2010

LKA BW

IuK-Kriminalität

JAHRESBERICHT 2010

Baden-Württemberg

LANDESKRIMINALAMT

IMPRESSUM

IUK-KRIMINALITÄT

JAHRESBERICHT 2010

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

© LKA BW, 2011

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

	2009	2010	
GESAMT	**29.868**	**32.249**	**+ 8,0 %**
COMPUTERKRIMINALITÄT	8.363	9.755	
INTERNETKRIMINALITÄT	21.505	22.494	
COMPUTERBETRUG	3.375	4.318	
VERBREITUNG VON KINDERPORNOGRAFIE	196	221	

INHALT

1 ANALYSEDARSTELLUNG

Im zurückliegenden Jahr stieg die Nutzungsintensität und damit die Bedeutung der Informations- und Kommunikationstechnik (IuK) für die Wirtschaft und für das Privatleben der Menschen weiter an. So wuchs nach aktuellen Verlautbarungen des Handelsverbandes Deutschland (HDE) vom 1. Februar 2011 der Onlinehandel viermal so stark wie der konventionelle Einzelhandel.
Im privaten Bereich hat die Nutzung „Neuer Medien" wie Facebook oder Twitter einen regelrechten Boom erlebt. Die Bewertung der damit einhergehenden Begleiterscheinungen kann, abhängig vom Alter der Nutzer, durchaus gegensätzlich sein. Während viele Bürger ihren persönlichen Lebensbereich durch Informationsdienste wie zum Beispiel „Google Street View" beeinträchtigt sehen und von der Politik entsprechende Reglementierungen einfordern, kommt die Offenheit und Bereitwilligkeit, mit der insbesondere jüngere Nutzer in sog. Sozialen Netzwerken Einblicke in ihr Privatleben gewähren, schon fast einer Zustimmung zur Vermarktung ihrer Privatsphäre gleich.
Diese Entwicklung begünstigt zunehmend den Missbrauch von digitalen Identitäten und die Begehung von Straftaten im Zusammenhang mit der Nutzung dieser „Neuen Medien".

Bei der Betrachtung der IuK-Kriminalität ist zwischen Internetkriminalität (IuK-Kriminalität im weiteren Sinne) und Computerkriminalität (IuK-Kriminalität im engeren Sinne) zu unterscheiden.

INTERNETKRIMINALITÄT (IUK-KRIMINALITÄT IM WEITEREN SINNE)

Die Zahl bekanntgewordener Fälle der Internetkriminalität[1] ist 2010 entsprechend dem Trend der Vorjahre weiter angestiegen. Der Zuwachs um 4,6 % bzw. um 989 auf 22.494 Fälle (21.505)[2] liegt jedoch unterhalb der Steigerungsrate des Vorjahres (6,6 %).

Beim Teilbereich Besitz/Verschaffen von kinderpornografischen Schriften verzeichnet die Polizeiliche Kriminalstatistik (PKS) einen Rückgang um 15,4 % auf 386 (456) Fälle. Die Verbreitung von Kinderpornografie stieg mit 221 (196) Fällen hingegen um 12,8 % an. Die Zunahme der Verbreitungshandlungen ist maßgeblich auf die in 2010 bearbeiteten größeren Verfahren zurückzuführen.

Die Ansprechstelle Kinderpornografie beim Landeskriminalamt BW (LKA BW) bearbeitete im Jahr 2010 insgesamt 71 (57) Sammelverfahren (sog. Umfangsverfahren) mit 629 (167) Tatverdächtigen. Mit der angestiegenen Anzahl dieser länderübergreifenden Umfangsverfahren ging im Vergleich zum Vorjahr eine Verdreifachung der Tatverdächtigenzahl einher. Der erhebliche Anstieg der Tatverdächtigenzahl ist damit zu erklären, dass bei drei bundesweiten Umfangsverfahren die vermehrte Verbreitung kinderpornografischer Schriften an einen größeren Nutzerkreis festgestellt und dadurch mehr Tatverdächtige ermittelt werden konnten.

[1] *Die Entwicklung der Internetkriminalität wird im Landeskriminalamt Baden-Württemberg sowohl in der Inspektion 460 – IuK-Kriminalität als auch in der Inspektion 440 – Wirtschaftskriminalität verfolgt. Es wird deshalb auf die diesbezüglichen Ausführungen im Jahresbericht Wirtschaftskriminalität verwiesen.*

[2] *Vorjahreszahlen in Klammern*

ANALYSEDARSTELLUNG

Die ursprünglich für den 23.02.2010 geplante Realisierung des Gesetzes zur Erschwerung des Zugangs zu kinderpornografischen Inhalten in Kommunikationsnetzen (ZugErschwG)[3] war kurzfristig ausgesetzt worden (sog. Accessblocking). Stattdessen erfolgt für die Dauer von einem Jahr an Stelle der Sperrung der vermehrte Versuch des Bundeskriminalamtes, kinderpornografische Inhalte löschen zu lassen. Im Anschluss daran ist eine Evaluierung vorgesehen.

VORRATSDATENSPEICHERUNG

Der Gesetzgeber ist weiterhin aufgefordert, die Gesetzgebung an das Urteil des Bundesverfassungsgerichts zur Vorratsdatenspeicherung vom 2. März 2010 anzupassen und die entstandene gesetzliche Lücke zu schließen. Nach dem Wegfall der Vorratsdatenspeicherung gibt es kein einheitliches Speicherverhalten der Provider mehr. Die Speicherfristen bei Verkehrs- und Bestandsdaten, die nach wie vor durch die Ermittlungsbehörden zur Bekämpfung von Straftaten erhoben werden dürfen, variieren zwischen null und sieben Tagen. Damit bleibt selbst bei unverzüglich durchgeführten Bestandsdatenanfragen – abhängig vom angefragten Provider – das Risiko einer Nichtbeauskunftung.
Erfahrungen des Arbeitsbereichs Internetrecherche (AIR) zeigen beispielsweise, dass die Identifizierung von Straftätern, die das Tatmittel Internet nutzen, seit Wegfall der Vorratsdatenspeicherung wesentlich erschwert ist. So sank schon im März/April 2010 (Zeitraum zwischen dem 09.03.2010 und dem 12.04.2010) die positive Beauskunftung von Bestandsdaten auf 41 %, während sie 2009 noch bei 91 % lag.

ARBEITSBEREICH INTERNETRECHERCHE (AIR)

Im Berichtsjahr wurden durch den AIR zur Bekämpfung des Besitzes und der Verbreitung kinderpornografischer Darstellungen über das Internet insgesamt 1.111 (2.643) Ermittlungsverfahren initiiert. Es konnten 66 deutsche und 1.045 ausländische Tatverdächtige ermittelt werden. Drei Personen stammen aus Baden-Württemberg. Die ausländischen Tatverdächtigen verteilten sich auf insgesamt 58 Nationen. In 39 Fällen konnten die Ermittlungen gegen deutsche Tatverdächtige nicht weitergeführt werden, da Bestandsdatenanfragen an die Provider nicht beauskunftet wurden (sog. Nichtspeicherungsfälle).

Wie in den Vorjahren nahm auch im Jahr 2010 die Anzahl der Fälle, in denen Flächendienststellen bei Amok-, Suizid- sowie sonstigen polizeilichen Lagen durch die Fachinspektion 460 des LKA BW unterstützt wurden, weiter zu. In der Regel erfolgte eine fallbezogene Beratung oder die gerichtsverwertbare Sicherung von Internetinhalten.

[3] *Der Zugriff auf Webseiten mit kinderpornografischen Darstellungen sollte innerhalb Deutschlands durch die Provider gesperrt werden. Anstelle der geblockten Webseite hätte der Anfragende ein Stopp-Schild mit Warnhinweis angezeigt bekommen.*

Die personalintensive Einbindung der Mitarbeiter des AIR in die anlassabhängige Auswertung von Internetinhalten bei öffentlichkeitswirksamen Großereignissen, die fallbezogene Unterstützung anderer Dienststellen und die notwendige personelle Unterstützung in Ermittlungsverfahren des Arbeitsbereichs IuK-Kriminalität sind für den Rückgang der Fallzahlen verantwortlich.

Immer häufiger spielt bei polizeilichen Lagen die Kommunikation über Web 2.0-Dienste (Soziale Netzwerke/Videoportale) eine Rolle.
Polizeiliche Ermittlungen in diesen „Neuen Medien" gewinnen zunehmend an Bedeutung und führen zu Aufklärungserfolgen. Web 2.0-Dienste sind in eine aktive Medienauswertung bei besonderen polizeilichen Lagen mit einzubeziehen. Sie können aber auch zur Steuerung allgemeiner polizeilicher Informationen wie z. B. der Nachwuchswerbung, von Warnmeldungen oder konkreten Fahndungen genutzt werden.

COMPUTERKRIMINALITÄT (IUK-KRIMINALITÄT IM ENGEREN SINNE)

Die Computerkriminalität (IuK-Kriminalität im engeren Sinne) ist mit 1.392 Fällen um 16,6 % auf 9.755 (8.363) Fälle angestiegen.
Der bereits in den zurückliegenden Jahren erkennbare Trend zur Verlagerung krimineller Aktivitäten aus der realen in die virtuelle Welt setzte sich 2010 weiter fort. Dies wurde begünstigt durch die einerseits weiter zunehmende Nutzung der IuK-Technologie insbesondere im privaten Bereich und andererseits durch die wachsenden Möglichkeiten, im Internet Rechtsgeschäfte aller Art, bis hin zu den damit verbundenen Bezahlvorgängen, zu realisieren.
Daneben zeigt sich die Verlagerung auch deutlich an der Entwicklung einzelner Delikte, insbesondere den Fällen des Ausspähens von Daten und des Computerbetruges, auf die der Anstieg der Computerkriminalität maßgeblich zurückzuführen ist. Zwischen beiden Tatbeständen besteht eine enge Beziehung, da sich das Ausspähen von Daten meist als Vor- oder Erlangungstat (sog. „Phishing")[4] darstellt, während im zweiten Schritt mit der rechtswidrigen Verwendung der erlangten Autorisierungsdaten zur betrügerischen Überweisung (Verwertungstat) der Computerbetrug verwirklicht wird.
Die Fallzahlen des Ausspähens von Daten (§ 202a StGB) sind im vergangenen Jahr mit 202 Fällen auf 1.444 Fälle (1.242) um 16,3 % angestiegen. Der Tatbestand Computerbetrug (§ 263a StGB), der statistisch den Vermögensdelikten zugerechnet wird, verzeichnet mit 27,9 % bzw. 943 Fällen (von 3.375 auf 4.318 Fälle) einen deutlichen Zuwachs.

[4] *Der Begriff „Phishing" setzt sich aus den englischen Wörtern „password" und „fishing", zu Deutsch „nach Passwörtern angeln", zusammen. Die Täter versuchen, Informationen, wie z. B. Kontodaten, Kreditkartendaten oder Daten für das Online-Banking, zu erlangen, um diese für eigene Transaktionen zu verwenden.*

ANALYSEDARSTELLUNG

Der Computerbetrug hat mit 44,3 % der Fälle einen erheblichen Anteil an der insgesamt bekannt gewordenen Computerkriminalität. Die Schadensentwicklung verläuft ebenfalls ansteigend. Der registrierte Schaden beläuft sich 2010 auf 5.899.424 (4.035.813) Euro; der Zuwachs beträgt 46,2 % oder absolut 1.863.611 Euro. Dies ist u. a. darauf zurückzuführen, dass von den Tätern höhere Geldbeträge von den einzelnen Konten mittels manipulierten Überweisungen abgerufen wurden.

Im Bereich Ausspähen von Daten/Computerbetrug waren im Jahr 2010 deutliche qualitative und quantitative Veränderungen hinsichtlich des Organisationsgrades der Täter und der von ihnen eingesetzten innovativen Techniken feststellbar. Die Ermittlungsergebnisse einer von den Landeskriminalämtern Baden-Württemberg und Nordrhein-Westfalen gebildeten Ermittlungskooperation belegen dies eindrücklich. Einer international agierenden Tätergruppe war es durch arbeitsteiliges und spezialisiertes Vorgehen gelungen, ein bislang als sicher geltendes Verfahren im Onlinebanking zu umgehen und in der Folge manipulierte Transaktionen zu veranlassen. Dabei kam professionell programmierte Schadsoftware und moderne Kommunikationstechnik zum Einsatz. Für die Weiterleitung der erlangten Geldbeträge ließen sich die Täter von sog. Finanzagenten unterstützen, welche ihre Konten gegen Abzug einer „Provision“ hierfür zur Verfügung gestellt hatten. Die Täter transferierten durch manipulierte Überweisungen mindestens 1,65 Mio. Euro ins In- und Ausland. Ein weiterer finanzieller Schaden in Höhe von rund 1,2 Mio. Euro konnte verhindert werden, da von den zwischenzeitlich informierten Kreditinstituten Kontoverfügungen unterbunden wurden.

Das beschriebene Ermittlungsverfahren ist ein Beispiel dafür, dass im Bereich der Computerkriminalität eine Verlagerung weg von Einzeltätern hin zu internationaler und bandenmäßiger Begehungsweise, teilweise mit Strukturen der Organisierten Kriminalität, stattgefunden hat. Täterkontakte finden nahezu ausschließlich virtuell statt, was neue Herausforderungen in der Ermittlungs- und Beweisführung bei der Identifizierung der einzelnen Täter mit sich bringt. Es ist festzustellen, dass die Täter regelmäßig und in immer kürzeren Zeitabständen neue Verbreitungswege für Schadsoftware entwickeln. Inzwischen existieren Techniken, bei denen eine Aktivität des Internetnutzers nicht mehr erforderlich ist. Schon das Aufrufen einer Webseite kann ausreichen, um Schadsoftware herunterzuladen und zu aktivieren (sog. Drive-by-Download).

Die zunehmende wirtschaftliche Bedeutung des Internets übt nicht nur eine wachsende Anziehungskraft auf Unternehmen und ihre potenziellen Kunden aus, sondern auch auf Personen mit krimineller Energie, die durch Täuschung und Betrug an das Geld ihrer Opfer gelangen wollen. Besonders gefährdet sind hier Kinder und Jugendliche sowie ältere Menschen. Beide Altersgruppen stellen einen schnell und deutlich wachsenden Anteil der privaten Internetnutzer dar.
Jedoch verfügen gerade sie oftmals nicht über die erforderliche Erfahrung und Sensibilität für die Risiken und Gefahren dieser Technologie. Daraus ergibt sich wiederum ein höheres Risiko, dass Angehörige dieser Gruppen bei der Nutzung des Internets Opfer einer Straftat werden.

NEUES PHÄNOMEN: DIGITALE SCHUTZGELDERPRESSUNG

Ein neues, in seiner Gefährlichkeit nicht zu unterschätzendes Phänomen sind die im Berichtszeitraum bundesweit aufgetretenen distributed-Denial-of-Service-Angriffe (dDoS-Attacken)[5]. Hierbei ist das Ziel der Täter, die angegriffenen Firmen oder Web-Shops unter dem Eindruck der von den Tätern verursachten Zugriffsprobleme zur Zahlung der geforderten Beträge zu erpressen. Andernfalls würde die Intensität der Angriffe bis zur völligen Blockade der Webpräsenz hin gesteigert werden. Die Folge wären erhebliche Umsatzeinbußen. Mit dieser Begehungsweise sind im vergangenen Jahr elf Fälle in Baden-Württemberg bekannt geworden.

Die Täter nutzten auch 2010 weiterhin häufig sogenannte Botnetze mit der Zielrichtung, ausgespähte Daten auszutauschen oder Botnetze für Angriffe auf andere Rechner oder Server zu missbrauchen. Wie das beschriebene Ermittlungsverfahren belegt, setzten die Täter für die Verwertung der über betrügerische Überweisungen erlangten Gelder weiterhin sog. Finanzagenten ein.

[5] *Bei dDoS-Angriffen (distributed Denial of Service) rufen alle in einem Botnetz oder einer Botnetzgruppe zugeordneten „Zombie-PC" auf Befehl des Botmasters (sozusagen der Besitzer des Botnetzes) innerhalb kürzester Abstände immer wieder z. B. eine nicht existente Seite auf den Webservern der angegriffenen Webseite auf. Diese Aufrufe werden so lange fortgesetzt, bis die Webserver unter der Last der Anfragen zusammenbrechen und damit ihren Service verweigern (Denial of Service). Die Webpräsenz der angegriffenen Firmen, Institute oder staatlichen Organisationen ist somit nicht mehr über das Internet erreichbar.*

MASSNAHMEN

2 HANDLUNGSEMPFEHLUNGEN / GETROFFENE MASSNAHMEN

GETROFFENE MASSNAHMEN

ERMITTLUNGSHILFEN

Mit Datum vom 19.01.2011 hat die Bundesnetzagentur in Bonn die Vodafone D2 GmbH verpflichtet, Auskunftsersuchen nach § 113 Telekommunikationsgesetz (TKG) unter Mitteilung dynamischer IP-Adressen mit Zeitstempel zu bearbeiten, wenn zur Feststellung der nachgesuchten Bestandsdaten eine Auswertung von Verkehrsdaten erforderlich und im Einzelfall auch möglich ist. Somit wurde die Firma Vodafone verpflichtet, ihrer Auskunftspflicht gemäß § 113 TKG sowohl bei Anfragen zu gespeicherten als auch aktuell genutzten IP-Adressen (sog. Beauskunftung „on the fly") nachzukommen.

AUS- UND FORTBILDUNG

Die Polizei Baden-Württemberg führt derzeit Schulungsveranstaltungen für über 400 IuK-Sachbearbeiter durch, um die Polizeibeamten der Polizeipräsidien und -direktionen gezielt für die spezifischen Besonderheiten der Ermittlungsführung im Bereich der IuK-Kriminalität zu qualifizieren. Die Schulungen werden bis Frühjahr 2012 beendet sein.

Die Staatsanwaltschaften in Baden-Württemberg beabsichtigen, sog. Ansprechpartner IuK-Kriminalität zu benennen, um die Zusammenarbeit von Polizei und Justiz bei der Bekämpfung der IuK-Kriminalität zu intensivieren.

Weiterhin unterstützt die Polizei die Justiz in Baden-Württemberg bei der Fortbildung im Bereich der IuK-Kriminalitätsbekämpfung. Die polizeiliche E-Learning-Anwendung „IuK für Ersteinschreiter" wird derzeit modifiziert und der Justiz zu Fortbildungszwecken zur Verfügung gestellt. Ergänzt wird dieses Angebot durch eintägige Präsenzveranstaltungen gesondert fortgebildeter Multiplikatoren.

AUSWERTUNG UND ANALYSE

Bei der Erfassung der bearbeiteten Verfahren der IuK-Kriminalität in der bundesweiten Verbunddatei IuK nimmt Baden-Württemberg mittlerweile einen der vorderen Plätze ein. Damit wird ein wichtiger Beitrag für die bundesweite Analyse und Bewertung der Entwicklung dieses Kriminalitätsbereiches geliefert. Die dezentrale Erfassung hat sich bewährt und soll in dieser Intensität beibehalten werden.

Am 01.10.2010 wurde die Einrichtung des Kompetenzzentrums IuK-Kriminalität (KIK), angegliedert an den Stab der Amtsleitung des LKA BW, abgeschlossen. Seine Aufgabe ist die abteilungsübergreifende Steuerung und Koordination der im LKA BW in den verschiedenen Fachabteilungen wahrgenommenen Aufgaben zu den Themen IuK-Kriminalität und digitale Spuren. Dem KIK gehören Vertreter der mit diesen Themen betrauten Organisationseinheiten an. Innenministerium, Akademie der Polizei, Bereitschaftspolizeipräsidium und Hochschule für Polizei haben feste Ansprechpartner für das KIK benannt. Dadurch soll die kontinuierliche Abstimmung bei der Erarbeitung und Umsetzung landesweiter Strategien, der technischen Entwicklung und von Aus- und Fortbildungsmaßnahmen gewährleistet werden.
Das KIK nimmt weiterhin die Aufgabe als „Zentrale Ansprechstelle Cybercrime" (ZAC) für die Wirtschaft und sonstige öffentliche und nicht-öffentliche Stellen in Baden-Württemberg wahr. Es steht dem genannten Adressatenkreis zur Klärung grundsätzlicher und strategischer Fragen zur Verfügung.

Mit der Einstellung von insgesamt 15 IT-Spezialisten beim Landeskriminalamt Baden-Württemberg und der Akademie der Polizei im Jahr 2011 verstärkt die Polizei nachhaltig den schnelllebigen und hochtechnischen Bereich der IuK-Kriminalität und Informationstechnik. Die Spezialisten werden in den Bereichen Ermittlungen und Ermittlungsunterstützung sowie der damit einhergehenden forensischen Beweissicherung von digitalen Spuren eingesetzt.

HANDLUNGSEMPFEHLUNGEN

NEUREGELUNG DER VORRATSDATENSPEICHERUNG

Der drastische Rückgang von erfolgreichen Bestandsdatenanfragen nach dem Wegfall der Vorratsdatenspeicherung belegt eindrücklich die absolute Notwendigkeit der Schaffung einer entsprechenden gesetzlichen Regelung.
Die Landeskriminalämter melden derzeit der Rechtstatsachensammel- und -auswertestelle des Bundeskriminalamts (RETASAST) alle Ermittlungsverfahren und präventivpolizeilichen Sachverhalte, bei denen die Identifizierung des/der Tatverdächtigen oder die weiteren Ermittlungen bzw. polizeilichen Maßnahmen durch den Wegfall der Vorratsdatenspeicherung erschwert oder verhindert wurden.

AKTUALISIERUNG DER AUS- UND FORTBILDUNGSINHALTE

Die Erfahrungen des Jahres 2010 im Zusammenhang mit Einsatzlagen belegen das Erfordernis, die polizeiliche Aus- und Fortbildung um Methoden zur Suche und Sicherung von relevanten Netzinhalten zu erweitern. Die Möglichkeiten, Chancen und Risiken der „Neuen Medien" müssen zukünftig in der Aus- und Fortbildung einen größeren Raum einnehmen. Hierbei sind neben den technischen Abläufen die rechtlichen Aspekte und die Grenzen – auch hinsichtlich ihrer privaten Nutzung – aufzuzeigen.

MASSNAHMEN

VERBESSERUNG DES DATENSCHUTZES IM INTERNET

Hinsichtlich der Preisgabe persönlicher Daten und Informationen über das Privatleben in Sozialen Netzwerken und Foren sollte der Schutz des Nutzers durch ein Widerrufsrecht und eine Löschverpflichtung des Betreibers auf Verlangen des Nutzers gestärkt werden.

VERBESSERUNG DER SICHERHEIT BEI DER INTERNETNUTZUNG

Ein wesentlicher Beitrag des einzelnen Internetnutzers zu seinem eigenen Schutz besteht nach wie vor darin, die jeweils aktuellste Version der verwendeten Software (Betriebssystem, Firewall und Virenschutz) zu nutzen. Nur auf diesem Wege ist sichergestellt, dass vorhandene Schwachstellen und Risiken regelmäßig beseitigt werden. Diese Maßnahmen zum Eigenschutz schließen auch die Nutzung der jeweils neuesten Online-Banking-Verfahren der Banken ein. Dies sind derzeit die Systeme HBCI und Smart-TAN.
Auf diese Umstände ist angesichts der weiter steigenden Nutzerzahlen unverändert bei allen polizeilichen Veranstaltungen und Publikationen hinzuweisen.

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 verbundene 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

http://sicher-im-netz.de
Deutschland sicher im Netz e.V. informiert Verbraucher über Gefahren im Internet.

http://www.sicherer-autokauf.de
Die Initiative „Sicherer Autokauf im Internet“ gibt Ratschläge zum Schutz gegen Online-Betrüger beim Kauf von Kraftfahrzeugen.

http://www.verbraucher-sicher-online.de
Die Initiative „Verbraucher sicher online“ verfolgt das Ziel, den Verbraucher über die sichere Nutzung des Computers zu informieren.

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

http://www.fragfinn.de
FragFINN – Ein Netz für Kinder.

http://time4teen.de
Umfangreiche Tipps und Informationen, speziell für Kinder und Jugendliche, sind auf den Seiten von time4teen.de zusammengefasst.

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

www.polizeiberatung.de/vorbeugung/gefahren_im_internet/
Allgemeine Sicherheitsempfehlungen für PC und Internet.

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.

Hinweis I 460:
Im Zuge einer Angleichung des Sprachgebrauches in Europa setzt sich zunehmend, auch national, für die Bezeichnung IuK-Kriminalität der Begriff „Cybercrime“ 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 (Kinderpornografie)
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 pornografischer 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 initiierte 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 2009 – 2010

	PKS-Schlüssel	2009	2010	in %	Tendenz
Computerbetrug (§ 263a StGB)	5175	3.375	4.318	+27,9	↗
Fälschung beweiserheblicher Daten (§ 269 StGB)/Täuschung im Rechtsverkehr (§ 270 StGB)	5430	672	638	-5,1	↘
Datenveränderung (§ 303a StGB)/ Computersabotage (§ 303b StGB)	6742	141	194	+37,6	↗
Ausspähen von Daten (§ 202a StGB)	6780	1.242	1.444	+16,3	↗
Computerkriminalität	8970	8.363	9.755	+16,6	↗

TABELLE IUK-KRIMINALITÄT IM ENGEREN SINNE 2006 - 2010

Berichtsjahr	2006	2007	2008	2009	2010
Computerbetrug PKS 5175	3.034	2.436	2.208	3.375	4.318
Schadenssumme in Euro Computerbetrug	2.862.311	5.261.621	2.165.982	4.035.813	5.899.424
Fälschung beweiserheblicher Daten/Täuschung im Rechtsverkehr PKS 5430	154	405	342	672	638
Datenveränderung/ Computersabotage PKS 6742	139	197	212	141	194
Ausspähen von Daten PKS 6780	280	522	828	1.242	1.444
Computerkriminalität PKS 8970	6.833	6.549	6.324	8.363	9.755
Schadenssumme in Euro Computerkriminalität	5.310.568	7.593.768	4.176.110	6.201.261	9.374.777

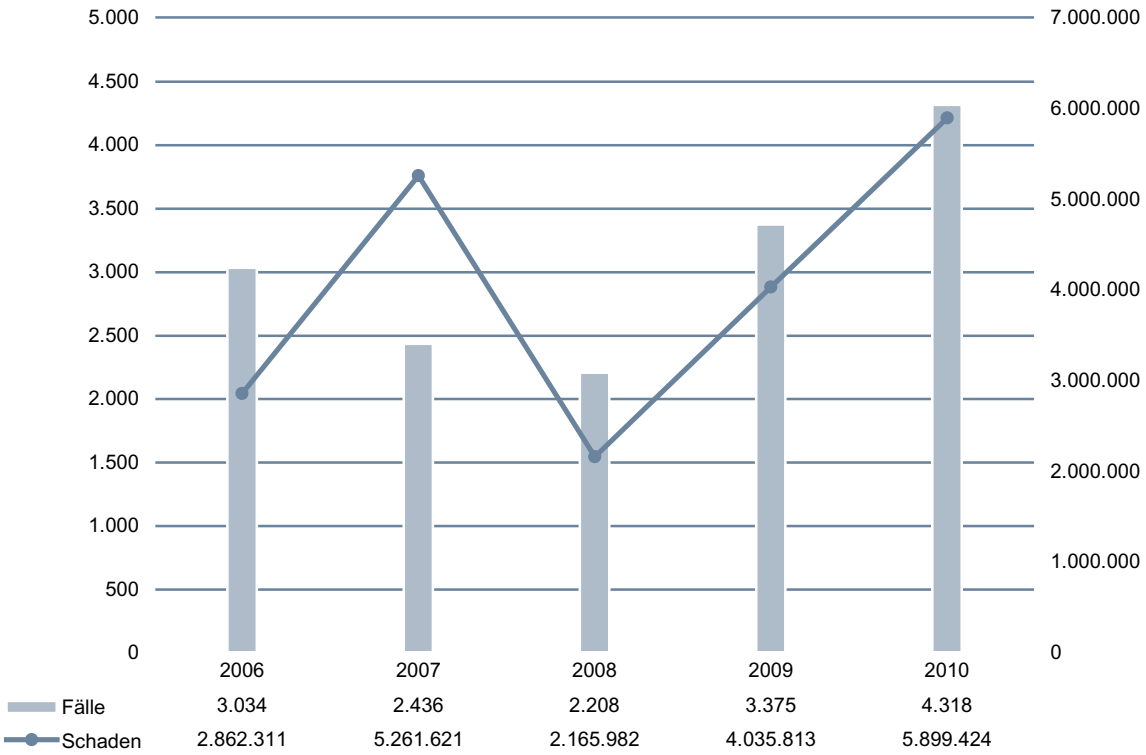
PKS-BAROMETER KINDERPORNOGRAFIE 2009 – 2010

	PKS-Schlüssel	2009	2010	in %	Tendenz
Besitz/Verschaffen von Kinder-pornografie (§ 184b StGB)	1433	456	386	-15,4	↘
Verbreitung von Kinderpornografie (§ 184b StGB)	1434	196	221	+12,8	↗

TABELLE STRAFVERFAHRENINITIIERUNGEN ARBEITSBEREICH INTERNETRECHERCHE (AIR) 2006 - 2010

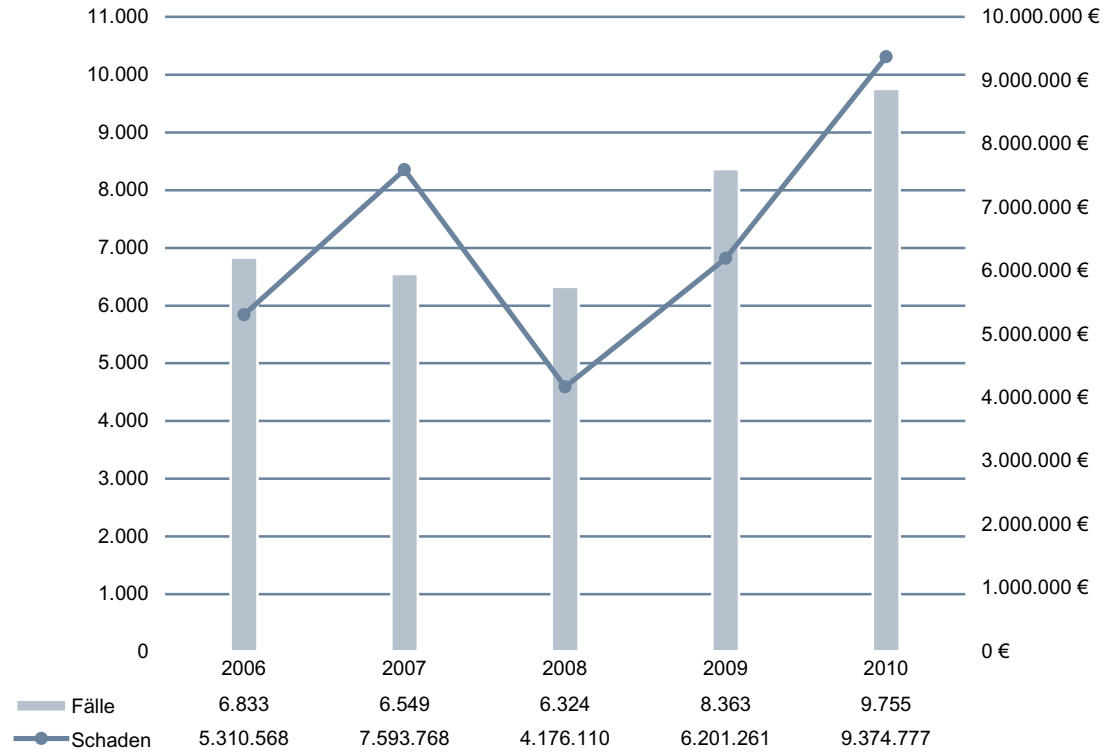
Berichtsjahr	2006	2007	2008	2009	2010
Deutschland	452	1.119	1.504	338	66
davon Baden-Württemberg	63	98	100	30	3
International	2.375	4.465	8.557	2.305	1.045
Gesamt	**2.827**	**5.584**	**10.061**	**2.643**	**1.111**

COMPUTERBETRUG 2006-2010



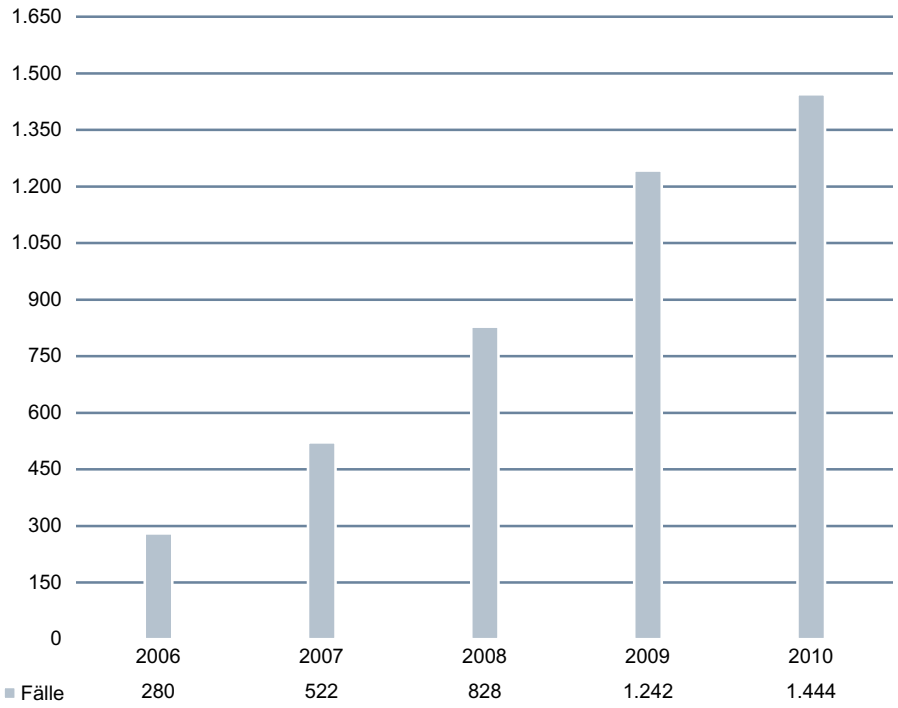
	2006	2007	2008	2009	2010
Fälle	3.034	2.436	2.208	3.375	4.318
Schaden	2.862.311	5.261.621	2.165.982	4.035.813	5.899.424

COMPUTERKRIMINALITÄT 2006-2010

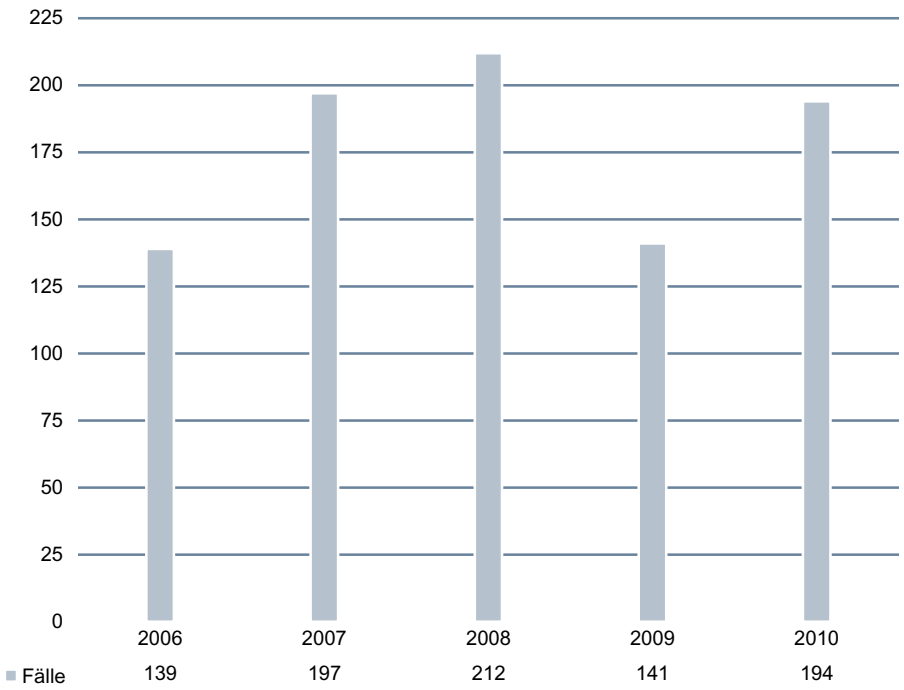


	2006	2007	2008	2009	2010
Fälle	6.833	6.549	6.324	8.363	9.755
Schaden	5.310.568	7.593.768	4.176.110	6.201.261	9.374.777

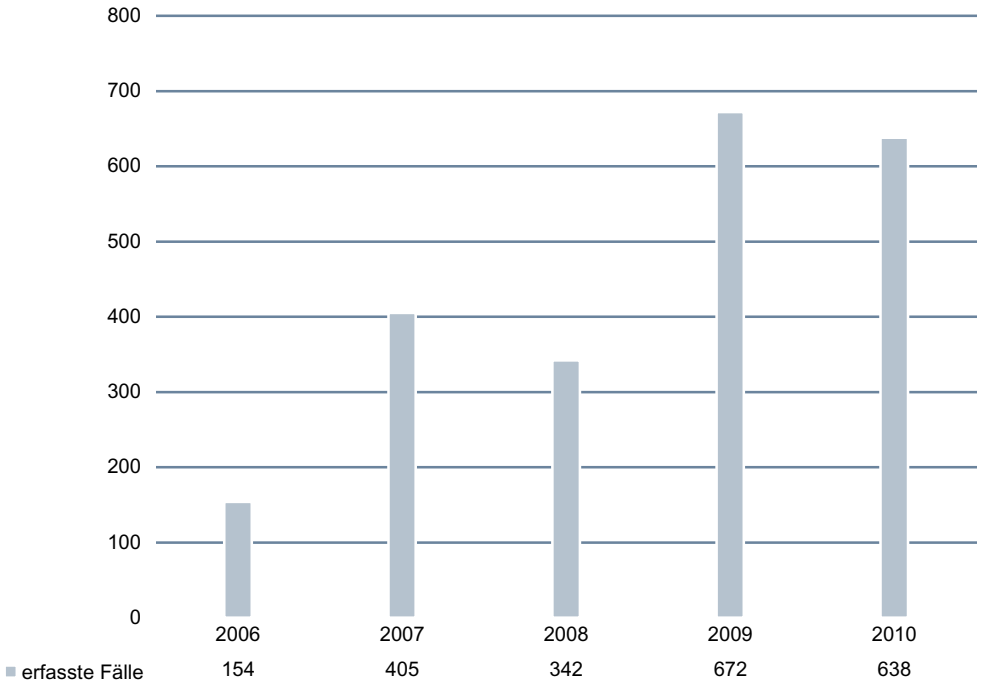
AUSSPÄHEN VON DATEN 2006-2010



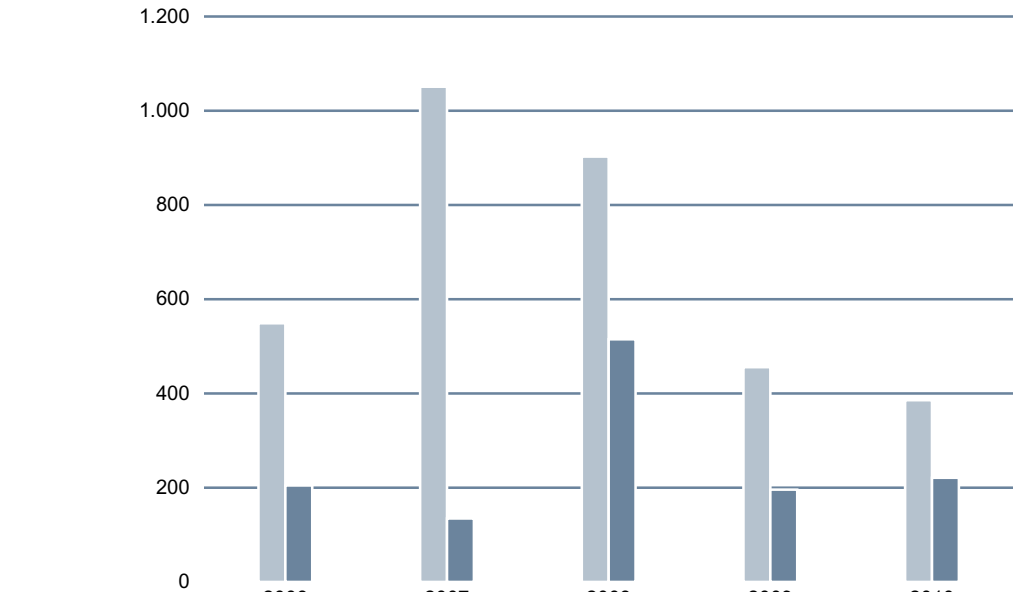
DATENVERÄNDERUNG – COMPUTERSABOTAGE 2006-2010



FÄLSCHUNG BEWEISERHEBLICHER DATEN – TÄUSCHUNG IM RECHTSVERKEHR 2006-2010



BESITZ / VERSCHAFFEN UND VERBREITEN VON KINDERPORNOGRAFIE 2006 - 2010



	2006	2007	2008	2009	2010
Besitz/Verschaffen	549	1.051	903	456	386
Verbreiten	205	135	515	196	221

ANSPRECHPARTNER

ÖFFENTLICHKEITSARBEIT

Telefon 0711 5401-2020 und -2021

Fax 0711 5401-2025

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

2010