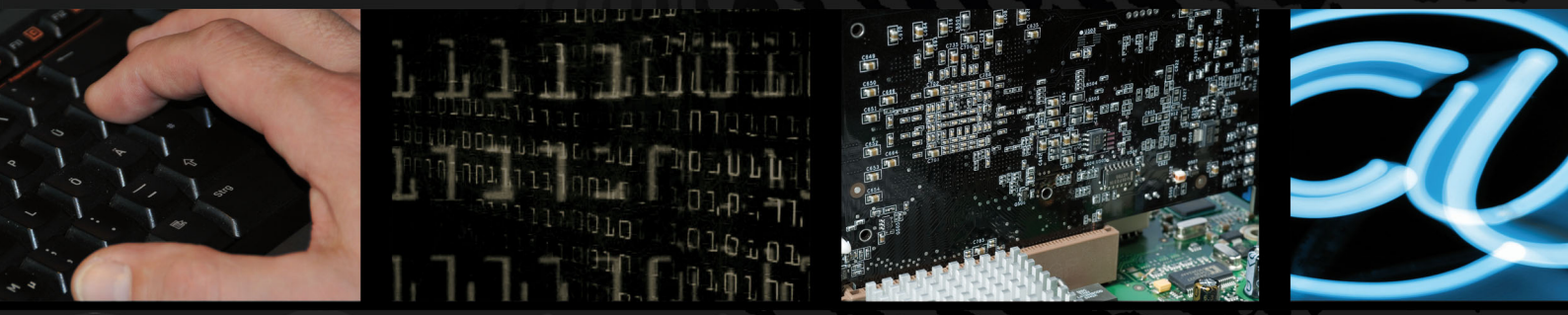


2011

LKA BW

IuK-Kriminalität

JAHRESBERICHT 2011

Baden-Württemberg

LANDESKRIMINALAMT

IMPRESSUM

IUK-KRIMINALITÄT

JAHRESBERICHT 2011

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

Druckerei Mack GmbH,
Schönaich

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

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

Untersagt ist auch die Weitergabe an Dritte zum Zwecke der Wahlwerbung.
Auch ohne zeitlichen Bezug zu einer Wahl darf die vorliegende Druckschrift nicht so verwendet werden, dass dies als Parteinahme 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.

IUK-KRIMINALITÄT

	2010	2011	
GESAMT	**32.249**	**30.036**	↘ **- 6,9 %**
COMPUTERKRIMINALITÄT	9.755	9.048	↘
INTERNETKRIMINALITÄT	22.494	20.988	↘
COMPUTERBETRUG	4.318	4.194	↘
VERBREITUNG VON KINDERPORNOGRAPHIE	221	162	↘

INHALT

1 ANALYSEDARSTELLUNG

MODERNE KOMMUNIKATION UND NUTZUNG DES INTERNET

Das Internet und die modernen Informations- und Kommunikationstechnologien gehören mittlerweile zum Alltag. Obwohl das Internet, wie wir es heute kennen, erst seit rund 20 Jahren existiert, sind nach einer aktuellen Studie des Bundesverbands Informationswirtschaft, Telekommunikation und neue Medien e. V. (BITKOM) über die sogenannte „Netzgesellschaft“[1] bereits 51 Millionen Bundesbürger regelmäßig online. Dies entspricht einem Anteil von 72 % aller Personen ab 14 Jahren in Deutschland.

Die Kommunikation in der Gesellschaft hat sich grundlegend verändert. Soziale Netzwerke sind inzwischen ein wesentlicher, sich dynamisch entwickelnder Teil der neuen Informations- und Kommunikationskultur. Derzeit sind bei Facebook weltweit ca. 775 Millionen Mitglieder registriert. Pro Sekunde kommen acht neue hinzu. Bei dem Kurznachrichtendienst Twitter werden pro Tag etwa 140 Millionen Nachrichten versandt. Auf der Videoplattform Youtube werden zwei Milliarden Videofilme täglich konsumiert. Pro Minute werden 35 Stunden Filmmaterial hochgeladen.

Für die meisten Deutschen ist ein Leben ohne Internet mittlerweile nahezu undenkbar, jeder zweite informiert sich über das Netz. Selbst die Altersgruppe der Senioren hat in den letzten Jahren aufgeholt. Ein Viertel der Bundesbürger ab 65 Jahren ist inzwischen online.

Neue Geräte zur Internetnutzung gewinnen mehr und mehr an Bedeutung. 24 % der Deutschen nutzen Laptop, Tablet-PC oder PDA[2] und 18 % auch Mobiltelefone, um Internetdienste nutzen zu können.

Mit der steigenden Nutzung des Internets nimmt die Gefahr zu, Opfer von IuK-Kriminalität zu werden. Laut einer BITKOM-Umfrage haben bereits 70 % aller deutschen Internet-Anwender ab 14 Jahren schon einmal negative Erfahrungen im Netz gemacht. Damit einher geht daher auch die Angst, Opfer einer Straftat zu werden. Fühlten sich 2010 noch 75 % aller Internetnutzer bedroht, sind es im Berichtsjahr schon 85 %.

Mit Wirkung zum 1. Januar 2012 wurde die Organisation des Landeskriminalamtes Baden-Württemberg (LKA BW) fortentwickelt, um der rasant zunehmenden Bedeutung der IuK-Kriminalität mit gebündelten Ressourcen, professionell geschultem Personal und technischem Know-How begegnen zu können. Die neu eingerichtete Abteilung 7 Cyberkriminalität/Digitale Spuren bündelt die Aufgaben der bisherigen Inspektionen, die sich in unterschiedlichen Abteilungen befanden.

[1] *„Netzgesellschaft – Eine repräsentative Untersuchung zur Mediennutzung und dem Informationsverhalten der Gesellschaft in Deutschland“, BITKOM, 02.08.2011*

[2] *Personal Digital Assistant: kompakter, tragbarer Computer, der hauptsächlich für die persönliche Aufgaben-, Kalender- und Adressverwaltung benutzt wird.*

ANALYSEDARSTELLUNG

DEFINITION IUK-KRIMINALITÄT

Die IuK-Kriminalität umfasst einerseits Internetkriminalität (IuK-Kriminalität im weiteren Sinne), darunter sind alle Straftaten zu subsumieren, die mit dem Tatmittel Internet begangen werden und andererseits Computerkriminalität (IuK-Kriminalität im engeren Sinne), also alle Straftaten, bei denen EDV in den Tatbestandsmerkmalen der Strafnorm genannt ist.

INTERNETKRIMINALITÄT (IUK-KRIMINALITÄT IM WEITEREN SINNE)

Die Internetkriminalität weist im Berichtsjahr 2011 entgegen dem Trend der Vorjahre mit 20.988 (22.494)[3] Fällen erstmals einen Rückgang von 6,7 % auf. Dieser ist vor allem geprägt durch die 2011 auf 16.220 (18.236) Fälle deutlich gesunkene Anzahl der Vermögens- und Fälschungsdelikte, was einem Rückgang von 11,1 % entspricht.

Ursächlich für diese Entwicklung ist der Deliktsbereich Warenbetrug, welcher um 28,5 % (- 2.220 auf 5.563 Fälle) zurückgegangen ist. Im 5-Jahres-Vergleich sind die Fallzahlen des Warenbetrugs bis 2009 (auf 8.965 Fälle) angestiegen und seither rückläufig. Warenbetrug wird maßgeblich durch umfangreiche Ermittlungsverfahren im Zusammenhang mit Auktionsplattformen bestimmt, die häufig mehrjährige Tatzeiträume betreffen. Im Jahr 2010 wurden im Gegensatz zu 2011 mehrere Großverfahren mit hohen Fallzahlen abgeschlossen.

Ohne Berücksichtigung des Warenbetruges ist die Internetkriminalität im Vergleich zu 2010 um 4,9 % (+ 714 auf 15.425 Fälle) gestiegen, darunter der Warenkreditbetrug mit 9,4 % (+ 195 auf 2.260 Fälle) und die Geldwäsche mit 43,2 % (+ 172 auf 570 Fälle).

Der bereits in den letzten Berichtsjahren festgestellte Rückgang bei Verstößen gegen das Urheberrechtsgesetz (UrhG) hat sich weiter fortgesetzt. Dies ist hauptsächlich auf das Auskunftsrecht der Rechteinhaber zurückzuführen, das im Jahr 2008 durch den Gesetzgeber verbessert wurde[4]. Im Jahr 2011 wurde ein Rückgang um 19,4 % auf 788 (978) Fälle registriert.

Dagegen ist im Jahr 2011 eine erhebliche Zunahme beim Besitz/Verschaffen kinderpornographischer Schriften um 21,2 % auf 468 (386) Fälle festzustellen. Im Teilbereich der Straftaten mit Tatmittel Internet stiegen die Fallzahlen um 16,8 % auf 327 (280) Fälle. Die Verbreitung von Kinderpornographie hingegen ging um 26,7 % von 221 auf 162 Fälle und die Straftaten mit Tatmittel Internet um 44,7 % auf 94 (170) Fälle im Jahr 2011 zurück. Die Entwicklung beider Bereiche bewegt sich mit 630 Fällen jedoch auf dem Niveau der Vorjahre (2010: 607, 2009: 652).

[3] *Vorjahreszahlen in Klammern*

[4] *Gesetz zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums vom 11. April 2008.*

Die Ansprechstelle Kinderpornographie der Fachinspektion 710 IuK-Kriminalität des LKA BW bearbeitete im Jahr 2011 insgesamt 63 Sammelverfahren (sog. Umfangsverfahren) mit 214 Tatverdächtigen. Im Vergleich zum Vorjahr sind die Zahlen der Ermittlungsverfahren wie auch die der Tatverdächtigen (2010: 71 Operationen (OP) mit 633 Tatverdächtigen) gesunken und liegen somit wieder auf dem Niveau des Jahres 2009 (57 Sammelverfahren mit 167 Tatverdächtigen).

Die Entwicklung der Internetkriminalität wird im LKA BW sowohl in der Inspektion 710 IuK-Kriminalität als auch in der Inspektion 440-Wirtschaftskriminalität verfolgt. Es wird deshalb ergänzend auf die Ausführungen im Jahresbericht Wirtschaftskriminalität verwiesen.

ZUGANGSERSCHWERUNGSGESETZ

Das Gesetz zur Erschwerung des Zugangs zu kinderpornographischen Inhalten in Kommunikationsnetzen (ZugErschwG) aus dem Jahr 2010 wurde per Gesetz zum Dezember 2011 aufgehoben. Wesentliche Gründe für das Scheitern des Gesetzes waren die nicht zu überwindenden politischen Hürden in der Diskussion über das Sperren oder Löschen von kinderpornographischen Internetseiten. Beim Sperren, dem sog. Access-Blocking, handelt es sich um eine Verweigerung des Zugriffs auf Seiten mit diesen Inhalten. Die technische Umsetzung sollte durch die Provider innerhalb Deutschlands erfolgen. Dadurch wären entsprechende Internet-Seiten blockiert bzw. die Anfrage des Kunden nicht weitergeleitet worden. Stattdessen wäre ein Stopp-Schild mit einem Warnhinweis erschienen.

Im Koalitionsvertrag der Bundesregierung wurde die Evaluation des Themas „Löschen vor Sperren“ vereinbart und auf ein Jahr[5] festgesetzt. In dieser Zeit wurden die Löschbemühungen seitens des Bundeskriminalamts national sowie international vorangetrieben.
Im Ergebnis zeigte sich, dass durch die Anstrengungen des Bundeskriminalamts (BKA) sowie der Länderpolizeien die Online-Verfügbarkeit der zu beanstandenden Inhalte verringert werden konnte. Die Intensivierung der nationalen sowie internationalen Kooperation und Sondervereinbarungen mit Diensteanbietern und Providern trugen maßgeblich mit zu diesem Ergebnis bei.
Es bleibt weiterhin ein wichtiges Ziel polizeilicher Arbeit, die Online-Verfügbarkeit von Webseiten mit kinderpornographischen Inhalten zu reduzieren.

[5] *Einjahreszeitraum von Januar 2010 bis Januar 2011*

ANALYSEDARSTELLUNG

ARBEITSBEREICH INTERNETRECHERCHE (AIR)

Im Berichtsjahr initiierte der AIR des LKA BW, Inspektion 710, zur Bekämpfung des Besitzes und der Verbreitung kinderpornographischer Darstellungen über das Internet weltweit insgesamt 8.164 (1.111) Ermittlungsverfahren. Hinsichtlich der Anzahl der ermittelten Tatverdächtigen liegen ausschließlich Daten zu Ermittlungsverfahren vor, die sich auf einen Tatort in Deutschland bezogen, da Auslandsstraftaten derzeit nicht in der PKS erfasst werden. Registriert wurden dabei 212 Tatverdächtige.

VORRATSDATENSPEICHERUNG

In allen Fällen des Besitzes oder der Verbreitung von Kinderpornographie werden unverzüglich Bestandsdatenanfragen durchgeführt. Von den deutschen Providern wurden aufgrund des Urteils des Bundesverfassungsgerichts zur Vorratsdatenspeicherung durchschnittlich 31 % der Anfragen nicht beauskunftet, d. h. es konnte kein Inhaber der angefragten IP-Adresse mitgeteilt werden. Im Jahr 2009 lag die Quote an nichtbeantworteten Auskunftsersuchen bei 9 %.

Unmittelbar nach Bekanntwerden des Urteils des Bundesverfassungsgerichts stellten viele Internet Service Provider die Beauskunftung von Anfragen i. S. d. § 113 Telekommunikationsgesetz (TKG) ein. Diese restriktive Haltung lockerte sich in der Zeit danach wieder. Auch bestehen bei Live-Auskünften, d. h. bei Auskünften, die im Rahmen der OP noch durchgeführt werden, während der Tatverdächtige noch online ist, inzwischen wieder höhere Aussichten auf eine Beauskunftung durch die Internet Service Provider. Hinzu kommt, dass ein Provider, der überwiegend in Hessen und Nordrhein-Westfalen vertreten ist, inzwischen zumindest teilweise Bestandsdatenanfragen beantwortet. Außerdem haben einige Internet Service Provider inzwischen die sog. Zwangstrennung abgeschafft, so dass mögliche Täter über einen längeren Zeitraum mit derselben IP-Adresse online sind. Dies erhöht die Chancen einer Beauskunftung.

Der Besitz sowie die Verbreitung von Kinderpornographie ist nur ein Deliktsbereich, der deutlich die grundsätzliche Notwendigkeit der Vorratsdatenspeicherung belegt. Es sollte nicht von der Bereitschaft der Provider zur Beauskunftung von Bestandsdaten abhängen, ob weitere Ermittlungshinweise erlangt werden können oder nicht. Vielmehr ist eine allgemeingültige gesetzliche Regelung zu schaffen. Ohne die Möglichkeit, in schweren Straftaten auf die Vorratsdatenspeicherung zurückzugreifen, besteht die Gefahr, dass rechtsfreie Räume im Internet entstehen und den Strafverfolgungsorganen mangels gesetzlicher Neuregelung die Hände gebunden sind.

Das Bundesjustizministerium hat im Berichtsjahr 2011 vor dem Hintergrund eines drohenden Strafverfahrens der EU-Kommission wegen der Nichteinhaltung der Frist zur Neuregelung der Vorratsdatenspeicherung (Fristablauf am 27. Dezember 2011 eingetreten) einen Gesetzentwurf zum sogenannten Quick-Freeze-Verfahren in die Ressortabstimmung gegeben.
Beim Quick-Freeze-Verfahren sollen die Verkehrsdaten, welche die Telekommunikationsunternehmen ohnehin zu geschäftlichen Gründen speichern, anlassbezogen gesichert („eingefroren") werden. In einer zweiten Stufe können sie dann mit Zustimmung eines Richters den Strafverfolgungsbehörden zur Verfügung gestellt („aufgetaut") werden. Für die Verfolgung von Straftaten im Internet soll eine kurze Datenspeicherung von sieben Tagen möglich gemacht werden, damit bei einem konkreten Verdacht dynamische IP-Adressen Personen zugeordnet werden können (Quelle: http://www.bmj.de). Dieses Verfahren wird nicht zuletzt wegen der Vorgänge um die rechtsterroristische Vereinigung „Nationalsozialistischer Untergrund" zwischen den Regierungsparteien kontrovers diskutiert. Mit einem Gesetzentwurf dürfte ggf. aufgrund des drohenden EU-Verbotsverfahrens im Jahr 2012 zu rechnen sein.

SOZIALE NETZWERKE

Im Rahmen einer durch den AIR durchgeführten Umfrage zum Problem der Bewältigung von Einsatzlagen der sog. „Facebook-Parties" meldeten die Dienststellen im Berichtsjahr rund 40 dieser Veranstaltungen mit ca. 10.000 Teilnehmern. Die Veranstaltungen stellen die Behörden und Organisationen mit Sicherheitsaufgaben, neben der Polizei bspw. auch Rettungsdienste und Feuerwehren, in Einzelfällen vor große Probleme.

COMPUTERKRIMINALITÄT (IUK-KRIMINALITÄT IM ENGEREN SINNE)

Die Computerkriminalität (IuK-Kriminalität im engeren Sinne) verzeichnet einen Rückgang um 7,2 % auf 9.048 (9.755) erfasste Fälle. Ursächlich hierfür ist u. a. die Anzahl der Delikte des Ausspähens von Daten (§ 202a StGB), die im vergangenen Jahr um 7,0 % von 1.444 auf 1.343 Fälle (1.444), gesunken sind.
Der Computerbetrug (§ 263a StGB) ist mit 2,9 % oder - 124 auf 4.194 Fälle (4.318) leicht rückläufig. Mit Ausnahme des Tatbestandes der Datenveränderung/Computersabotage ist bei allen Delikten eine geringe Abnahme zu verzeichnen.
Gegenläufig zur allgemeinen Entwicklung der Fallzahlen der Computerkriminalität ist der Trend beim verursachten Schaden. Dieser liegt bei 9.575.267 Euro und ist damit im Vergleich zum Vorjahr mit 9.374.777 Euro leicht um 2,1 % angestiegen.

Diese rückläufige Entwicklung der Fallzahlen der Computerkriminalität ist zum einen auf Großverfahren, welche bei einigen Dienststellen im Jahr 2010 anhängig waren, zurückzuführen. Zum anderen wurden im Jahr 2011 von Kreditinstituten vermehrt die Einführung neuer Sicherheitsstandards (mTAN-/chipTAN-Verfahren) betrieben, durch welche die Verwertung der erlangten Daten zusätzlich erschwert worden sein dürfte.

ARBEITSBEREICH ERMITTLUNGEN

Die aktuell beim LKA BW geführten Ermittlungsverfahren bestätigen die in den vergangenen Jahren bereits festgestellte Entwicklung einer qualitativen und quantitativen Veränderungen des Organisationsgrades der Täter und der von ihnen eingesetzten innovativen Techniken im Bereich der IuK-Kriminalität.

Die festgestellten Gruppierungen agieren international, bandenmäßig und teilweise in Strukturen der Organisierten Kriminalität. Diese Täter nutzen vermehrt sog. „Botnetze[6]“, um ihre kriminellen Ziele zu erreichen.

Ein immer größer werdendes Problem ist das Volumen der auszuwertenden Datenmenge. Neben der Anzahl und Speicherkapazität der sichergestellten Beweismittel steigt insbesondere bei Überwachungsmaßnahmen die auszuwertende Datenmenge stetig an. Für eine effektive Strafverfolgung sind deshalb fortwährende infrastrukturelle und technische Anpassungen notwendig. Diese entfalten jedoch nur ihre Wirkung, wenn für deren Entwicklung und Anwendung qualifiziertes Personal im erforderlichen Umfang verfügbar ist.

Über das Internet werden verschiedene Baukasten-Tools für kriminelle Zwecke inkl. Serviceleistungen angeboten. Waren bislang vor allem heimische Personal Computer (PC) Ziel krimineller Aktivitäten, wurden mittlerweile die ersten Schadsoftwarevarianten gegen Mobiltelefone (sog. Smartphones) bekannt. Durch den Einsatz von speziellen Trojanern sind nunmehr auch die mobilen Endgeräte gefährdet, von den Tätern für ihre Zwecke missbraucht zu werden.

Ferner werden durch Hackergruppierungen mit zunächst unbekannter Motivlage sowohl Privatunternehmen als auch Behörden angegriffen. Zum Teil geht es hierbei um Vergeltung für vermeintlich unerwünschte Verhaltensweisen oder Maßnahmen der Angegriffenen, zum Teil aber auch um die öffentlichkeitswirksame Demonstration, dass ein digitaler Angriff möglich ist. Zuletzt wurden Daten von Nutzern eines Kinderpornographietauschrings und Unterstützern rechtsextremer Organisationen bzw. Parteien ins Internet gestellt.

[6] *Als Botnetz bezeichnet man den Zusammenschluss einer Vielzahl infizierter Rechner zu einem Netzwerk. Die infizierten PC („sog. Zombie-PC“) werden über einen Rechner („Botmaster“) fremdgesteuert und zur Begehung von Straftaten genutzt.*

NEUES PHÄNOMEN: RANSOMWARE

Im Jahr 2011 konnten bundesweit verschiedene Modi Operandi der sogenannten „Digitalen Schutzgelderpressung“ festgestellt werden. Anhand der Inpol-Fall-Anwendung IuK, in der alle Straftaten des IuK-Meldedienstes[7] erfasst werden, ist diese Entwicklung nachvollziehbar. Die Erpressungen im Zusammenhang mit IuK-Delikten belaufen sich im Jahr 2011 auf insgesamt 2.899 (zwei) Fälle, welche allerdings nur zu einem kleinen Teil durch die bundesweit auftretenden DDoS-Attacken verursacht werden. Eine neue Begehungsweise der digitalen Schutzgelderpressung erlangte ab März 2011 unter der Bezeichnung „Ransomware“ („ransom“, englisch für Lösegeld) eine große Bedeutung. Diese Bezeichnung wird für Computerprogramme verwendet, die es einem Täter ermöglichen, Daten auf fremden Computern zu verschlüsseln oder die Benutzung des Computers auf andere Art und Weise zu verhindern. Ziel des Täters ist es, vom Geschädigten ein Lösegeld für die vermeintliche Entschlüsselung oder die Freigabe des Computersystems zu fordern. Die Infektion eines Rechners erfolgt dabei meistens durch entsprechend präparierte E-Mail-Anhänge oder durch das Aufrufen manipulierter Webseiten (sog. Drive-by-Download).

Von den insgesamt im Zusammenhang mit Erpressungsdelikten erfassten 2.899 Fällen können 2.654 Fälle gesichert einer Variante des Phänomens Ransomware zugeordnet werden. Die Fallzahlen im Bundesgebiet und in Baden-Württemberg stiegen dabei im Berichtszeitraum kontinuierlich an.
Dem Nutzer eines infizierten Rechners wird eine angeblich behördliche Mitteilung als Pop-up-Fenster eingeblendet. Durch verschiedene Logos der Bundespolizei und des BKA soll dieser behördliche Charakter untermauert werden. Dem eingeblendeten Text zufolge sollen von dem betroffenen Rechner u. a. pornographische, kinderpornographische und gewaltverherrlichende Inhalte aufgerufen worden sein. Deshalb sei der Rechner zur Vermeidung weiterer illegaler Aktivitäten gesperrt und könne gegen Zahlung einer Gebühr angeblich wieder freigeschaltet werden.
Mittlerweile wurden mehrere Varianten dieser Ransomware festgestellt, wobei noch unklar ist, ob diese Varianten ein und derselben Tätergruppe zuzuordnen sind. Es handelt sich hierbei zum einen um die Variante „Windows“, welche dem Nutzer die angeblich illegale Nutzung seiner privaten Windows-Betriebssystem-Version vorwirft. Zum anderen wurde die Variante „GEMA“ bekannt, welche dem Nutzer einen Verstoß gegen die Schutzrechte der GEMA mittels illegalen Herunterladens von Musikstücken anlastet.

Ransomware findet in vielen Fällen keinen Eingang in die Polizeiliche Kriminalstatistik (PKS), da das Tatortprinzip nach den PKS-Richtlinien vorsieht, keine Auslandsstraftaten zu erfassen. Eine Vielzahl

[7] *§ 202a StGB Ausspähen von Daten, § 202b StGB Abfangen von Daten, § 202c StGB Vorbereiten des Ausspähens und Abfangens von Daten, § 263a StGB Computerbetrug, § 269 StGB Fälschung beweiserheblicher Daten, § 270 StGB Täuschung im Rechtsverkehr bei Datenverarbeitung, §§ 271, 274 I Nr. 2, 348 StGB Falschbeurkundung/Urkundenunterdrückung im Zusammenhang mit Datenverarbeitung, § 303a StGB Datenveränderung, § 303b StGB Computersabotage.*

von Erkenntnissen führt in diesem Zusammenhang jedoch ins Ausland. Dies schließt daher eine Erfassung in der PKS aus. Ein Rückgriff auf die Inpol-Fall-Datei „IuK", in der durch den Meldedienst „IuK-Kriminalität" sämtliche Ransomware-Fälle erfasst werden, zeigt, dass im Jahr 2011 2.654 dieser Fälle für das Bundesland Baden-Württemberg Auslandsbezug hatten, aber nicht in die PKS eingeflossen sind. Eine entsprechende Abfrage im polizeilichen Informationssystem Baden-Württemberg (POLAS BW) führt zu einem annähernd gleichen Ergebnis. Hier werden für Straftaten mit dem Führungsdelikt „Erpressung", welche mit dem Sonderkenner „Internet" begangen wurden und deren Tatort im Ausland liegt, insgesamt 2.302 erfasste Fälle ausgewiesen, die somit nicht in die PKS eingehen. Zum Vergleich wurden in der PKS im Jahr 2011 lediglich 190 (27) Fälle der Erpressung mit Tatmittel Internet erfasst.

CYBERGROOMING

Neben den im sozialen Nahraum begangenen Sexualdelikten an Kindern und Jugendlichen kommt es auch immer wieder nach Kontaktanbahnungen über das Internet (sog. Cybergrooming) zu sexuellen Übergriffen.

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 im Jahr 2007 festgestellt, dass annähernd 38 % aller Befragten bereits zu ungewollter Kommunikation mit sexuellem Inhalt im Internet gedrängt wurden. 25 % wurden zur Beschreibung von sexuellen Handlungen aufgefordert und an fast 10 % wurde pornographisches Material gesandt.[8]

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

2 MASSNAHMEN / HANDLUNGSEMPFEHLUNGEN

BUND-LÄNDER-PROJEKT-GRUPPE „DEFINITION CYBERCRIME“

Die Kommission Kriminalitätsbekämpfung (KKB) richtete 2011 eine Bund-Länder-Projekt-Gruppe (BLPG) unter Beteiligung der Länder Baden-Württemberg, Bremen, Hessen, Niedersachsen, Nordrhein-Westfahlen, Thüringen unter der Federführung des Bundeskriminalamts (BKA) auf Leiterebene ein, um eine zukunftsfähige Bestimmung des Begriffs „Cybercrime“ zu erstellen. Dabei sollen nationale sowie internationale Sicherheitsstrategien und Definitionen berücksichtigt werden, um eine weitgehend einheitliche Nutzung des Begriffs zu ermöglichen. Darüber hinaus werden Empfehlungen zur Überarbeitung des Kriminalpolizeilichen Meldedienstes (KPMD), von INPOL-Fall und der Polizeilichen Kriminalstatistik erarbeitet.

SONDERLAUFBAHN IUK-KRIMINALIST

Die erfolgreichen Erfahrungen im Bereich der Sonderlaufbahn Wirtschaftskriminalist sollten Vorbild für die Schaffung einer Sonderlaufbahn IuK-Kriminalist sein.
Spezielles IuK-Fachwissen wird auf allen polizeilichen Ebenen dringend benötigt. Allein über polizeiinterne Qualifikation wird es aufgrund der Dynamik des Kriminalitätsfeldes IuK-Kriminalität bzw. Cyberkriminalität und der nachhaltig auf aktuellem Stand zu haltenden Kenntnisse dauerhaft nicht in ausreichendem Maß zu generieren sein. Die Einstellung von IuK-Kriminalisten sollte im gehobenen Dienst erfolgen. Einstellungsvoraussetzung ist ein Diplom-/Bachelorabschluss im Bereich der Informations- und Kommunikationstechnik. Wie bei der Sonderlaufbahn Wirtschaftskriminalist wird eine einjährige Basisausbildung mit theoretischen und praktischen Segmenten vorgeschlagen, die in Teilen gemeinsam mit den Wirtschaftskriminalisten erfolgen könnte.

VERBEAMTUNG VON IT-EXPERTEN

IT-Experten sollten künftig grundsätzlich im Beamtenverhältnis eingestellt werden. Abhängig vom jeweiligen Ausbildungsstand ist eine Einstellung sowohl im gehobenen als auch höheren Dienst vorzusehen. Die Möglichkeit des Aufstiegs in den höheren Dienst bei Erwerb einer weiterführenden Qualifikation (Master) ist zu prüfen.
Für die Entwicklung, Standardisierung und Fortschreibung von IT-Lösungen besteht ein Bedarf an IT-Experten. Es hat sich gezeigt, dass die Polizei für qualifizierte Informatiker grundsätzlich ein interessanter Arbeitgeber ist. Durch eine Verbeamtung ließe sich die Attraktivität des LKA BW erhöht werden.

AUSBAU DER FORTBILDUNG IM BEREICH CYBERKRIMINALITÄT

Die Fortbildungsmöglichkeiten sind mit Blick auf die notwendige Spezialisierung, die Nachhaltigkeit und stets neue Schulungserfordernisse auszubauen.
Es gibt zwar schon ein vielfältiges und differenziertes Fortbildungsangebot. Die bisherigen personellen Kapazitäten setzen aber einer zeitnahen, bedarfsorientierten und nachhaltigen Fortbildung enge Grenzen. Die Schulung zu der neuen Hauptauswertesoftware wird in naher Zukunft zudem erhebliche Kapazitäten binden. Hochtechnische Spezialthemen müssen über externe Referenten abgedeckt werden.

MASTERSTUDIENGANG „DIGITALE FORENSIK"

Seit dem Jahr 2010 wird durch die Hochschule Albstadt-Sigmaringen ein Masterstudiengang „Digitale Forensik" angeboten, der sich unter anderem auch gezielt an Polizeibeamte richtet.

ZENTRALE PROVIDERDATENBANK (ZPD)

Auf Anregung der Koordinierungsgruppe für anlassunabhängige Recherchen im Internet (KaRIn) und auf Basis der Beschlüsse der Kommission Kriminalitätsbekämpfung (KKB) der AG Kripo wurde die bundeseinheitliche Providerdatenbank unter der Bezeichnung „Zentrale Providerdatenbank (ZPD)" zum 1. August 2011 über Extrapol (http://zpd.extrapol.de/) in den Wirkbetrieb genommen. Die ZPD soll im Frühjahr 2012 evaluiert werden.

BEKÄMPFUNG DER KINDERPORNOGRAPHIE

Die beiden Tatbestände Besitz/Verschaffen und Verbreitung von Kinderpornographie müssen im Rahmen der Bearbeitung von Verfahren zusammen betrachtet werden. Ob ein Verfahren wegen der Verbreitung kinderpornografischer Schriften an die Staatsanwaltschaft vorgelegt werden kann, stellt sich zumeist erst nach der Auswertung aller Beweismittel heraus. Andernfalls wird die Strafanzeige wegen Besitz gefertigt.

EINFÜHRUNG EINER AUSWERTESOFTWARE

In zahlreichen polizeilichen Gremien[9] wurde festgestellt, dass zur effektiven Bekämpfung von Ermittlungsverfahren der Kinderpornographie und zur Bewältigung des Massenproblems der gesicherten Datenträger eine professionelle Auswertesoftware erforderlich ist. Um die psychischen Belastungen der Sachbearbeiter zu reduzieren, soll eine weitestgehend automatisierte Abarbeitung ermöglicht werden.
In der Folge wurde ein Konzept zur Realisierung einer landesweiten Ausstattung auf Basis von Regionalmodellen durch das LKA BW erarbeitet. Die ausgewählten Gerätekonfigurationen werden zum Jahresbeginn 2012 einsatzfähig sein.

[9] *Tagung Kriminalitätsbekämpfung, Tagung Polizeiliche Aufgaben, Steuerungskreis IuK-Kriminalität*

MASSNAHMEN

FAHNDUNGSMASSNAHMEN BEI UNBEKANNTEN BILDERSERIEN

Im Deliktsbereich des sexuellen Missbrauchs/Verbreitung von kinderpornographischen Schriften ist es oftmals notwendig, umfangreiche Identifizierungsmaßnahmen durchzuführen, um die Opfer und/oder den Täter zu ermitteln.
In Ausnahmefällen kann die Fahndung auch auf Personengruppen, die beruflich mit Kindern in Kontakt kommen, ausgeweitet werden. In bislang zwei Fällen wurden im Jahr 2011 Bilder der Opfer von sexuellen Missbräuchen weiterführenden Schulen im Bundesgebiet zugeleitet, um von Lehrkräften Erkenntnisse zur Identität der Opfer zu erlangen. Diese Vorgehensweise wird als weitere qualitativ hochwertige Option zur Gewinnung von Ermittlungsansätzen angesehen.

SOZIALE NETZWERKE – FACEBOOK-PARTIES

Als besondere Maßnahmen zur Bewältigung dieser neuartigen Veranstaltungsform kommen z. B. in Betracht:

- Erlass von gemeindlichen Verbotsverfügungen,
- Zwangsgeldandrohungen bei Nichtbefolgung der Rückrufaufforderung, polizeirechtliche Durchsuchungen und Beschlagnahmen,
- Veröffentlichungen von Informationen/rechtlichen Hinweisen durch die sachbearbeitende Polizeidienststelle auf der Facebook-Veranstaltungsseite,
- Gefährderansprachen beim Veranstalter,
- Kontaktaufnahmen mit den örtlichen Schulen, um innerhalb der Klassenverbände Problemstellungen aufzuzeigen,
- Befragungen der örtlichen Jugendszene.

Die Rechtsstelle beim BKA (KI 15) hat festgestellt, dass polizeiliche Anfragen bei ausländischen Diensteanbietern nicht von § 14 BKA-Gesetz, der die ausschließliche Datenübermittlung durch das BKA an ausländische staatliche Stellen regelt, umfasst sind. Dies bedeutet, dass vor jeder Anfrage, welche nicht wegen einer begründeten Gefahr für Leib und/oder Leben gestellt wird, eine Entscheidung der Staatsanwaltschaft zur Prüfung eines Rechtshilfeersuchens eingeholt werden sollte.

ERFASSUNG VON AUSLANDSSTRAFTATEN IN DER PKS

Das Problem der Auslandsstraftaten stieß in der polizeifachlichen Diskussion zunehmend auf Kritik, da Internetkriminalität aufgrund des grenzüberschreitenden Charakters des Internets eine Vielzahl von Tathandlungen, die sich im Inland auswirken, nicht in die Statistik eingehen. Die Kommission PKS (KPKS) ist aktuell beauftragt, die Erfassung von Auslandstaten in der PKS neu zu regeln.

CYBERGROOMING

Das LKA BW wird das Phänomen „Cybergrooming“ in die nächste Tagung der KaRIn am 28. März 2012 einbringen.

PRÄVENTION

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

ONLINE-ANGEBOTE DER POLIZEILICHEN KRIMINALPRÄVENTION DER LÄNDER UND DES BUNDES (PROPK) FÜR DIE BEVÖLKERUNG

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

Allgemeine Handreichung 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 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 der Polizeilichen Kriminalprävention der Länder und des Bundes (ProPK) mit dem Ziel, vor Betrug bei Onlinekäufen zu schützen und den Wissensstand über sicheren Online-Handel zu erhöhen:
http://www.kaufenmitverstand.de

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

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

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

ANLAGEN

3 ANLAGEN

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

DEFINITIONEN

IUK-KRIMINALITÄT

Die IuK-Kriminalität umfasst alle Straftaten, die unter Ausnutzung der Informations- und Kommunikationstechnik oder gegen diese begangen werden.

Im Zuge einer Angleichung des Sprachgebrauches in Europa setzt sich zunehmend, auch national, für die Bezeichnung IuK-Kriminalität der Begriff „Cybercrime/Cyberkriminalität“ durch. Damit geht jedoch keine Veränderung in der Aufbauorganisation oder Aufgabenzuweisung einher.

CYBERCRIME

Der Begriff Cybercrime beinhaltet Straftaten, die unter Ausnutzung des Internets begangen werden. Gemäß der am 01.07.2009 in Kraft getretenen „Cybercrime-Konvention“ des Europarates (Deutschland ratifizierte die EU-Konvention am 09.03.2009) sind die nachfolgenden Straftaten vom Begriff der Cybercrime umfasst:

1. Straftaten gegen die Vertraulichkeit, Unversehrtheit und Verfügbarkeit von Computerdaten und -systemen
2. Computerbezogene Straftaten (computerbezogene Fälschung und Betrug)
3. Inhaltsbezogene Straftaten (Kinderpornographie)
4. Straftaten im Zusammenhang mit Verletzungen des Urheberrechts und verwandter Schutzrechte
5. gemäß Zusatzprotokoll von 2006 mittels Computersysteme begangene Handlungen rassistischer und fremdenfeindlicher Art

INTERNETKRIMINALITÄT (IUK-KRIMINALITÄT IM WEITEREN SINNE)

Straftaten, die mit dem Tatmittel Internet begangen werden (z. B. Waren- und Warenkreditbetrug, Verstoß gegen UrheberrechtsG, Verbreitung pornographischer Schriften).

COMPUTERKRIMINALITÄT (IUK-KRIMINALITÄT 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 Abfangens von Daten	(§ 202c StGB)
-	Softwarepiraterie, privat und gewerbsmäßig	(UrhG)

ARBEITSBEREICH INTERNETRECHERCHE (AIR)

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

PKS-BAROMETER IUK-KRIMINALITÄT 2010 – 2011

	PKS-Schlüssel	2010	2011	in %	Tendenz
Computerbetrug (§ 263a StGB)	5175	4.318	4.194	-2,9	↘
Fälschung beweiserheblicher Daten (§ 269 StGB)/Täuschung im Rechtsverkehr (§ 270 StGB)	5430	638	618	-3,1	↘
Datenveränderung (§ 303a StGB)/ Computersabotage (§ 303b StGB)	6742	194	236	+21,6	↗
Ausspähen von Daten (§ 202a StGB)	6780	1.444	1.343	-7,0	↘
Computerkriminalität	8970	9.755	9.048	-7,2	↘

IUK-KRIMINALITÄT IM ENGEREN SINNE 2007 - 2011

Berichtsjahr	2007	2008	2009	2010	2011
Computerbetrug PKS 5175	2.436	2.208	3.375	4.318	4.194
Schadenssumme in Euro Computerbetrug	5.261.621	2.165.982	4.035.813	5.899.424	7.509.910
Fälschung beweiserheblicher Daten/Täuschung im Rechtsverkehr PKS 5430	405	342	672	638	618
Datenveränderung/ Computersabotage PKS 6742	197	212	141	194	236
Ausspähen von Daten PKS 6780	522	828	1.242	1.444	1.343
Computerkriminalität PKS 8970	6.549	6.324	8.363	9.755	9.048
Schadenssumme in Euro Computerkriminalität	7.593.768	4.176.110	6.201.261	9.374.777	9.575.267

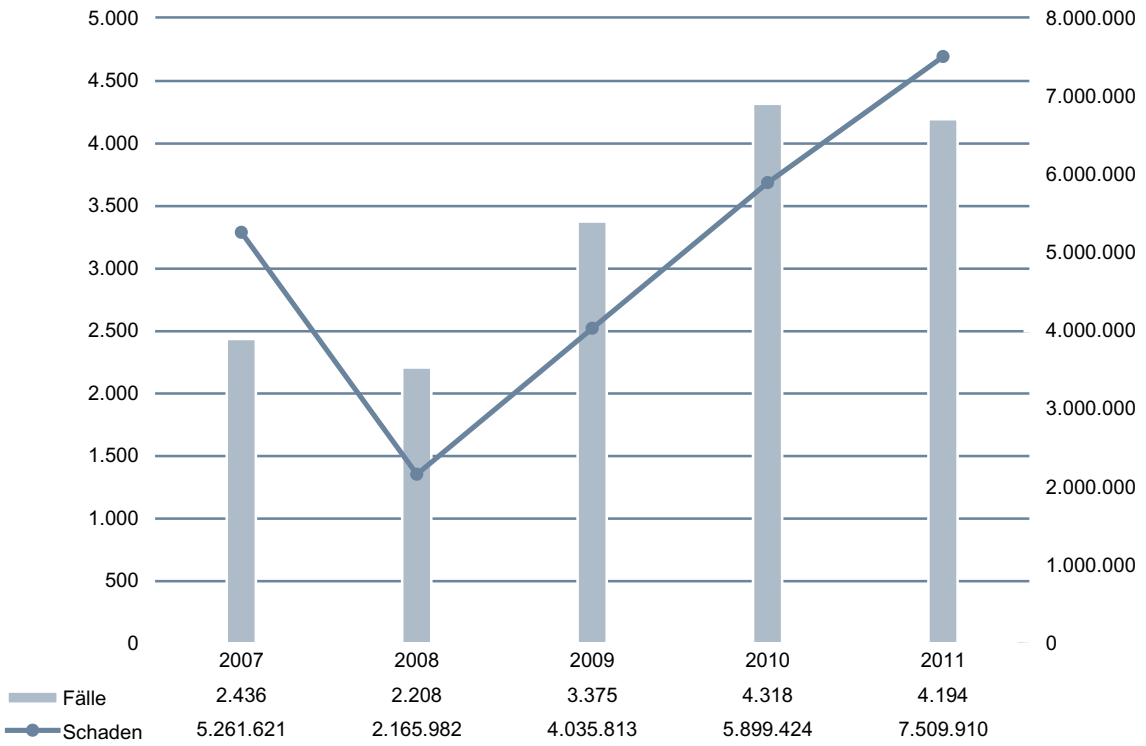
PKS-BAROMETER KINDERPORNOGRAPHIE 2010 – 2011

	PKS-Schlüssel	2010	2011	in %	Tendenz
Besitz/Verschaffen von Kinder-pornographie (§ 184b StGB)	1433	386	468	+21,2	↗
Verbreitung von Kinder-pornographie (§ 184b StGB)	1434	221	162	-26,7	↘

STRAFVERFAHRENINITIIERUNGEN ARBEITSBEREICH INTERNETRECHERCHE (AIR) 2007 - 2011

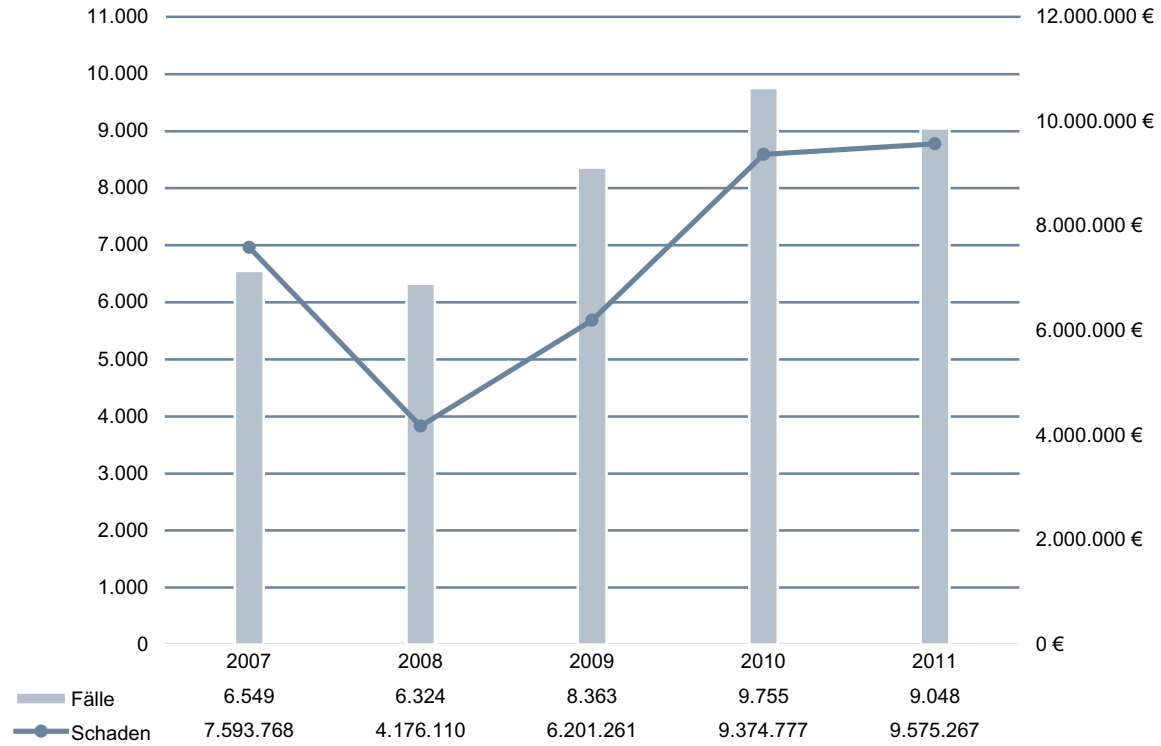
Berichtsjahr	2007	2008	2009	2010	2011
Deutschland	1.119	1.504	338	66	420
davon Baden-Württemberg	98	100	30	3	24
International	4.465	8.557	2.305	1.045	7.720
Gesamt	**5.584**	**10.061**	**2.643**	**1.111**	**8.164**

COMPUTERBETRUG 2007-2011



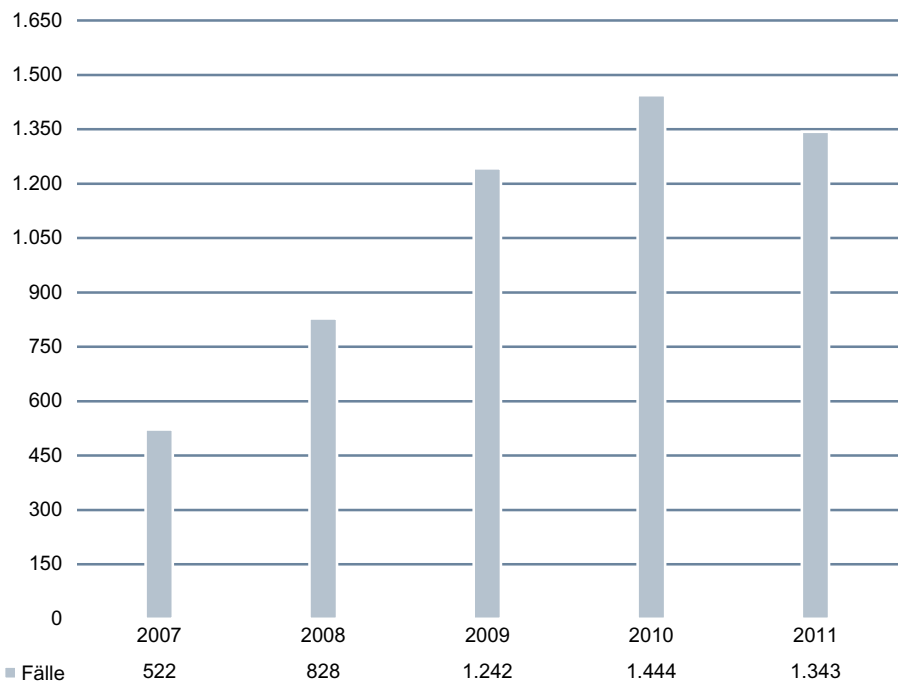
	2007	2008	2009	2010	2011
Fälle	2.436	2.208	3.375	4.318	4.194
Schaden	5.261.621	2.165.982	4.035.813	5.899.424	7.509.910

COMPUTERKRIMINALITÄT 2007-2011

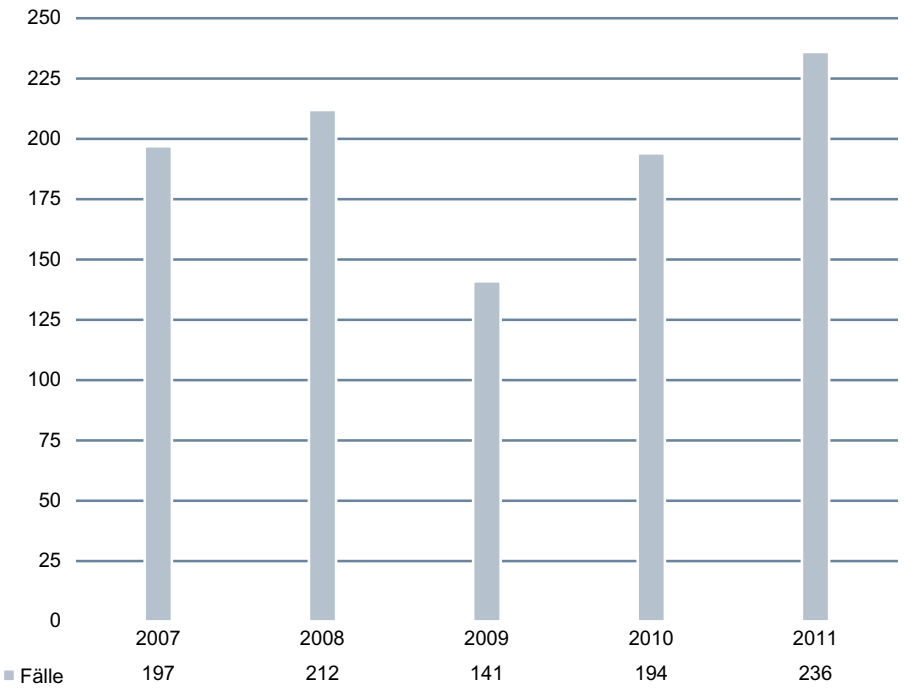


	2007	2008	2009	2010	2011
Fälle	6.549	6.324	8.363	9.755	9.048
Schaden	7.593.768	4.176.110	6.201.261	9.374.777	9.575.267

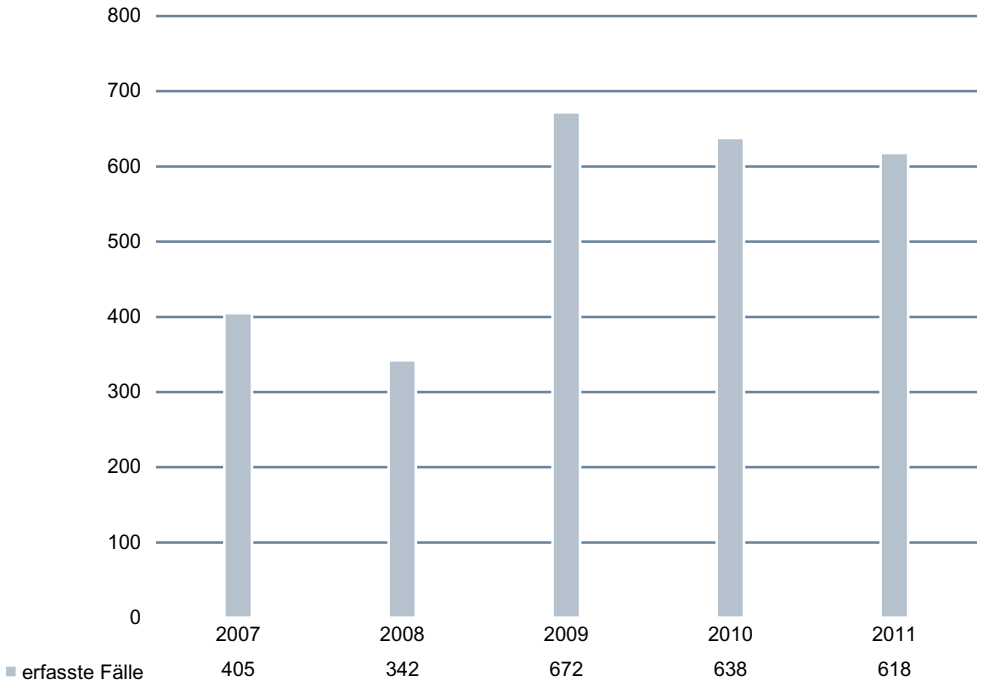
AUSSPÄHEN VON DATEN 2007-2011



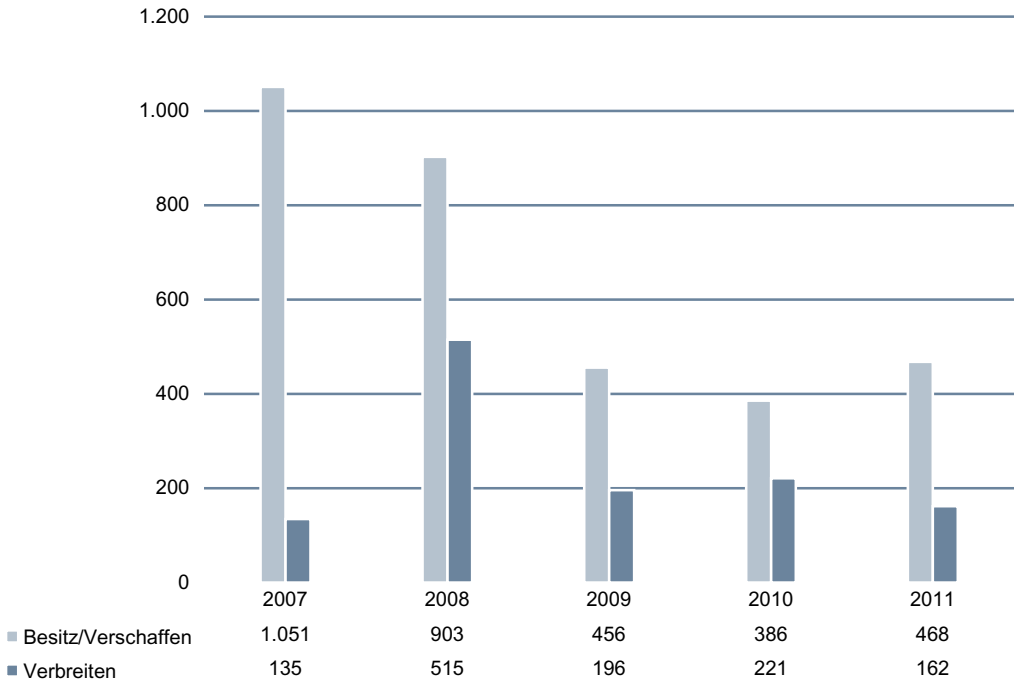
DATENVERÄNDERUNG – COMPUTERSABOTAGE 2007-2011



FÄLSCHUNG BEWEISERHEBLICHER DATEN – TÄUSCHUNG IM RECHTSVERKEHR 2007-2011



BESITZ / VERSCHAFFEN UND VERBREITEN VON KINDERPORNOGRAPHIE 2007 - 2011



	2007	2008	2009	2010	2011
Besitz/Verschaffen	1.051	903	456	386	468
Verbreiten	135	515	196	221	162

ANSPRECHPARTNER

ÖFFENTLICHKEITSARBEIT

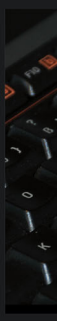
Telefon 0711 5401-2020 und -2021

Fax 0711 5401-2025

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

2011

IUK-KRIMINALITÄT



60 JAHRE

LANDESKRIMINALAMT
Baden-Württemberg