE – LANDESWEITE ÜBERSICHT



14 | FISBW – LANDESWEITE ÜBERSICHT (STAND NOVEMBER 2012)



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.*
Bots, Botnetze/Botnet, Command & Control-Server, Zombie-PC	*Unter einem Bot (vom 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. 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.*
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. 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 Verfahren des Cyberwar umfassen verschiedene Straftatbestände bzw. Modi Operandi wie Spionage, DDoS-Attacken aber auch materielle Angriffe (Zerstörung, Sabotage etc.). Auf physikalischer Ebene hingegen werden insbesondere Kampfmittel verwendet, die auf Strahlungsemission beruhen und hierdurch elektronische Geräte stören, etwa EMP-Waffen (elektromagnetischer Impuls).*

Datenarten (Bestandsdaten, Verkehrsdaten und Inhaltsdaten)	***Bestandsdaten*** *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 hinterlegt (z. B. Adresse, Kontoverbindungen, Kopien, Personalausweisdaten etc.). Welche Auskünfte der Provider geben muss, ist in § 11 TKG geregelt.* ***Inhaltsdaten*** *Alle tatsächlich übertragenen Daten, die nicht lediglich reine Verbindungs- und Steuerungsfunktion haben, z. B. der Inhalt von Telefongesprächen.* ***Verkehrsdaten*** *Daten nach § 3 Nr. 30 TKG, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden (z. B. 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, ergeben sich aus § 96 TKG.*
Datengrössen/ Digitale Masseinheiten	*Ausgangsgröße ist das Byte. Größere Mengen werden mittels einer Zehnerpotenz dargestellt:* *1 Kilobyte (KB) sind 10^3 Byte = 1.000 Byte* *1 Megabyte (MB) sind 10^6 Byte = 1.000.000 Byte* *1 Gigabyte (GB) sind 10^9 Byte = 1.000.000.000 Byte* *1 Terabyte (TB) sind 10^{12} Byte = 1.000.000.000.000 Byte* *1 Petabyte (PB) sind 10^{15} Byte = 1.000.000.000.000.000 Byte* *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 der Cyberkriminalität kann in vielerlei Ausprägungen stattfinden. Strafrechtlich relevant ist vor allem das „Ausspähen von Daten" (§ 202a StGB).*
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.* *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.*
Drive-by-Download	*Bereits beim Betrachten von malwareverseuchten Webseiten kann sich der ungeschützte Anwender Schadprogramme einfangen. Da die Seiten zum Betrachten auf den Rechner geladen werden, können bei diesem Vorgang unbemerkt Schadprogramme installiert (drive-by bedeutet im Vorbeifahren) werden.*

Exploit, Zero-Day-Exploit	*Exploits sind Programme oder Skripte und nutzen gezielt Schwachstellen, Sicherheitslücken oder Programmierfehler in Programmen aus. Das Ziel ist meist eine Manipulation, um sich zu Ressourcen Zugang zu verschaffen oder Systeme zu beeinträchtigen. Ein Exploit, das vor oder am selben Tag erscheint, an dem die Sicherheitslücke allgemein bekannt wird, nennt man Zero-Day-Exploit.*
Filehoster	*Als Filehoster werden Internetdienstanbieter bezeichnet, bei denen der Anwender Dateien unmittelbar mit oder ohne vorherige Anmeldeprozedur speichern oder herunterladen kann.*
(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.*
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. In einem 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.*
IMEI	*IMEI steht für International Mobile Station Equipment Identity und ist die 15-stellige individuelle Seriennummer eines Mobiltelefons.*
IMSI	*IMSI steht für 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.*
Kernbereichsschutz	*Das BVerfG hat entschieden (Entscheidung vom 27. Juli 2005, BVerfG 113, 348 ff.), dass es einen höchstpersönlichen Lebensbereich geben muss, der besonders vor staatlichen Eingriffsmaßnahmen geschützt wird. In den sogenannten Kernbereich privater Lebensgestaltung fallen bspw. Äußerungen über das Intimleben, Ausdrucksformen der Sexualität, intensiv geäußerte Glaubensüberzeugungen und ärztlichen Beratungsgespräche. Nicht zum Kernbereich gehören alle Kommunikationsinhalte, die in unmittelbarem Bezug zu begangenen und bevorstehenden strafbaren Handlungen stehen, auch wenn diese mit kernbereichsbezogenen Inhalten verknüpft werden, um eine Überwachung zu erschweren oder zu verhindern. Des Weiteren fallen Gespräche über geschäftliche Angelegenheiten und schlichte Privatgespräche, zum Beispiel auch über Liebes- und Beziehungsangelegenheiten Dritter, nicht unter den Kernbereichsschutz. Das Gericht hat entschieden, dass der Staat Vorkehrungen treffen muss, dass Kommunikationsinhalte des höchstpersönlichen Bereichs nicht gespeichert und verwertet werden dürfen und dass eine unverzügliche Löschung erfolgen muss, wenn es ausnahmsweise zu ihrer Erhebung gekommen ist. Diese Vorgaben des BVerfG sind im LKA BW umgesetzt.*
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).*
Live Forensik (Online-Forensik)	*Die IT-Forensik lässt sich in die Post-mortem-Analyse (auch Offline-Forensik) und die Live-Forensik (auch Online-Forensik) einteilen. Das Unterscheidungskriterium liegt bei dieser Betrachtung auf dem Zeitpunkt der Untersuchung. Bei der Post-mortem-Analyse (lat. „nach dem Tod") werden Spuren im Anschluss an einen Vorfall untersucht (in der Regel anhand von Datenträgerabbildern, sog. Images), während bei der Live Forensik die Untersuchung evtl. schon während des relevanten Vorfalls, zumindest aber noch am laufenden System erfolgt. Bei der Live-Forensik steht insbesondere die Sicherung flüchtiger Daten im Vordergrund, also Daten, die beim Ausschalten des Systems verloren gehen. Dies sind in erster Linie Daten im Arbeitsspeicher, Informationen zu laufenden Prozessen oder Dienste, verschlüsselte Daten, die während der Laufzeit entschlüsselt sind oder bestehende Verbindungen des Systems innerhalb eines Netzwerks.*
Logdatei	*Eine Logdatei dient der Aufzeichnung/Niederlegung aller oder einzelner Aktionen von Prozessen im Computersystem. Häufig eine automatisch erstellte Datei (z. B. im Bereich Datenveränderungen).*

MAC-Adresse	*MAC steht für Media-Access-Control-Adresse und ist eine einmalig genutzte Hardware-Adresse von Geräten (je nach System auch als ID oder physikalische Adresse bezeichnet). Mittels der MAC-Adresse können Geräte in einem Netzwerk eindeutig identifiziert werden. Durch Einsatz eines MAC-Filters erhalten Geräte nur dann Zugang zum Netzwerk, wenn sie in der Filtertabelle eingetragen sind. Zu beachten ist jedoch, dass MAC-Adressen von Angreifern gefälscht werden können.*
Man-in-the-Middle (Angriffsform)	*Ein Man-in-the-middle-Angriff (MITM-Angriff), auch Mittelsmannangriff oder Janusangriff (nach dem doppelgesichtigen Janus der römischen Mythologie) genannt, ist eine Angriffsform, die in Rechnernetzen ihre Anwendung findet. Der Angreifer steht dabei entweder physikalisch oder heute meist logisch zwischen den beiden Kommunikationspartnern und hat dabei mit seinem System vollständige Kontrolle über den Datenverkehr zwischen zwei oder mehreren Netzwerkteilnehmern. Dadurch kann er Informationen nach Belieben einsehen oder gar manipulieren.* *Ein typischer Fall der MITM ist das Zwischenschalten bei Kommunikationsvorgängen im Bereich Onlinebanking. Dadurch erhält der Täter die notwendigen PIN-/TAN-Daten vom Opfer (Bankkunden), um Überweisungen zu (ver-)fälschen bzw. auf sich oder Dritte, sogenannte „Finanzagenten", umzuleiten.*
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 für Mobile Communications)* *GSM ist ein Standard für Mobilfunknetze. Er wird hauptsächlich für Telefonie genutzt. Zudem ermöglicht er die Übertragung von Kurzmitteilungen.* *UMTS (Universal Mobile Telecommunations System)* *UMTS ist ein Standard für Mobilfunk der dritten Generation (3G). Im Vergleich zu GSM sind deutlich höhere Datenübertragungsraten möglich.* *LTE (Long Term Evolution)* *Mobilfunkstandard der vierten Generation, der beispielsweise eine Downloadrate von bis zu 300 MBit/Sekunde erlaubt und damit UMTS nochmals übertrifft.*

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. 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.*
Pharming	*Als Pharming wird eine Manipulation der Hostdatei von Webbrowsern bezeichnet, um Anfragen auf gefälschte Webseiten umzuleiten. Es handelt sich um eine Weiterentwicklung des klassischen Phishings. Pharming-Betrüger unterhalten eigene große Server-Farmen, auf denen gefälschte Webseiten abgelegt sind. Pharming hat sich auch als Oberbegriff für verschiedene Arten von DNS-Angriffen etabliert. Das Domain Name System (DNS) ist einer der wichtigsten Dienste im IT-Netzwerk. Seine Hauptaufgabe ist die Beantwortung von Anfragen zur Namensauflösung (Zuordnung der eingegebenen URL zur entsprechenden IP-Adresse). Bei einem derartigen Angriff auf die Host-Datei wird unter Zuhilfenahme eines Trojanischen Pferdes oder eines Virus eine gezielte Manipulation des Systems vorgenommen. Die Folge davon ist, dass von diesem System nur noch gefälschte Webseiten abrufbar sind, selbst wenn die Web-Adresse korrekt eingegeben wurde. Gibt das Opfer Daten auf der gefälschten Webseite ein, kann der Täter die Daten für Missbrauchshandlungen und Identitätsdiebstahl verwenden.*
Phishing	*Phishing bedeutet übersetzt das „Fischen nach persönlichen Daten des Internetnutzers". Der Phisher schickt seinem Opfer in der Regel offiziell wirkende Schreiben, wie beispielsweise E-Mails, 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 (z. B. Kontextmenü, das mittels rechter Maustaste in vielen Programmen aufgerufen werden kann) oder unerwünscht (z. B. 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 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, z. B. 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, Malware	*Sammelbegriff für Computerprogramme, die unerwünschte, schädliche oder zerstörende Funktionen haben. Der Begriff Malware ist dabei eine Wortschöpfung aus den 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 legt, während klassische Mobiltelefone den Schwerpunkt auf Telefonie und Dienste zur einfachen Nachrichtenübermittelung (z. B. SMS) legen.*
Spam	*Als Spam-Mail werden unerwünscht übertragene Nachrichten bezeichnet. Der Inhalt reicht von lästiger Werbung über Phishing-Mails bis hin zur Übersendung von Malwaren (häufig in Anlagen integriert, die beim absichtlichen oder versehentlichem Öffnen Schadsoftware auf den Rechner übertragen).*

Spyware	*Diese Art von Software forscht bzw. spioniert (engl. 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 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.*
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 sog. 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 etc.) 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.* *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.* *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.*
Web 2.0 (-Dienste), Social Media/ Soziale Medien	*Der Begriff Web 2.0 entwickelte sich Anfangs des 21. Jahrhunderts. Bis in die 1990er Jahre war das Internet, dessen Inhalte und andere Dienste vorwiegend geprägt durch Informationen, die von zentralen Stellen (z. B. Firmen oder Behörden) erstellt und die von den Internetnutzern aufgerufen wurden. Im Mittelpunkt des Web 2.0 stehen Beteiligung und Zusammenarbeit. Der Nutzer ist nicht nur Konsument und nimmt die Informationen auf, sondern er erschafft eigene Informationen und stellt Inhalte zur Verfügung. Der Begriff Web 2.0 wird zunehmend durch den Begriff Soziale Medien bzw. Social Media verdrängt.* *Beispiele sind Wikis (Informationsseiten, Enzyklopädien), Blogs (Online-Tagebücher), Podcasts (Audio- und Videodateien) und Soziale Netzwerke.*
(Computer)Wurm	*Würmer ähneln Viren und verbreiten sich direkt über Netzwerke wie das Internet, Firmenintranets, Peer-to-Peer-Netzwerke aber auch Wechselmedien. Zielrichtung eines Wurms ist dabei die schnelle (weltweite) Verbreitung.*

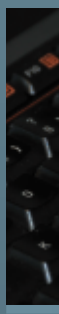
ANSPRECHPARTNER

ANSPRECHPARTNER FÜR FACHFRAGEN

ZENTRALE ANSPRECHSTELLE CYBERCRIME (ZAC)

Name	Jürgen Fauth, Heike Deringer, Saskia Lehmann
Telefon	0711 5401-2444
E-Mail	cybercrime@polizei.bwl.de

CYBERKRIMINALITÄT / DIGITALE SPUREN



2012

60 JAHRE

LANDESKRIMINALAMT
Baden-Württemberg