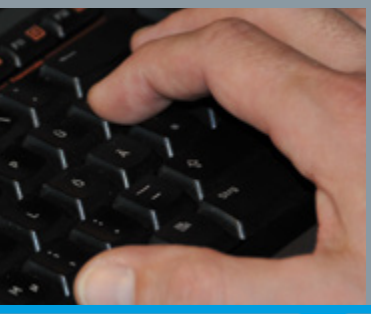
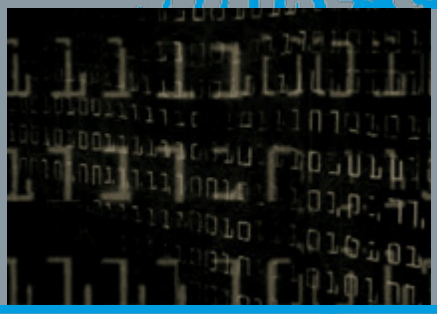
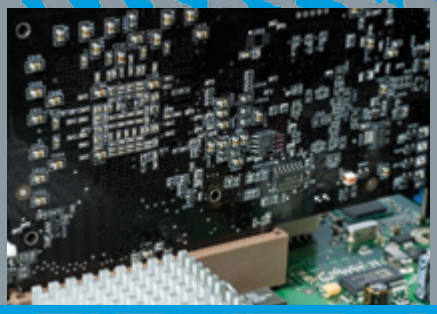





2013

LKA BW

Cybercrime / Digitale Spuren

JAHRESBERICHT 2013

Baden-Württemberg

LANDESKRIMINALAMT

CYBERCRIME / DIGITALE SPUREN
AUF EINEN BLICK

CYBERCRIME WIRD BISLANG NUR UNVOLLSTÄNDIG IN DER POLIZEILICHEN KRIMINALSTATISTIK ABGEBILDET.

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

COMPUTERKRIMINALITÄT (CYBERCRIME IM ENGEREN SINNE) AUF UNVERÄNDERT HOHEM NIVEAU.

DER IM JAHR 2012 FESTGESTELLTE RÜCKGANG DER INTERNETKRIMINALITÄT (CYBERCRIME TATMITTEL) HAT SICH IM BERICHTSJAHR 2013 NICHT FORTGESETZT.

	2012	2013	IN %	
GESAMT[1]	**20.913**	**23.014**	**+ 10,0**	↗
COMPUTERKRIMINALITÄT	8.907	8.893	- 0,2	→
INTERNETKRIMINALITÄT	16.912	18.804	+ 11,2	↗
GESAMTBEREICH KINDERPORNOGRAFISCHE SCHRIFTEN	559	693	+ 24,0	↗
VERFAHRENSINITIIERUNGEN AIR	40	297	+ 642,5	↗
RANSOMWARE	3.226	2.417	- 25,1	↘
NEUE AUFTRÄGE ITB	10.732	11.225	+ 4,6	↗
FISBW-ANFRAGEN	5.318	7.529	+ 41,6	↗
ANFORDERUNG MOBILFUNKAUFKLÄRUNG	620	789	+ 27,3	↗

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

INHALT

1 ANALYSE

Das Handeln im Internet und die Nutzung seiner Anwendungen und Möglichkeiten ist in Teilen konträr gegenüber dem, was wir seit jeher gewohnt sind. Wir nutzen das Internet vorwiegend nonpersonal, häufig anonym oder pseudonym. Wir können sogar Verträge unter unserem Nicknamen abschließen, mit einer Internetwährung bezahlen und haben digitale Freunde. Freunde, die wir ausschließlich aus dem Netz kennen und noch nie gesehen haben. Das moderne Internet ist in seiner heutigen Form noch keine 30 Jahre alt, die sogenannten Web 2.0-Dienste gibt es erst seit knapp über zehn Jahren. Zwischenzeitlich gibt es bereits eine ganze Generation, die mit dem Internet aufgewachsen ist und sich „im Netz" verhält, als habe es andere Kommunikationsmöglichkeiten nie gegeben. Ältere Generationen hingegen tun sich teilweise schwer, Zugang zu dieser Form von Kommunikation zu finden und sind dann, wenn sie Nutzer des Internets sind, auch eher in der Gefahr, Opfer von Straftaten im Netz zu werden.

Der Staat gestaltet das Leben und Handeln seiner Menschen maßgeblich mit. Aufgabe der Legislative ist es dabei, die Balance zwischen Freiheit und Sicherheit bei der Gesetzgebung zu halten. Die Polizei nimmt als Teil der Exekutive die Aufgaben Gefahrenabwehr und Strafverfolgung wahr. Hierzu benötigt sie Gesetzesgrundlagen, die im realen und im virtuellen Raum gleichermaßen gelten und den Schutz der Gesellschaft gewährleisten. Die aktuelle Gesetzgebung berücksichtigt die Besonderheiten des Internets und seiner Nutzung durch Straftäter noch nicht in ausreichendem Maße.

Die mit der Bekämpfung von Cybercrime befassten Polizeibeamten bekommen die Auswirkungen in der täglichen Arbeit zu spüren.

Eines der größten Probleme im Internet ist für die Polizei die Attribution von Angriffen und Straftaten. Damit ist die Zuordnung und Identifizierung von Tatverdächtigen und Handelnden gemeint. Attribution hat verschiedene Teilaspekte. Zunächst ist es erforderlich, den Rechner zu identifizieren, von dem aus Straftaten begangen werden (technische Attribution). Im nächsten Schritt ist es erforderlich, die Person zu ermitteln, die hinter der Straftat steht (personale Attribution). Abschließend bedarf es der motivationalen Attribution, also der Klärung der Frage, warum es zu dem Angriff kam. Diesen Fragen wird im weitesten Sinne auch in der klassischen Kriminalitätsbekämpfung und Strafverfolgung nachgegangen. Es geht um die Tatwaffe, den Täter und das Motiv – im Falle der Cybercrime um die Besonderheiten des Internets, wie spezifischen Aufbau (Globalität, Dezentralität), Datentransport (Flüchtigkeit der Daten, zufällige bzw. flexible Nutzung von freien Ressourcen), Datenmenge und der Asymmetrie zwischen Angriff und Verteidigung (der Verteidiger muss Millionen von Codezeilen pro Programm schützen, dem Angreifer reicht mitunter ein simpler Schreibfehler, um einen Angriffsvektor zu haben). Zudem erschwert die zunehmende Anonymität die Beantwortung dieser Fragen im Vergleich zur Bearbeitung der klassischen Kriminalitätsformen erheblich. Gesellschaft und Politik müssen sich die Frage stellen, ob sie sich einen Staat wünschen, der auch im Internet Recht und Gesetz verlässlich durchsetzt, oder einen solchen, der dieses Feld – weitgehend unreguliert – den freien Kräften überlässt.

ONLINE-NUTZUNG

ARD und ZDF erstellen seit dem Jahr 1997 die ARD/ZDF-Onlinestudie[2] zur Entwicklung der Internetnutzung in Deutschland sowie dem Umgang der Nutzer mit den Angeboten. Zielgruppe der repräsentativ durchgeführten Befragung sind alle in Deutschland lebenden Erwachsenen ab 14 Jahren. 77,2 Prozent der Befragten gaben im Jahr 2013 an, dass sie mindestens gelegentlich online sind, was 54,2 Millionen Einwohnern entspricht. Der Zuwachs gegenüber dem Vorjahr betrug 1,3 Prozent und liegt damit in der Größenordnung der Zuwachsraten der vorigen Jahre mit Steigerungen um jeweils zwei Prozent. Eine erstaunliche Entwicklung ergibt sich bei den Altersgruppen zwischen 20 und 49 Jahren. Hier sind jeweils geringe Rückgänge festzustellen (20-29 Jahre: - 1,1 Prozent, 30-39 Jahre: - 2,1 Prozent und 40-49 Jahre: - 0,5 Prozent). Eine hohe Anstiegsrate ist hingegen bei den 50- bis 59-Jährigen mit 5,9 Prozent und bei den über 60-Jährigen mit 3,7 Prozent festzustellen.
Dies deckt sich mit aktuellen Untersuchungen sozialer Netzwerke, die gerade bei älteren Generationen einen Zuwachs feststellen. Die Altersgruppe 14 bis 19 Jahre erreicht seit Jahren einen Wert von 100 Prozent. Insgesamt zugenommen hat die durchschnittliche Verweildauer bei der Onlinenutzung. Zwischenzeitlich geben die Befragten an, je Tag 169 Minuten online zu sein. Ein Jahr zuvor waren dies noch 133 Minuten. Die zunehmende Verschmelzung von Internetzugang und Multimediakonsum zeigt sich auch in der Entwicklung der internetfähigen Fernsehern bzw. Smart-TV-Geräte.
29 Prozent der Online-Haushalte verfügen über ein derartiges Gerät. Während im letzten Jahr 2 Prozent die Online-Funktion ihres TV-Geräts nutzten, waren es im Jahr 2013 bereits 12 Prozent.

Immer mehr Haushaltsgeräte, Gegenstände des täglichen Bedarfs aber auch komplexere Systeme wie die Haussteuerung (Smart Homes) oder Fahrzeuge verfügen über eine Internetschnittstelle.
Diese neuen Möglichkeiten bieten Chancen, aber auch Risiken. So wurde im Jahr 2013 ein größeres Botnetz festgestellt, dessen infizierte Geräte nicht nur Computer umfassten, sondern auch andere Geräte wie internetfähige Fernseher und Router, aber auch einen Kühlschrank mit entsprechender Internetschnittstelle[3].
Aber nicht nur Haushaltsgeräte des täglichen Bedarfs sind zunehmend von einer funktionierenden IT-Infrastruktur abhängig. Internet und computergesteuerte Technik sind auch in der Industrie nicht mehr wegzudenken. Das hat in einem Wirtschaftsstandort wie Baden-Württemberg auch erhebliche Auswirkungen auf die Verletzbarkeit und Angreifbarkeit von Unternehmen. Sei es durch klassische Wirtschaftsspionage, also durch Nachrichtendienste fremder Staaten organisierte und gelenkte Cyberspionage, oder durch Konkurrenzausspähung sowie sonstige Delikte der Cybercrime.

2 *vergleiche http://www.ard-zdf-onlinestudie.de (aufgerufen am 12. Februar 2014).*

3 *vergleiche http://www.golem.de/news/thingbot-botnetz-infiziert-kuehlschrank-1401-103978.html (aufgerufen am 17. Januar 2014).*

DUNKELFELD

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

- Die Straftat wird nicht erkannt.
  Beispiel 1: Der Abfluss von Daten mit dem Hintergrund Wirtschafts- oder Industriespionage wird von der betroffenen Firma nicht bemerkt.
  Beispiel 2: Der Rechner des Opfers ist Teil eines Botnetzes, das Botnetz wird zur Begehung von Straftaten genutzt, der User weiß davon aber nichts.
- Die Straftat wird als irrelevant eingeschätzt oder gar nicht als Straftat bewertet.
  Beispiel 1: Es werden Unregelmäßigkeiten im Netzwerkverkehr einer Firma festgestellt, Schäden werden nicht erkannt.
  Beispiel 2: Der mit einem Trojanischen Pferd infizierte Rechner wird mit einem Virenscanner überprüft, die Malware wird erkannt und bereinigt, eine Strafanzeige wird nicht erstattet.
- Die Straftat wird aufgrund des Aufwands nicht angezeigt.
  Beispiel: Bei einem Onlinebetrug (z. B. bei der Nutzung von Internet-Auktionshäusern) entsteht ein Schaden von 20 Euro. Der Geschädigte geht deswegen nicht zur Polizei.
- Die Straftat wird aus Scham nicht angezeigt.
  Beispiel: Das Opfer wurde zu gemeinsamen sexuellen Handlungen vor einer Webcam überredet, die Handlungen wurden heimlich aufgezeichnet. Das Opfer wird erpresst, es wird mit der Veröffentlichung der Bilder bzw. der Weiterleitung an den Freundeskreis des Opfers in Sozialen Netzwerken gedroht.
- Die Straftat wird nicht angezeigt, weil die begrenzten Erfolgsaussichten der Ermittlungsbehörden in diesem Kriminalitätsbereich bekannt sind („Da kann man ja sowieso nichts machen.“).
- Die Straftat wird aus Angst vor einem Imageschaden nicht angezeigt. Dies trifft häufig im Falle geschädigter Wirtschaftsunternehmen zu. Die eingetretenen Schäden werden „intern“ reguliert; das Unternehmen verzichtet auf eine Anzeigeerstattung.

Eine simple Errechnung des Dunkelfeldes auf Basis des polizeilichen Hellfeldes ist nicht möglich. Hierzu sind im Regelfall kriminologische Studien erforderlich. Das Landeskriminalamt Niedersachsen hat am 22. November 2013 eine solche repräsentative Dunkelfeldstudie veröffentlicht. Demnach wurden rund 30 Prozent der niedersächsischen Einwohnerinnen und Einwohner über 16 Jahre im

Jahr 2012 Opfer mindestens einer Straftat. Das Ausmaß der Straftaten sei dabei sehr unterschiedlich. So wurden 106 von 1.000 der befragten Personen Opfer einer Straftat im Zusammenhang mit Computern, darunter Datenverlust durch Viren, Phishing oder Betrugshandlungen im Internet. Das Landeskriminalamt Niedersachsen nahm auf Basis der Dunkelfeldstudie eine Hellfeld-Hochrechnung vor und verglich diese mit dem tatsächlichen Hellfeld aus der Polizeilichen Kriminalstatistik (PKS) des Jahres 2012. Dabei ergibt sich das eindrucksvolle Ergebnis, dass „Cybercrime" (vorgenannte Straftaten im Zusammenhang mit Computern) statt 20.311 registrierten Straftaten tatsächlich mit rund 225.700 Straftaten in der Statistik erfasst sein müsste. Dies ist auf die sehr niedrige Anzeigequote (neun Prozent) bei „Cybercrime" zurückzuführen. „Cybercrime" rangiert damit in der Hellfeld-Hochrechnung auf Basis der Studie im Vergleich zu allen errechneten Hellfeld-Werten fast unmittelbar nach den Eigentumsdelikten auf Rang zwei und liegt noch vor den Körperverletzungsdelikten, Sachbeschädigung und Betrug (ohne Internetnutzung) sowie anderen Delikten wie Drohung, Sexualdelikten und Raub.

ZENTRALE ANSPRECHSTELLE CYBERCRIME

Die Zentrale Ansprechstelle Cybercrime (ZAC) des Landeskriminalamtes Baden-Württemberg (LKA BW) hat die Aufgabe des Single Point of Contact für Wirtschaftsunternehmen sowie öffentliche und nichtöffentliche Stellen auf Bundes- und Landesebene. Diese Aufgabe wird innerhalb der Führungsgruppe der Abteilung Cybercrime/Digitale Spuren wahrgenommen. Die ZAC ist rund um die Uhr erreichbar, wobei das Führungs- und Lagezentrum die Aufgabe an Wochenenden und in der Nachtzeit übernimmt. Bei entsprechender Entwicklung des Anzeigenaufkommens ist eine Erreichbarkeit der ZAC-Angehörigen in Form einer Bereitschaft rund um die Uhr vorgesehen. Die ZAC soll einen wesentlichen Beitrag dazu leisten, das erwartete Dunkelfeld im Bereich Cybercrime gerade im Bereich der Wirtschaft abzubauen.
Im Jahr 2013 wurden durch die ZAC 167 Hinweise bearbeitet. Einen Schwerpunkt stellen derzeit noch Anfragen und Strafanzeigen von Bürgern ohne Geschädigten-Eigenschaft als Wirtschaftsunternehmen dar.

Anlagen | 1-8

CYBERCRIME IM ENGEREN SINNE (COMPUTERKRIMINALITÄT)

Die in der PKS registrierte Anzahl der Fälle der Computerkriminalität zeigt sich weiterhin stabil und erreichte im Jahr 2013 annähernd den Wert des Vorjahres. Statistisch ist nur ein sehr geringer Rückgang um 0,2 % auf 8.893 Fälle zu verzeichnen. Der registrierte Schaden in der Computerkriminalität beträgt 10.254.150 Euro und ist damit im Vergleich zum Vorjahr mit 5.843.142 Euro wieder deutlich um 75,5 % gestiegen. Maßgeblich für den Anstieg des Schadens ist der Computerbetrug.
Die Anzahl der erfassten Fälle des Computerbetrugs ging um 3,3 % auf 3.539 Fälle zurück. Hierbei ist jedoch zu beachten, dass viele Fälle des Computerbetrugs im Zusammenhang mit Online-Banking, dem Hacken und Verändern von Webseiten, der Übernahme von Facebook-, E-Mail- oder

Verkaufsportal-Accounts sowie dem Eindringen in Telefonanlagen unter dem „Führungsdelikt“ Datenveränderung/Computersabotage erfasst werden. Bei diesem Deliktsschlüssel ist ein Anstieg um 34,2 % auf 392 Fälle zu verzeichnen. Dies ist gleichzeitig die höchste Veränderung der Fallzahlenentwicklung unter den Einzeldelikten der Computerkriminalität im Jahresvergleich.
Die Entwicklung der Schadenshöhe für den Tatbestand des Computerbetrugs hat entgegen der Anzahl der Fälle einen Anstieg um 124,5 % auf 7.665.352 Euro (3.414.341 Euro) zu verzeichnen und erreicht damit dasselbe Niveau wie bereits im Jahr 2011 (7.509.910 Euro). Diese Entwicklung ist zu einem großen Teil auf ein durch das Polizeipräsidium Stuttgart im Jahr 2013 abgeschlossenes Ermittlungsverfahren mit „Führungsdelikt“ Computerbetrug zurückzuführen. Der Schaden im für das Verfahren tatrelevanten Zeitraum (21. August 2008 bis 2. August 2013) beläuft sich auf 2.932.379,59 Euro, der letztlich richtlinienkonform erst im Jahr 2013 in die PKS mit einfloss. Gegenstand dieses Verfahrens ist das Handeln eines Mitarbeiters eines führenden europäischen Anbieters von Zahlungsverkehrsdienstleistungen für Banken, der seit dem Jahr 2003 regelmäßig widerrechtliche Überweisungen zu seinen Gunsten vornahm. Zur Verschleierung seiner Handlungen glich der Beschuldigte den jeweils aktuell aufgelaufenen Schaden in Höhe von zuletzt 6,7 Mio. Euro durch diverse Belastungen von den Konten der von ihm betreuten Banken in Deutschland aus.
Der Tatbestand des Ausspähens von Daten (§ 202a StGB) ist nahezu unverändert geblieben. Im Jahr 2013 sind mit 1.334 erfassten Fällen zwölf Fälle weniger als im Vorjahr zu verzeichnen, was einer Abnahme um 0,9 % entspricht.
Die angeführte Tendenz der Fallzahlenentwicklung in der PKS im Deliktsbereich Datenveränderung/Computersabotage wird ebenfalls durch die verstärkt seit Anfang des Jahres auftretenden Fälle des sogenannten „Windowsverschlüsselungstrojaners“ (WVT) beeinflusst. Da aktuelle Versionen des von der Ermittlungsgruppe „WVT“ in Niedersachsen bearbeiteten trojanischen Pferdes seit Anfang des Jahres 2013 wieder verstärkt verbreitet wurden, erfuhren diese Deliktschlüssel im Jahr 2013 einen Anstieg. Ein weiterer Indikator für den Anstieg der Fallzahlen der PKS aufgrund des Deliktsphänomens Ransomware ist die Anzahl der Fälle der Erpressung. Im Jahr 2013 stiegen diese Fallzahlen um 46,3 % auf 1.204 Fälle. Vergleicht man die Anzahl der Fälle der Erpressung mit Tatmittel Internet, so erfuhr diese einen hohen Zuwachs um 193,8 % auf 476 Fälle. Die Differenz von 314 Fällen entspricht nahezu der Zunahme der Fallzahlen der Erpressung ohne Sonderkenner Internet (+ 381 Fälle).
Im Detail betrachtet ist eine hohe Anzahl dieser Fälle dem Phänomen Ransomware zuzuordnen.

ARBEITSBEREICH ERMITTLUNGEN CYBERCRIME

Die im Jahr 2013 beim LKA BW bearbeiteten Ermittlungsverfahren zeigen, dass Straftäter im virtuellen Raum die Techniken und Möglichkeiten zur Verschleierung ihrer Identitäten stetig weiterentwickeln. Anonymisierungsdienste wie z. B. TOR und Botnetze werden zielgerichtet eingesetzt, um eine Rückverfolgung zu erschweren. Die Täter passen sich zeitnah an technische Sicherungsmechanismen an und ändern oft unmittelbar ihre Vorgehensweise, um einer Strafverfolgung zu entgehen.

ERMITTLUNGSVERFAHREN „MINER"

Über das Bundesamt für Sicherheit in der Informationstechnik (BSI) und das Bundeskriminalamt (BKA) wurde das LKA BW informiert, dass ein von einem weltweit tätigen IT-Sicherheitsunternehmen analysiertes neues Botnetz namens „Miner" existiert. Durch dieses Botnetz wurden DDoS-Attacken auf überwiegend deutsche Unternehmen durchgeführt. Allein in der ersten von mehreren Angriffswellen wurden 30 Internetpräsenzen deutscher Unternehmen angegriffen, welche dadurch über mehrere Tage nicht mehr zu erreichen waren. Neben einer Vielzahl von privaten Firmen wurde auch die Seite des Bundesgerichtshof (BGH) und die Seite der Deutschen Bundesbank angegriffen. Die geschädigten Unternehmen erhielten im Vorfeld eine erpresserische E-Mail, in der ein DDoS-Angriff angekündigt wurde, der durch eine Zahlung von 100 Bitcoins (Ein Bitcoin entsprach am 31.12.2014 573,17 Euro) abgewendet werden könne.
Neben der Möglichkeit, DDoS-Angriffe durchzuführen, hatte das Botnetz die Funktion, die Rechenleistung der infizierten PC zur Erzeugung von Bitcoins missbräuchlich zu verwenden und das Guthaben im Bitcoin-System, das von dem infizierten Rechner aus verwaltet wurde, dem Eigentümer zu entziehen. Darüber hinaus konnte jeder infizierte Rechner als Proxy genutzt werden. Das Botnetz wurde auch für sogenannte Pay-Per-Install-Services verwendet und konnte weitere Schadsoftware, wie den sogenannten ZeroAccess-Trojaner, auf fremden Rechnern installieren. Im Rahmen des Ermittlungsverfahrens wurden Überwachungsmaßnahmen durchgeführt sowie Daten im In- und Ausland sichergestellt. Es konnten in der Folge jedoch keine Täterzugriffe auf diese Daten festgestellt werden. In Zusammenarbeit mit einem IT-Sicherheitsdienstleister wurden gefahrenabwehrrechtliche Maßnahmen wie die Weiterleitung der Schadsoftware an die Antiviren-Industrie und Benachrichtigungen der Internet-Service-Provider der Geschädigten durchgeführt.

ERMITTLUNGSVERFAHREN „KLICK"

Unbekannte Täter registrierten eine Vielzahl von missbräuchlich verwendeten Publisher-Accounts bei einem Affiliate-Marketing-Unternehmen und stellten dabei teilweise Werbeflächen auf Internetseiten bereit. Hierzu fertigten die Täter eine Vielzahl von Fake-Webseiten, in denen in der Folge der Werbebanner eines der führenden deutschen Reiseunternehmen implementiert wurde. Zudem wurden fremde Webseiten durch die Täter als Werbeflächen angegeben. Da im firmeninternen System zeitweise keine Verifikation der Werbefläche stattfand, wurden diese vom System in einem gewissen Zeitraum als solche akzeptiert. Zudem war es den Tätern zeitweise möglich, Werbeverträge mit dem

betreffenden Reiseunternehmen mit ausstehender Verifikation abzuschließen. Die Täter riefen dann im weiteren Verlauf die Werbebanner auf den Fake-Webseiten auf und wurden so auf die Webseite des Reiseunternehmens weitergeleitet. In den Fällen, in denen keine Fake-Webseiten erstellt wurden, öffneten die Täter den Werbelink des Werbeunternehmens und wurden somit ebenfalls auf die Webseite des Reiseunternehmens weitergeleitet. Dort wurden unautorisiert Reisebuchungen getätigt, wodurch eine automatische Vergütung der missbräuchlichen Buchungen generiert wurde, die den Tätern über die verwendeten Publisher-Accounts beim Werbeunternehmen ausgezahlt wurden. Somit wurden ca. 8.600 Euro auf diverse ausländische Konten der Täter überwiesen, während sich der Schaden des Reiseunternehmens durch entstandene Stornokosten der bereits gebuchten Reisen auf über 150.000 Euro beläuft. Die Täter verwendeten für ihre Handlungen infizierte Rechner eines Botnetzes, um ihre IP-Adresse bei den missbräuchlichen Reisebuchungen zu verschleiern.

RANSOMWARE – EINE VARIANTE DER DIGITALEN SCHUTZGELDERPRESSUNG

Nach einer Auswertung über den Sondermeldedienst Cybercrime in INPOL Fall mit 2.417 Fällen für das Jahr 2013 (Vorjahr: 3.226 Fälle) wird deutlich, dass dieses Kriminalitätsphänomen nach wie vor eine große Rolle spielt und sich die Fallzahlen seit dem Aufkommen des Phänomens im Jahr 2011 auf einem anhaltend hohen Niveau befinden. Nach der Infizierung mit der Malware zeigt der Rechner des Geschädigten in der Regel einen Sperrbildschirm und hat zur Folge, dass der berechtigte Nutzer des Rechners diesen ganz oder teilweise nicht mehr nutzen kann. Ein Zugriff auf das System und die gespeicherten Daten ist nicht mehr möglich. Für die vermeintliche Freigabe des Computers bzw. der Daten wird eine Zahlung von meist 100 Euro über bargeldlose Zahlungsmittel wie Paysafecard verlangt.

Nach Medienberichten sind inzwischen sogenannte Toolkits für Ransomware über das Internet erhältlich. Für 100 US Dollar erhält der Benutzer ein Baukastensystem, mit dem er sich eigene Ransomware-Varianten erstellen und verschiedene Funktionen auswählen kann. Damit sind nun auch Nicht-Programmierer in der Lage, Ransomware zu verbreiten.

Bemerkenswert unter den vielen Sperrbildschirmvarianten des Jahres 2013 waren vor allem Versionen, die ihren vermeintlich offiziellen Charakter mit den Namen „Bundesamt für Sicherheit in der Informationstechnik“, „Gesellschaft zur Verfügung von Urheberrechtsverletzungen e. V.“ (GVU), dem „Bundeskriminalamt in Baden-Württemberg (BW)“ und dem „Bundesnachrichtendienst“[4] darstellten. Die Begriffe wurden mit einer Vielzahl von Symbolen, beispielsweise dem Bundesadler oder dem Wappen des Bundesnachrichtendienstes untermauert. Die erwünschte Aussagekraft wurde in einigen Varianten zusätzlich durch ein Bild der Bundeskanzlerin Angela Merkel in energischer Pose sowie das des baden-württembergischen Ministerpräsidenten Winfried Kretschmann unterstrichen. Eine weitere Version zeigte Bundespräsident Joachim Gauck zusammen mit Bundeskanzlerin Angela Merkel. Auch ein Countdown-Zähler, der von 48 Stunden auf null rückwärts zählt, um die Bezahlfrist zu unterstreichen, wurde von den Tätern in einigen Versionen eingeführt. In einer anderen Variante wurde zum ersten Mal die „Bundesnetzagentur“ in einer Symbolik mit Bundesadler

[4] *Die Bezeichnungen wurden jeweils aus dem Original übernommen.*

ins Spiel gebracht. Im Unterschied zu den bislang bekannten Ransomware-Varianten schaltete diese das Browserfenster in den Vollbildmodus, welcher über gängige Tastenkombinationen nicht reversibel ist. Außerdem wird suggeriert, dass eine Verschlüsselung der Daten des Rechners stattfindet, welche aber tatsächlich technisch nicht vorgenommen wird. Mitte des Jahres 2013 wurde eine bislang unbekannte Variante dieses „Browlock"-Trojaners erstmals auf einem Rechner mit dem Betriebssystem Mac OS und dem Safari-Browser festgestellt. Zuvor waren hauptsächlich Windows-Betriebssysteme von derartigen Erpressungstrojanern befallen. Aufgrund dieser aktuellen Erkenntnisse wird der neuen Schadsoftwarevariante hinsichtlich des Gefährdungspotentials eine neue Bedeutung zugewiesen, da nun definitiv auch andere Betriebssysteme wie Mac OS bzw. Linux-Systeme infiziert werden können. Daneben existieren inzwischen Varianten, bei denen eine Verschlüsselung der Daten tatsächlich stattfindet – liegen keine aktuellen Datensicherungen durch den Geschädigten vor, sind die persönlichen oder auch geschäftlichen Daten verloren, denn die Zahlung des Geldbetrags führt entgegen der Erwartung in aller Regel nicht zur Entsperrung bzw. Entschlüsselung des Rechners. Eine neue Stufe erreichten Ransomware-Varianten, die den Geschädigten den Besitz von Kinderpornografie vorwarfen und zu diesem Zweck mehrere vermeintliche „Beispielbilder" darstellten, die zumindest jugendpornografische, teilweise vermutlich sogar kinderpornografische, Bilder unter dem Namen des BKA, des BSI oder der GVU in ihre Bildschirmmitteilung zeigten. Eine detailliertere Einschätzung konnte aufgrund der Größe der gesicherten Bilder nicht abschließend getroffen werden.

Anlagen | **9-12**

CYBERCRIME TATMITTEL (INTERNETKRIMINALITÄT)

Der deutliche Rückgang der in der PKS registrierten Kriminalität des letzten Jahres hat sich bei der Internetkriminalität im Jahr 2013 nicht fortgesetzt. Im Jahr 2013 wurde ein statistischer Anstieg um 11,2 % auf 18.804 Fälle verzeichnet. Das Niveau der Jahre 2009 bis 2011 wurde damit jedoch nicht wieder erreicht.

Bei den Straftaten gegen die sexuelle Selbstbestimmung ist eine Zunahme von 637 auf 851 Fälle festzustellen. Dies stellt einen Spitzenwert im Fünfjahresvergleich dar. Die Aufklärungsquote erreicht mit 91,7 % ebenfalls den höchsten Wert der letzten Jahre. Zu beachten ist jedoch, dass gewisse statistische Schwankungen bei Sexualdelikten normal sind. Ursachen für den Anstieg der Aufklärungsquote sind nicht erkennbar. Maßgeblich für den Anstieg der Fallzahlen ist der sexuelle Missbrauch mit einem Anstieg von 132 auf 188 Fälle und die Verbreitung pornografischer Schriften mit einem Anstieg von 498 auf 657 Fälle. Detailliertere Ausführungen zu diesen Deliktsbereichen sind unter der Überschrift Ansprechstelle Kinderpornografie dargestellt.

Einen starken Einfluss auf die Gesamtentwicklung der Straftaten Cybercrime Tatmittel haben stets die Vermögens- und Fälschungsdelikte. Während in den letzten beiden Jahren Rückgänge im vierstelligen Bereich zu verzeichnen waren, wurde im Jahr 2013 wieder ein Anstieg von 12.219 auf 13.593 Fälle festgestellt. Dies stellt im Fünfjahresvergleich dennoch einen niedrigen Wert dar. Für den Anstieg bei den Vermögens- und Fälschungsdelikten ist der Warenbetrug maßgeblich verantwortlich. Es wurde ein Anstieg von 3.402 auf 4.363 Fälle registriert. Weitere Anstiege gibt es bei Warenkredit-

betrug, Betrug mit rechtswidrig erlangten unbaren Zahlungsmitteln und den sogenannten weiteren Betrugsarten sowie dem Gebrauch von gefälschten Karten/Vordrucken.
Bei den sonstigen Straftatbeständen des StGB ist nach einem geringen Rückgang im Jahr 2012 wieder ein Anstieg von 3.021 auf 3.341 Fälle festzustellen. Angestiegen ist der Deliktsbereich Datenveränderung/Computersabotage mit einem Plus von 33,9 % auf 342 Fälle. Mitursächlich für den Anstieg bei den sonstigen Straftatbeständen ist zudem das Phänomen Ransomware (auch als digitale Erpressung bezeichnet), das als Erpressung mit Tatmittel Internet mit 476 Fällen (+ 314 Fälle) erfasst wurde. Zu beachten ist jedoch, dass die Mehrheit der Ransomware-Fälle nach den derzeitig gültigen PKS-Richtlinien nicht statistisch erfasst werden darf, da der Tatort als Handlungsort des Täters häufig im Ausland liegt und für die Erfassung in der PKS ein Inlandstatort erforderlich ist.
Bei den strafrechtlichen Nebengesetzen wurde ein geringer Rückgang von 691 auf 664 Fälle verzeichnet. Bei einzelnen Delikten gibt es dennoch Veränderungen. Straftaten nach dem Urhebergesetz (UrhG) sind von 572 auf 471 Fälle zurückgegangen. Innerhalb der UrhG-Verstöße ist ein Rückgang von privater und gewerbsmäßiger Softwarepiraterie festzustellen, während Verstöße gegen das Kunsturhebergesetz um 65 Fälle auf 145 Fälle zugenommen haben. Auffällig ist zudem die Entwicklung der Rauschgiftdelikte gemäß Betäubungsmittelgesetz (BtMG). Die Fallzahlen stiegen von 47 auf 101 Fälle. Dieser Anstieg ist auf eine Zunahme bei Verstößen mit den sog. sonstigen Betäubungsmitteln zurückzuführen. Hierunter fallen die neuen psychoaktiven Substanzen, d. h. Kräutermischungen und Research Chemicals, die zunehmend im Internet gehandelt werden.
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. Informationen zur Internetkriminalität finden sich deshalb auch in den anderen Jahresberichten des LKA BW. Beispielsweise werden die Zusammenhänge und Bezüge von Organisierter Kriminalität und Bandenkriminalität zu Cybercrime 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 dazu sind dem Jahresbericht „Politisch Motivierte Kriminalität“ des LKA BW zu entnehmen. Eine ausführliche Betrachtung der Vermögensdelikte und der Wirtschaftskriminalität sowie deren Bezüge zu Cybercrime sind im Jahresbericht „Wirtschaftskriminalität“ zu finden.

ANSPRECHSTELLE KINDERPORNOGRAFIE

Die Ansprechstelle Kinderpornografie (ASt KiPo) ist der Inspektion 510 des LKA BW angegliedert. Sie ist die zentrale Ansprech- und Koordinierungsstelle des Landes für den Straftatenkomplex Besitz/Verschaffen und Verbreitung von Kinderpornografie. Die beiden Bereiche Besitz/Verschaffen und Verbreitung von kinderpornografischen Schriften sind aufgrund der engen Beziehung zueinander bei der Bearbeitung von Ermittlungsverfahren stets zusammen zu betrachten. Ob ein solches Ermittlungsverfahren wegen der Verbreitung von kinderpornografischen Schriften an die Staatsanwaltschaft vorgelegt werden kann, stellt sich zumeist erst nach der Auswertung aller Beweismittel heraus. Kann dieser Nachweis der Verbreitung nicht geführt werden, wird der Vorgang wegen Besitzes von kinderpornografischen Schriften der Staatsanwaltschaft vorgelegt.

Anlagen | 13, 14

FALLZAHLEN KINDERPORNOGRAFIE

Im Deliktsbereich Besitz/Verschaffen kinderpornografischer Schriften ist für das Jahr 2013 ein Anstieg der Fallzahlen um 23,0 % auf 492 Fälle zu verzeichnen. Diese Deliktsform wird vorwiegend über das Internet begangen. Die Fallzahlen mit Sonderkenner „Internet“ (Tatmittel Cybercrime), stellen eine Teilmenge der 492 Gesamtfälle dar und erhöhten sich korrespondierend um 16,5 % auf 317 Fälle. Die Zahl der polizeilich registrierten Straftaten der Verbreitung von kinderpornografischen Schriften stieg um 201 Fälle, was einer Zunahme um 26,4 % entspricht. Der Anteil der Straftaten mit Tatmittel Cybercrime hat dabei um 13,3 % auf 136 Fälle zugenommen.
Die Entwicklung des Gesamtbereichs Besitz/Verschaffen und Verbreitung kinderpornografischer Schriften bewegt sich mit 693 Fällen auf gleichbleibendem Niveau der Vorjahre (Jahr 2012: 559, Jahr 2011: 630, Jahr 2010: 607, Jahr 2009: 652 Fälle).

OPERATIONEN / UMFANGSVERFAHREN

Die ASt KiPo bearbeitete im Jahr 2013 66 Sammelverfahren (sog. Umfangsverfahren) mit 534 Tatverdächtigen in Baden-Württemberg. Allein 15 Umfangsverfahren gingen aus Verfahren hervor, die in Baden-Württemberg geführt oder initiiert wurden.
Herausragend ist ein Umfangsverfahren mit Ursprung in Niedersachsen, in dessen Verlauf Nutzer protokolliert wurden, die auf eine bestimmte Webseite mit kinderpornografischen Inhalten im Internet zugegriffen haben. Nach einer Auswertung dieser Daten konnten allein in Baden-Württemberg 268 Ermittlungsverfahren wegen des Verdachtes des Besitzes kinderpornografischer Schriften eingeleitet werden. Bei einem Beschuldigten wurden Videodateien aufgefunden, in denen er selbst den mehrfachen schweren sexuellen Missbrauch an seiner 10-jährigen Tochter dokumentiert hat.

BEKÄMPFUNG DES SEXUELLEN MISSBRAUCHS VON KINDERN UND DER KINDERPORNOGRAFIE

Im Bereich der Auswertung von Bild- und Videodateien und deren Bewertung stellt die Verwendung von Hashwerten eine verlässliche Methode zur automatisierten Datenselektion und -reduktion dar. Die Datenmengen, mit denen die Polizei konfrontiert ist, nehmen stetig zu. Dies wird anhand der von den Landespolizeidienststellen an die Ast KiPo übersandten Datenmengen deutlich. Im Jahr 2013 wurden bei 35 Anlieferungen 1.346.194 Bilder und Videos an die ASt Kipo übermittelt.
Der hohe Anstieg im Vergleich zum Vorjahr resultiert aus einem Verfahren der Polizeidirektion Böblingen. Auch im Bereich der Bekämpfung des sexuellen Missbrauchs und der Kinderpornografie zeigt sich deutlich die Zunahme der Speicherkapazitäten. Handelsübliche Speicher sind in den letzten Jahren deutlich größer und billiger geworden. Damit steigt auch die Möglichkeit, große Bild- und Videosammlungen anzulegen.

LÖSCHUNG VON INTERNETSEITEN MIT KINDERPORNOGRAFISCHEM INHALT

Das Bundeskriminalamt (BKA) ist zuständig für die Überwachung des Löschens von ausländischen Internetseiten mit kinderpornografischen Inhalten. Die abgestimmte Jahresstatistik 2013 liegt derzeit noch nicht vor. Laut der mit den Internet-Beschwerdestellen abgestimmten Jahresstatistik 2012 des BKA wurden im Jahr 2012 5.463 URLs (Jahr 2011: 3.828 URLs) weltweit festgestellt. Zusätzlich wurden 545 TOR-Webseiten ermittelt. Auf inländische URLs entfallen davon 24 % (1.336), auf im Ausland registrierte URLs 76 % (4.127). Laut Statistik gingen 71 % (3.833) der Hinweise über die Hotlines der Beschwerdestellen ein, von deutschen Polizeidienststellen 28 % (1.502). 89 % der deutschen URLs waren auf Anforderung nach zwei Tagen gelöscht. Nach einer Woche waren es 98 %. Bei ausländischen URLs waren nach einer Woche noch 27 % verfügbar. Nach vier Wochen waren auch dort 97 % nicht mehr erreichbar.
Durch das BKA wurde im Rückblick auf die letzten drei Jahre ein Anstieg der Meldungen bezüglich ausländischen URLs festgestellt. Die URLs mit kinderpornografischen Inhalten werden mehrheitlich in den USA (31 %), Russland (28 %) und in den Niederlanden (20 %) gehostet.

VERBREITUNG VON KINDERPORNOGRAFIE IN TAUSCHBÖRSEN

Das Landeskriminalamt Hamburg teilte im September 2013 mit, dass durch Initiativermittlungen des AIR ein andauernder sexueller Missbrauch eines sechsjährigen Mädchens beendet werden konnte. Im Rahmen der dort durchgeführten Ermittlungen konnten bei der Auswertung eines Mobiltelefons des Beschuldigten mehrere Filme gesichert werden, die den Missbrauch eines Kindes zeigten.
Das Kind wurde schließlich als Tochter der Lebensgefährtin des Beschuldigten identifiziert.
Der Beschuldigte wurde im September 2013 durch das Landgericht Hamburg zu fünfeinhalb Jahren Unterbringung in einem psychiatrischen Krankenhaus gem. § 63 StGB verurteilt.

ARBEITSBEREICH INTERNETRECHERCHE

INITIIERUNG VON ERMITTLUNGSVERFAHREN

Im Rahmen zweier Operationen wegen Verdachts der Verbreitung von Kinderpornografie in Tauschbörsen wurden durch den AIR im Berichtszeitraum weltweit 5.716 Strafverfahren initiiert, davon 25 in Baden-Württemberg (bundesweit: 297 Strafverfahren). Durch den Rücklauf der mit den Operationen verbundenen Erkenntnisanfragen wurde festgestellt, dass mehrere Tatverdächtige bereits Vorstrafen im Bereich der schweren sexuellen Missbrauchshandlungen zum Nachteil von Kindern hatten. Zudem können aufgrund derartiger Operationen in Einzelfällen ebenfalls anhaltende Missbrauchshandlungen aufgedeckt und damit unterbunden werden.

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 I 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. Diskussionen um die Vorratsdatenspeicherung werden teilweise unpräzise geführt. Verschiedene Datenarten wie Bestandsdaten, Verkehrsdaten und Inhaltsdaten werden in der Diskussion thematisch vermischt. Dies wird der Bedeutung dieses Themas im notwendigen gesamtgesellschaftlichen Diskurs nicht gerecht. Festzustellen ist, dass es nach dem Wegfall der Vorratsdatenspeicherung kein einheitliches Speicherverhalten der Provider mehr gibt. Die Dauer der Speicherung der Verkehrsdaten obliegt aufgrund der Freiwilligkeit dem Ermessen der Verpflichteten und variiert zwischen null und sieben Kalendertagen. Da Straftaten allerdings häufig erst bekannt werden, nachdem die Daten bereits gelöscht oder anonymisiert sind, erschwert die fehlende Vorratsdatenspeicherung die Ermittlungen erheblich oder macht sie unmöglich. Selbst bei unverzüglich durchgeführten Bestandsdatenanfragen – abhängig vom angefragten Provider – besteht das Risiko einer sogenannten Nichtbeauskunftung. Es bleibt also damit nur dem Zufall überlassen, ob der Täter, bzw. der Anschlussinhaber/Nutzer der IP-Adresse, durch eine Bestandsdatenauskunft identifiziert werden kann oder nicht.

Bei den Ermittlungen des AIR im Jahr 2013 konnten bei 64 der 297 in Deutschland initiierten Fälle (22 %) die Ermittlungen gegen deutsche Tatverdächtige nicht weitergeführt werden, da Bestandsdatenanfragen an die Provider negativ beauskunftet wurden. Das bedeutet, dass keine Daten gespeichert waren, selbst in den Fällen, in denen der Täter zum Moment der Bestandsdatenabfrage noch im Internet online war. In einzelnen Operationen in den vergangenen Jahren lag der Anteil der Fälle, die aufgrund fehlender Datenspeicherung nicht mehr verfolgt werden konnten, bei über 50 %.
Im Ergebnis bleibt festzustellen, dass die Verbreitung kinderpornografischer Dateien im Bereich der Netzwerke und damit auch die Beendigung von laufenden Missbrauchshandlungen ohne Vorratsdatenspeicherung derzeit nur unzureichend verfolgt werden kann.

GEFÄHRDUNGSLAGEN

Der AIR bearbeitete im Berichtszeitraum 19 Gefährdungslagen (17 Suizidankündigungen und zwei Amokandrohungen), die über Dienstanbieter sozialer Netzwerke mitgeteilt bzw. dem LKA BW von Dritten übermittelt worden sind. Das Antwort-Zeit-Verhalten deutscher Dienstanbieter kann als überwiegend positiv bezeichnet werden. Bei den vorwiegend amerikanischen Anbietern sozialer Netzwerke wurde hingegen ein unterschiedliches Auskunftsverhalten festgestellt. Bereits Ende 2011 wurden deutsch-amerikanische Konsultationen durchgeführt, bei denen das US-Department of Justice als maßgebliche US-amerikanische Einrichtung beteiligt war. Im Ergebnis wurde die Duldung direkter Kontaktaufnahmen deutscher Strafverfolgungsbehörden mit US-amerikanischen Dienstanbietern bei der Bearbeitung von Gefahrenlagen wie Amok- und Suizidandrohungen vereinbart.
Die Herausgabe der Daten erfolgt seitens US-Unternehmen auf freiwilliger Basis. Die Dienstanbieter müssen jedoch grundsätzlich im Einzelfall zunächst vom Vorliegen eines Notfalls[5] argumentativ überzeugt werden. Dies war nach eigenen Erfahrungen in der Vergangenheit nicht immer erfolgreich. Obwohl eine polizeiliche Bewertung der Gefahrenlage vorlag und eine Vielzahl von Informationen zum Gefährdungssachverhalt in englischer Sprache vorgelegt wurde, ist eine Herausgabe entsprechender Informationen teilweise verweigert worden.

[5] *US-amerikanische Dienstanbieter sind gesetzlich verpflichtet, sich zu überzeugen, dass ein Notfall besteht, der mit einer „unmittelbaren Gefahr des Todes oder der ernsthaften körperlichen Verletzung einer Person" einhergeht (die hypothetische Möglichkeit einer Gefahr reicht für die Erfüllung dieses Prüfmerkmals nicht aus), und aufgrund dieser Gefahr eine unverzügliche Herausgabe der Informationen erforderlich ist.*

PHÄNOMENE

ANRUFE ANGEBLICHER MITARBEITER VON NAMHAFTEN UNTERNEHMEN DER IT-BRANCHE

Wie schon im Vorjahr kam es auch im Laufe des Jahres 2013 bundesweit immer wieder zu Fällen von Anrufen angeblicher Mitarbeiter von namhaften Unternehmen der IT-Branche[6]. Die Anrufe erfolgten in der Regel mit unterdrückter oder ausländischer Rufnummer auf den Festnetzanschluss des Geschädigten. In englischer Sprache teilte 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 versuchten die Täter, über das Internet weitere Schad- oder Fernwartungssoftware auf dem Rechner des Angerufenen zu installieren oder Schutzsoftware (wie Anti-Viren-Software) zu deinstallieren. Schließlich wurde 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. Alternativ forderten die Täter für die geleistete Arbeit eine Gebühr. 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, alternativ oder zusätzlich die Daten seiner Kreditkarte oder den Zugang zum Online-Banking, zu erlangen. Bei Preisgabe der Kreditkartendaten, besteht zudem im Anschluss die Gefahr, dass diese im Nachhinein der mehrfachen missbräuchlichen Verwendung dienen. Alle bisherigen Geschädigten geben an, dass die unbekannten Anrufer während des gesamten Telefonats nur in schlechtem Englisch mit indischem Akzent gesprochen haben. Weiterhin glaubten einige der Geschädigten, dass sie im Hintergrund Geräusche ähnlich einem Callcenter gehört hätten. Die Telefonnummern der Geschädigten dürften die Täter vermutlich dem öffentlichen Telefonbuch entnommen haben. In den bislang bekannten Fällen hat sich aufgrund weiterer Ermittlungen gezeigt, dass diese Anrufe offensichtlich aus dem Ausland kamen. Aufgrund der Verschiedenartigkeit der vermeintlichen Herkunftsländer ist aber von einer Verschleierung über das Internet auszugehen. Zudem ist aufgrund der Häufung der Vorfälle zum Jahresende 2013 hin und dem offensichtlich in vielen Fällen erfolgreichen Vorgehen der Täter mit einigen Nachahmern zu rechnen. Laut einer Lagebild-Land-Auswertung für das Jahr 2013 sind in Baden-Württemberg 112 Fälle zu verzeichnen. Es muss von einem hohen Dunkelfeld ausgegangen werden.

[6] *Das LKA BW verzichtet an dieser Stelle auf die Nennung des Unternehmens, da der Modus Operandi problemlos die Möglichkeit bietet, den Firmennamen zu wechseln, unter dem die angebliche Mitarbeiterin/der angebliche Mitarbeiter anruft.*

PHISHING IM ZUSAMMENHANG MIT ONLINE-BANKING

Bundesweit kommt es seit Mitte des Jahres 2013 vermehrt zu Fällen zum Nachteil von Kunden der Sparkassen, in denen Anrufe angeblicher Mitarbeiter der örtlichen Sparkasse mit dem Erhalt von sogenannten Phishing-Mails einhergehen. Einige Tage vor der eigentlichen Tatausführung werden den jeweiligen Geschädigten Phishing-Mails übersendet. Mit Layout der Sparkasse wird den Geschädigten suggeriert, dass Sicherheitsprobleme durch das Aufspielen eines neuen Updates geschlossen werden sollten. Hierzu wird in der E-Mail jeweils ein Link angegeben, den die Geschädigten aufrufen sollen. Danach öffnet sich ein Popup-Fenster, in das persönliche Daten wie z. B. die Zugangsdaten und die Handynummer einzutragen sind. Wenige Stunden später werden die Geschädigten von einer angeblichen Mitarbeiterin des Bankinstituts mit zumeist unterdrückter Rufnummer angerufen.
Als Begründung wird u. a. ein notwendiger Datenabgleich hinsichtlich der Umstellung zum SEPA-Verfahren angegeben. Die Kunden werden in dem Gespräch aufgefordert, ihre TAN-Generatoren manuell zu bedienen und die jeweiligen TANs telefonisch durchzugeben. Eine widerrechtliche Abbuchung lässt dann meist nicht lange auf sich warten.

DIGITALE FORENSIK

AUFTRAGSAUFKOMMEN

Das landesweite Auftragsaufkommen wird seit dem Jahr 2006 statistisch erfasst. Im Jahr 2006 wurden 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. Im Jahr 2012 hätte sich statistisch eine Trendwende andeuten können, es wurde nur ein moderater Anstieg festgestellt. Diese Trendwende hat sich mit Blick auf die neuen Aufträge des Jahres 2013 mit 11.225 Aufträgen nicht bestätigt. Vielmehr hat sich der Anstieg der Vorjahre wieder fortgesetzt.

TECHNISCHE KOMPLEXITÄT UND STEIGENDE DATENMENGEN

Die zunehmende technische Komplexität der IT-Systeme und die ständig steigende Datenmengen auf Grund der kontinuierlich ansteigenden Datenträgerkapazitäten und deren Verbreitung stellen nach wie vor große Herausforderungen im Bereich der IT-Beweissicherung dar.
Im Jahr 2013 mussten beispielsweise in einem einzelnen Verfahren 70 TB Daten aus zahlreichen Asservaten beim LKA BW gesichert und aufbereitet werden. Die Verarbeitung solcher Datenmengen bringen die eingesetzte Hard- und Software an die Grenzen der Leistungsfähigkeit.

DATENANALYSE

Die Analyse und Auswertung strukturierter Massendaten bezieht sich in erster Linie auf Funkzellendaten. Die Analyse von Funkzellendaten stellt einen Schwerpunkt der Tätigkeit der Datenanalysten dar, ist jedoch nicht darauf beschränkt.

KOMPETENZZENTRUM TELEKOMMUNIKATIONSÜBERWACHUNG (TKÜ)

Der moderne Kommunikationsmarkt ist von rasanten Entwicklungen geprägt. Übertragungsgeschwindigkeiten, Bandbreiten und Datenmengen nehmen stark zu. Darüber hinaus zeichnet er sich durch eine zunehmende Verschlüsselung der Kommunikationsinhalte, technisch bedingte oder absichtlich erzeugte Anonymisierung von Teilnehmeranschlüssen, Internationalisierung und die Einführung neuer technischer Standards aus.
Herkömmliche Kommunikationsdienste und Internet verschmelzen miteinander und führen zu einer steigenden Anzahl an Kommunikationsmöglichkeiten und vielfältigen Nutzungsmöglichkeiten. 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 TKÜ muss begegnet werden, sonst entzieht sich die gesamte beweiserhebliche Täterkommunikation den Strafverfolgungsbehörden. Weitere Herausforderungen ergeben sich aus einer Zunahme an Beratungstätigkeit, Schulungen und Projektarbeiten.

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

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.

MOBILFUNKAUFKLÄRUNG

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

MASSNAHMEN

2 MASSNAHMEN / HANDLUNGSEMPFEHLUNGEN

ÜBERSICHT

- Vorbereitungsmaßnahmen für die Polizeireform zum 1. Januar 2014
- Aufbau eines leistungsfähigen landesweiten Netzwerks von Fachdienststellen
- Bearbeitung von Handlungsempfehlungen aus der Gesamtkonzeption „Cyberkriminalität/ Digitale Spuren“
- Einführung der Sonderlaufbahn Cyberkriminalist im Jahr 2014
- Realisierung einer 24/7-Erreichbarkeit der ZAC
- Verstärkung der ZAC-Maßnahmen (z. B. Vortragstätigkeiten)
- Empfehlung der weiteren Aufhellung des Dunkelfeldes
- Verbesserungen bei der Erfassung von Auslandsstraften und Geschädigtenzählung in der PKS
- Optimierung der PKS- und POLAS-Erfassung in Zusammenhang mit Ransomware
- Notwendige personelle Verstärkung für die Ansprechstelle Kinderpornografie
- Weitere bundesweite Abstimmung der Schulfahndung
- Verbesserung der Bekämpfung von Cybergrooming; Umsetzung der EU-Richtlinie 2011/92/EU
- Notwendige Regelung der Vorratsdatenspeicherung
- Ergebnisse des Techniker-Workshops 2013
- Ergänzende Regelungen für die Datenanalyse
- Fortentwicklung des Kompetenzzentrums TKÜ BW
- Präventionsangebote für alle
- Präventions- und Informationsangebote für die Polizei

POLIZEIREFORM 2014

Am 1. Januar 2012 wurde die Abteilung Cybercrime/Digitale Spuren im LKA BW eingerichtet. Seitdem wurde die Abteilung kontinuierlich personell verstärkt, so dass zum Jahresbeginn 2014 rund 100 Mitarbeiterinnen und Mitarbeiter in der Abteilung tätig sind und ihre jeweiligen fachlichen Expertisen unterschiedlichster Art einbringen. Dies ist Ausdruck der Schwerpunktsetzung des LKA BW in diesem Deliktsfeld. Mit Umsetzung der Polizeireform zum 1. Januar 2014 wurden in Baden-Württemberg durch Zusammenlegung bestehender Polizeipräsidien und Polizeidirektionen zwölf leistungsstarke Polizeipräsidien geschaffen. Die Krimimalinspektionen 5 (K 5) in diesen Polizeipräsidien sind zuständig für die Bearbeitung von Cybercrime-Delikten und damit neu geschaffene Partner der Abteilung Cybercrime/Digitale Spuren des LKA BW. Sie bilden ein leistungsfähiges Netzwerk an Fachdienststellen für die Bekämpfung von Cybercrime und die Bearbeitung digitaler Spuren.

MASSNAHMEN

Die Kriminalinspektionen bestehen aus den Bereichen Ermittlungen, Auswertung sowie IT-Beweissicherung und spiegeln in weiten Teilen den Aufbau der Abteilung im LKA BW wieder.
Deshalb wurde dort auch der Aufgabenbereich Datenanalyse (ehemals Auswertung strukturierter Massendaten) angesiedelt. Durch die Abteilung Cybercrime/Digitale Spuren des LKA BW werden landesweite Serviceleistungen und Ermittlungsunterstützung angeboten. Hierzu gehören der Arbeitsbereich Internetrecherche (AIR) und die Ansprechstelle Kinderpornografie (ASt KiPo) sowie Betrieb der landesweiten Telekommunikationsüberwachungs (TKÜ)-Anlage. Ebenso die Elektronische Schnittstelle Behörden (ESB), die zentralen Rechnungsprüfung TKÜ-Maßnahmen, die Operative Netzwerkforensik (OIT) und die Mobilfunkaufklärung.

GESAMTKONZEPTION „CYBERKRIMINALITÄT / DIGITALE SPUREN"

Das LKA BW wurde durch das Innenministerium Baden-Württemberg, Landespolizeipräsidium (IM -LPP-), beauftragt, eine landesweite Gesamtkonzeption „Cyberkriminalität/Digitale Spuren" zu erstellen. Diese Konzeption wurde am 1. Februar 2013 dem IM -LPP- vorgelegt. Die Gesamtkonzeption wurde zuvor innerhalb der Projektstruktur zur Polizeireform mit Vertretern der Landespolizei und des IM -LPP- abgestimmt. Mit der Gesamtkonzeption sollen landesweit die Aufgabenfelder und -abgrenzungen bei der Bekämpfung und Bearbeitung von Delikten der Cybercrime, Fachaufsicht, Personal und Personalausstattung, Aus- und Fortbildung, technische Ausstattung und deren Beschaffung, Raumbedarf sowie Gremienarbeit im Themenfeld Cybercrime geregelt werden. Im Rahmen der Erarbeitung der Konzeption wurden 25 Handlungsempfehlungen erstellt. Zur Bearbeitung der Umsetzung der Handlungsempfehlungen wurde eine Teamsite eingerichtet. Landesweit wurden die beauftragten Mitglieder der Arbeits- und Projektgruppen berechtigt. Gegenüber dem IM -LPP- besteht quartalsweise eine Berichtspflicht. Ein Teil der Handlungsempfehlungen wurde vor bzw. mit Umsetzung der Polizeireform im Jahr 2014 umgesetzt. Mittel- und langfristig angelegte Handlungsempfehlungen sind derzeit noch in Bearbeitung bzw. in der letzten Abstimmung innerhalb der Arbeitsgruppen und Projekte.

SONDERLAUFBAHN CYBERKRIMINALIST

Baden-Württemberg hat im Jahr 2012 die Einführung der Sonderlaufbahn Cyberkriminalist beschlossen und im Jahr 2013 die Rahmenbedingungen dafür geschaffen. Neben den notwendigen Anpassungen der Laufbahnverordnung der Polizeibeamten wurden innerdienstliche Anordnungen getroffen, die analog der Sonderlaufbahn der Wirtschaftskriminalisten die neue Sonderlaufbahn Cyberkriminalist regeln. Weiterhin wurde das Fortbildungskonzept erarbeitet und abgestimmt. Es ist vorgesehen im Jahr 2014 15 Stellen zu besetzen. Die Stellen wurden Ende 2013 landesweit ausgeschrieben und Auswahlverfahren durchgeführt. Bewerben konnte sich, wer

- ein mindestens drei Jahre dauerndes Hochschulstudium (FH, DHBW, BA oder vergleichbare Bildungseinrichtung) in einem für die Bearbeitung von Cybercrimedelikten geeigneten Studiengang mit mindestens befriedigend bestanden und
- nach Abschluss des Studiums mindestens drei Jahre eine für die Laufbahn einschlägige Tätigkeit ausgeübt hat.

Die Ausbildung und formelle Einstellung der Cyberkriminalisten beginnt am 1. April 2014.
Die Cyberkriminalisten werden im Eingangsamt des gehobenen Dienstes (A9) eingestellt und zur Kriminalkommissarin/zum Kriminalkommissar auf Probe ernannt.

ZENTRALE ANSPRECHSTELLE CYBERCRIME

Die ZAC hat die 24/7-Erreichbarkeit realisiert. Über die zentrale E-Mail-Anschrift cybercrime@polizei.bwl.de oder die Telefonnummer 0711/5401-2444 ist die ZAC erreichbar. Beginnend ab Oktober 2013 wurde und wird die ZAC aktiv nach außen hin als Ansprechpartner beworben. Es wurden beispielsweise Handreichungen/Plakate erstellt und die Vortragstätigkeiten wurden intensiviert und ausgebaut. Partner sind hierbei die Industrie- und Handelskammern, aber auch Verbände und Organisationen. Ein weiterer Ausbau sowie diverse Veranstaltungen sind für das Jahr 2014 vorgesehen.
Die ZAC ist zudem die Schnittstelle für viele Kooperationen, beispielsweise mit dem Landeskriminalamt Nordrhein-Westfalen und des BITKOM e. V.[7] oder der Allianz für Cybersicherheit, welcher das LKA BW in der Rolle eines Multiplikators angehört.

DUNKELFELD

Das Bundesland Niedersachsen ist ein einwohnerstarkes Flächenland, das in weiten Teilen mit Baden-Württemberg vergleichbar ist. Die Ergebnisse der Dunkelfeldstudie des Landes Niedersachsen aus dem Jahr 2013 sind auf die Verhältnisse in Baden-Württemberg somit durchaus übertragbar. Insbesondere im Bereich des Cybercrime-Dunkelfeldes sind nach Ansicht des LKA BW keine wesentlich anderen Werte und Ergebnisse zu erwarten. Die polizeiliche Schwerpunktsetzung in der Aufhellung dieses Dunkelfeldes ist deswegen richtig und muss weiter ausgebaut werden.

PKS-ERFASSUNG VON AUSLANDSSTRAFTATEN UND GESCHÄDIGTENZÄHLUNG

Zur besseren Abbildung von Cybercrime in der PKS wurden im Jahr 2013 die Arbeiten der bundesweiten Arbeits- und Projektgruppen bzw. die Gremienarbeit fortgesetzt.
Mit der Thematik Erfassung von Geschädigten in der PKS waren die Bund-Länder-Projektgruppe „Geschädigtenerfassung“ der Kommission PKS und die Unterarbeitsgruppe „Erfassungskriterien für eine Geschädigtenzählung in der PKS“ der Leitertagung Cybercrime befasst. Die Unterarbeitsgruppe

[7] *Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (Branchenverband der deutschen Informations- und Telekommunikationsbranche, der mehr als 2.100 Unternehmen vertritt).*

hat für den Bereich Cybercrime einen Bericht (Stand: 27. Januar 2014) vorgelegt. Dieser fließt in die Arbeit der übergreifenden Bund-Länder-Projektgruppe „Geschädigtenerfassung“ ein.
Ein weiterer Punkt ist die Prüfung der Möglichkeit einer zukünftigen Erfassung von Auslandsstraftaten in der PKS. Die derzeit gültigen PKS-Richtlinien sehen nach dem Territorialitäts- und dem Flaggenprinzip der §§ 3, 4 StGB vor, dass in der PKS nur Straftaten erfasst werden, die in diesem Geltungsbereich des deutschen Strafrechts begangen werden. Dies hat u. a. zur Folge, dass Tathandlungen, die im Ausland erfolgen, sich aber im Inland auswirken, keinen Eingang in die PKS finden. Aufgrund des grenzüberschreitenden Charakters von Cybercrime-Delikten finden eine Vielzahl bzw. die Mehrzahl der maßgeblichen Tathandlungen im Ausland statt, wirken sich aber auf Geschädigte in Deutschland aus. Diese Fälle finden bislang keinen Eingang in die PKS und verzerren dadurch das Bild. Die tatsächlichen Fallzahlen, deren Bearbeitung auch Ressourcen der Polizei bindet, werden statistisch nicht treffend dargestellt. Hinzu kommt die bereits beschriebene Dunkelfeld-Problematik. Das Lastenheft zur „Weiterentwicklung der Polizeilichen Kriminalstatistik zur Verbesserung der Aussagekraft“ (Stand 22. Februar 2013) wurde in der 172. Tagung der Arbeitsgemeinschaft der Leiter der Landeskriminalämter mit dem Bundeskriminalamt (AG Kripo) am 12./13. März 2013 behandelt und zur Kenntnis genommen. Weiterhin erfolgte eine Erörterung der Thematik auf der 239. Sitzung des Arbeitskreises II (AK II) „Innere Sicherheit“ der Ständigen Konferenz der Innenminister und -senatoren der Länder am 29./30. Oktober 2013. Der AK II beauftragte die AG Kripo, die Arbeiten zur Erfassung von Auslandsstraftaten und zur Anzahl der Geschädigten, insbesondere von Delikten im Bereich Cybercrime, im Erfassungssystem für die PKS fortzusetzen und nach zweijähriger Pilotphase einen Evaluationsbericht vorzulegen.

PKS- UND POLAS-ERFASSUNG – RANSOMWARE

Der seit Anfang des Jahres 2013 auftretende sog. „Windowsverschlüsselungstrojaner“ (WVT) beeinflusst die PKS im Deliktsbereich Datenveränderung/Computersabotage. Der WVT ist eine spezielle Form von Ransomware, die in einem ZIP-Anhang in Verbindung mit einer E-Mail, getarnt als Rechnung bzw. Mahnschreiben, verbreitet wird. Diese Straftaten werden trotz der hiesigen, in der Vergangenheit mehrfach verbreiteten Handlungsempfehlungen zur strafrechtlichen Einordnung in der Regel mit „Führungsdelikt“ Computersabotage/Datenveränderung oder Vorbereitung des Ausspähens von Daten in die PKS eingetragen und unter diesen Deliktschlüsseln angezeigt. Da aktuelle Versionen des von der Ermittlungsgruppe „WVT“ in Niedersachsen bearbeiteten trojanischen Pferdes seit Anfang des Jahres 2013 wieder verstärkt verbreitet wurden, erfuhren diese Deliktschlüssel 2013 einen Anstieg.
Eigentlich dürften Ransomware-Straftaten nach den PKS-Richtlinien zur Tatorterfassung weitgehend keinen Eingang in die polizeiliche Kriminalstatistik finden. Betrachtet man die jeweiligen Einzelfälle, wird schnell klar, dass die statistische Einordnung des Tatorts nach den Richtlinien der PKS derzeit größtenteils nur unzureichend getroffen wird: Nach den PKS-Richtlinien ist eine Erfassung in der

PKS nur zulässig, „wenn konkrete Anhaltspunkte vorliegen, dass im Inland gehandelt wurde". Demzufolge darf eine Freigabe für die PKS nicht erfolgen, wenn der Erfolgsort bzw. der Wohnort des Geschädigten als Tatort erfasst wurde, die Handlung des Täters jedoch im Ausland liegt.
In vielen Fällen wird diese Richtlinie zur Tatorterfassung nicht eingehalten, weswegen einige Fälle in der Landesstatistik auftauchen, die eigentlich nicht gezählt werden dürften. Viele Fälle werden so fälschlicherweise mit dem Wohnort des Geschädigten als Tatort erfasst. Bezüglich der Interpretation der Erfassungsrichtlinien zum Thema „Tatort" bestehen demnach immer noch Defizite.
Darüber hinaus sollten diese Fälle, falls sie einem bundesweiten Sammelverfahren zuzuordnen sind, weder im polizeilichen Auskunftssystem POLAS BW eingetragen, noch in der PKS zählbar sein.
Ist vorab zentral festgelegt, dass Fälle eines bestimmten Phänomens nach Anzeigenaufnahme einer anderen Dienststelle, die über die dortige Staatsanwaltschaft ein Sammelverfahren führt, abzugeben sind, so ist keine POLAS BW-Erfassung vorzunehmen. Erfassende Dienststelle in diesem Zusammenhang ist immer die endsachbearbeitende Dienststelle. Endsachbearbeitende Dienststelle ist diejenige, die das Sammelverfahren führt. Diese nimmt die Eingabe in das jeweilige Landeserfassungssystem vor.

BEKÄMPFUNG DES SEXUELLEN MISSBRAUCHS UND DER KINDERPORNOGRAFIE

Um die immer größer werdende Masse an Daten zu bewältigen, wurde bis April 2012 durch die Sachbearbeiter Kinderpornografie bundesweit das Programm PERKEO (Programm zur Erkennung relevanter kinderpornografisch eindeutiger Objekte, Software zur Feststellung bereits bekannter kinderpornografischer Bild- und Videodateien bei der Auswertung des Datenmaterials i. Z. m. Ermittlungsverfahren wegen des Besitzes bzw. der Verbreitung von kinderpornografischen Schriften) verwendet. Bis zur Umsetzung der derzeit in der Erarbeitung befindlichen bundesweiten Hash-Datenbank Pornografische Schriften (Hash-DB PS) steht eine Übergangslösung zur Verfügung.
Die verstärkte Nutzung technischer Möglichkeiten im Bereich Ansprechstelle Kinderpornografie wird eine personelle Verstärkung zur Folge haben müssen.

SCHULFAHNDUNG

Eine Schulfahndung umfasst Fahndungsmaßnahmen an Schulen mittels Bild- oder Tonaufnahmen von bislang ungeklärten Straftaten, die den Tatbestand des sexuellen Missbrauchs von Kindern darstellen. Primäre Zielrichtung derartiger Schulfahndungen ist die Beendigung andauernder Missbrauchshandlungen durch Identifizierung der Opfer.
Eine Schulfahndung wird als Mindermaßnahme (geringerer Eingriff und geringere sekundäre Viktimisierung des Opfers) zu einer Öffentlichkeitsfahndung gesehen.
Derzeit befinden sich die durch eine bundesweite Arbeitsgruppe erarbeiteten Standards für Fahndungen an Schulen zur Bekämpfung des sexuellen Missbrauchs an Kindern im Abstimmungsprozess mit den Bundesländern.

MASSNAHMEN

CYBERGROOMING

Die EU-Richtlinie 2011/92/EU forderte die Mitgliedsstaaten bereits im Jahr 2011 auf, bezüglich der Kontaktaufnahme zu Kindern für sexuelle Zwecke im Bereich der Strafbarkeit nachzubessern.
Die neue Bundesregierung beabsichtigt, im Bereich des Sexualstrafrechts inakzeptable Schutzlücken zu schließen und fordert das Ermöglichen von einfacheren Meldewegen von Cybergrooming in sozialen Netzwerken.

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 und so die bestehende gesetzliche Lücke nach nun vier Jahren zu schließen.

TECHNIKER-WORKSHOP 2013

Das LKA BW war vom 23. bis 25. April Gastgeber des Techniker-Workshops 2013. Die Inspektion 510 lud nach Beschluss der 16. KaRIn[8]-Tagung im November 2012 in Mainz zu einem länderübergreifenden Techniker-Workshop nach Stuttgart ein. Im LKA BW trafen sich Kollegen aus entsprechenden Arbeitsgebieten des BK Österreich, der Stadtpolizei Zürich, der Fedpol/KOBIK Schweiz, des BKA sowie der Landeskriminalämter der Bundesländer Hessen, Niedersachsen, Nordrhein-Westfalen und Rheinland-Pfalz.
Diese Veranstaltung sollte dazu dienen, Entwicklungen der verschiedenen Bundesländer vorzustellen und auszutauschen sowie die Kontakte zu den jeweiligen Arbeitsbereichen länderübergreifend herzustellen bzw. zu vertiefen. Thematischer Schwerpunkt war dabei die „ermittlungsunterstützende Informatik".
Ebenso wurde die Linux Live-DVD „SBIuKKrim live" vorgestellt. Diese DVD wurde im Rahmen der „Sicherheitsoffensive Polizei 2012" entwickelt und stellt ein auf Ubuntu Linux basierendes Betriebssystem für die Internet-Ermittlungs-PC im Land zur Verfügung. Der Desktop und die Anwendungen sind dabei speziell auf die Bedürfnisse für Ermittlungstätigkeiten im Internet abgestimmt.
Von den Bundesländern wurden verschiedene andere eigenentwickelte Programme vorgestellt, wie beispielsweise ein Facebook-Plugin für den Firefox Web-Browser, Software zur IP-Adressenfeststellung von E-Mail-Inhabern oder Skype-Benutzern sowie der derzeitige Entwicklungsstand der Software „AVIDA" zur Erfassung von Hash-Werten für die zentrale Hash-Datenbank des BKA.
An letzterem Projekt ist auch die Inspektion 510 mit einem Informatiker an der Weiterentwicklung beteiligt. Am Ende der gelungenen Veranstaltung mit erheblichem Wert für alle Teilnehmer wurde eine Fortführung dieses Workshops als wünschenswert erachtet.

[8] *Koordinierungsgruppe für anlassunabhängige Recherchen im Internet. Die Inspektion 510 ist durch den AIR vertreten.*

DATENANALYSE

Unter Federführung des LKA BW hat eine Projektgruppe „Analyse und Auswertung strukturierter Massendaten“ Standards für die zukünftig auch bei den regionalen Polizeipräsiden eingerichteten Arbeitsbereiche „Datenanalyse“ erarbeitet. Die Projektgruppe hat ihre Arbeit noch im Jahr 2013 mit der Vorlage eines Projektgruppenberichts vorläufig abgeschlossen. Zahlreiche Zwischenergebnisse der Projektgruppe sind jedoch bereits im Vorfeld in die parallel laufenden Vorbereitungen zur Umsetzung der Polizeireform eingeflossen und dienen in der Folge als Grundlage und Rahmen für den Aufbau der neuen Arbeitsbereiche bei der Landespolizei ab 1. Januar 2014.

FORTENTWICKLUNG DES KOMPETENZZENTRUMS TKÜ BW

Im Berichtsjahr 2013 wurde eine Projektgruppe eingesetzt, die sich mit der Fortentwicklung des TKÜ-Zentrums in den Folgejahren befasst. Die Einrichtung der Projektgruppe wurde als Handlungsempfehlung in der Gesamtkonzeption Cybercrime/Digitale Spuren beschlossen.

MASSNAHMEN

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.

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

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

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

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

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

ONLINE-ANGEBOTE CYBERCRIME / DIGITALE SPUREN FÜR DIE POLIZEI

ProPK-Medienportal mit umfangreichen Informationen für Polizeibeschäftigte und für die Bevölkerung:
http://www.gsbl.extrapol.de/propkmedienportal/

Deliktsspezifische Informationen des LKA BW, Inspektion 510, für die Polizei Baden-Württemberg:
http://moss.polizei-online.bwl.de/kriminalitaet/delikte/comp/seiten/default.aspx

ANLAGEN

3 ANLAGEN

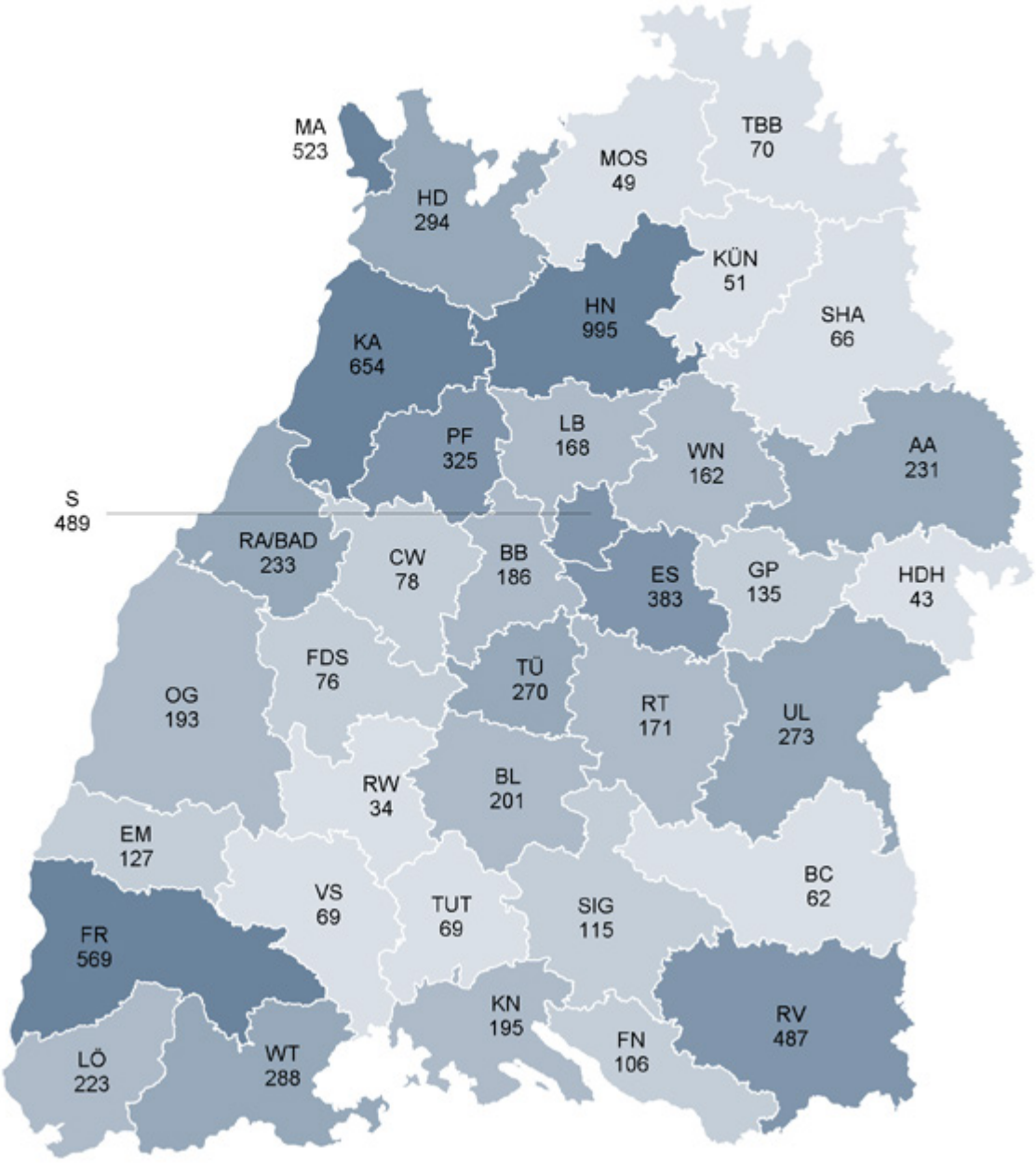
VISUALISIERUNG CYBERCRIME IM ENGEREN SINNE UND CYBERCRIME TATMITTEL

Als Kriterium für die Visualisierung der Fallzahlen in den Baden-Württemberg-Karten wurde die Sachbearbeitung durch die Dienststellen gewählt. Es handelt sich demnach nicht um eine tatortbezogene Betrachtung.

HINWEIS

Die Polizeireform, deren Umsetzung am 1. Januar 2014 erfolgte, ist mit strukturellen Veränderungen verbunden. Der Anlagenteil der diesjährigen Jahresberichte enthält daher zu Beginn eine grafische Gegenüberstellung der jeweiligen Kernzahlen des Berichts in alter und neuer Struktur.

1 | CYBERCRIME IM ENGEREN SINNE – STRUKTUR BIS 2013

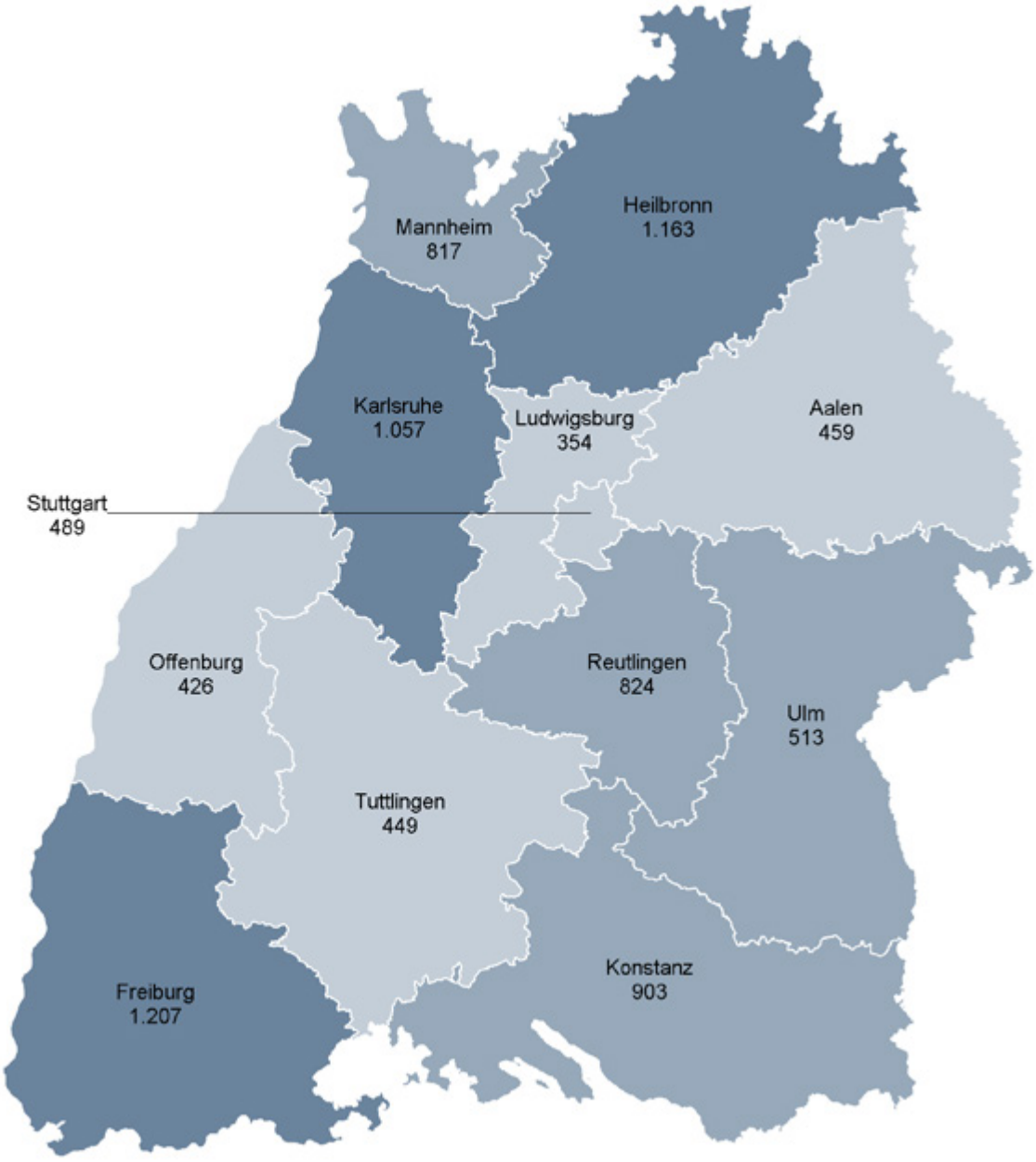


Topografisch nicht darstellbare Dienststellen

LKA BW	LPD S	LPD KA	LPD FR	LPD TÜ	andere Bundesländer
2	0	0	0	0	228

≤ 75
≤ 150
≤ 225
≤ 300
≤ 500
≤ 1.000

2 | **CYBERCRIME IM ENGEREN SINNE – STRUKTUR AB 2014**



Topografisch nicht darstellbare Dienststellen

LKA BW	andere Bundesländer
2	228

≤ 500
≤ 1.000
≤ 1.250

ANLAGEN

DATENGRUNDLAGE DES JAHRESBERICHTS

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

FACHBEGRIFFE UND GLOSSAR

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

DEFINITION CYBERCRIME

Cybercrime umfasst nach bundesweit gültiger Definition alle 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.

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

CYBERCRIME IM ENGEREN SINNE – COMPUTERKRIMINALITÄT

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

Der Summenschlüssel „897000 Computerkriminalität“ umfasst die folgenden Straftatenschlüssel:

- 516300 Betrug mittels rechtswidrig erlangter Debitkarten mit PIN
- 517500 Computerbetrug – soweit nicht unter den Schlüsseln 516300 bzw. 517900 zu erfassen
- 517900 Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten
- 543000 Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung
- 674200 Datenveränderung, Computersabotage

- 678000 Ausspähen, Abfangen von Daten einschließlich Vorbereitungshandlungen
- 715100 Softwarepiraterie (private Anwendung zum Beispiel Computerspiele)
- 715200 Softwarepiraterie in Form gewerbsmäßigen Handelns

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

SONDERMELDEDIENST CYBERCRIME

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

Der Meldedienst umfasst folgende Delikte:

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

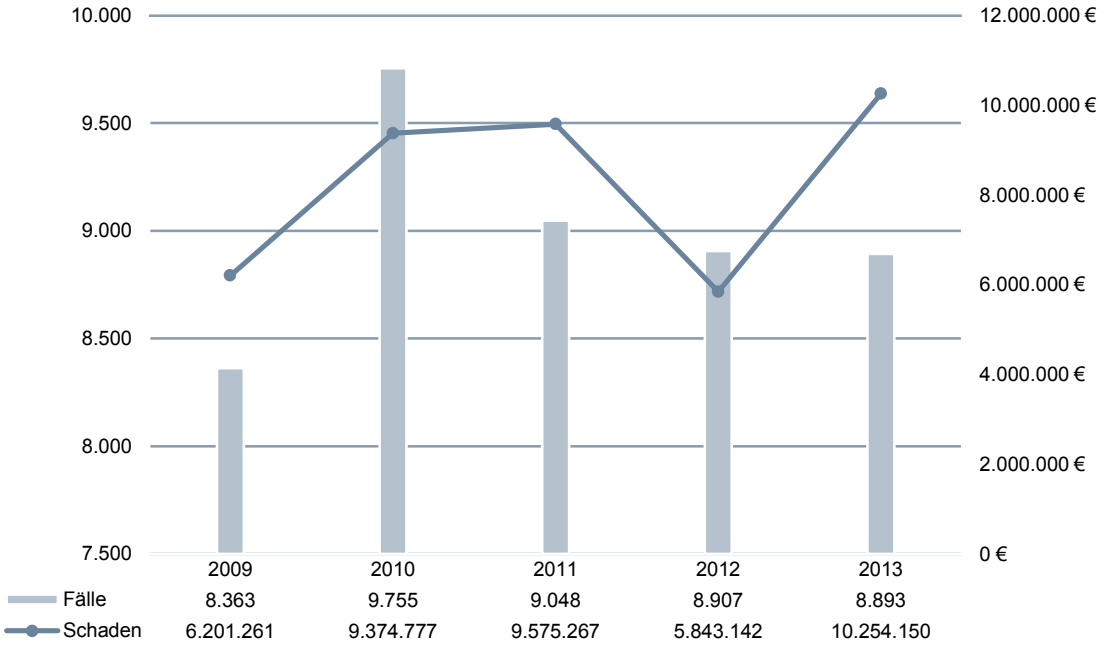
CYBERCRIME TATMITTEL – INTERNETKRIMINALITÄT

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

3 | PKS-BAROMETER CYBERCRIME IM ENGEREN SINNE (2012-2013)

	PKS-Schlüssel	2012	2013	in %	Tendenz
Computerbetrug (§ 263a StGB)	5175	3.658	3.539	-3,3	↘
Fälschung beweiserheblicher Daten (§ 269 StGB)/Täuschung im Rechtsverkehr (§ 270 StGB)	5430	649	692	+6,6	↗
Datenveränderung (§ 303a StGB)/ Computersabotage (§ 303b StGB)	6742	292	392	+34,2	↗
Ausspähen von Daten (§ 202a StGB)	6780	1.346	1.334	-0,9	→
Computerkriminalität	8970	8.907	8.893	-0,2	→

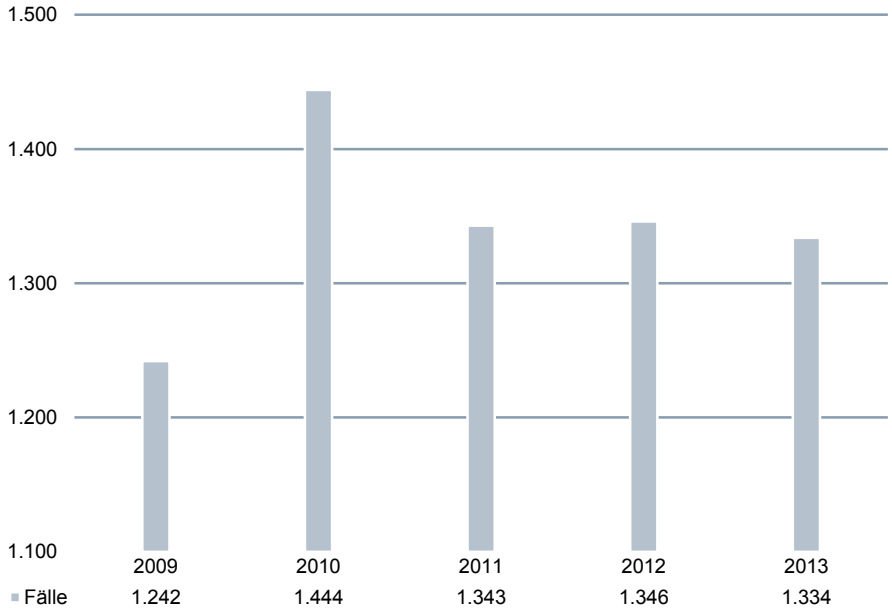
4 | CYBERCRIME IM ENGEREN SINNE FÜNFJAHRESVERGLEICH (2009-2013)



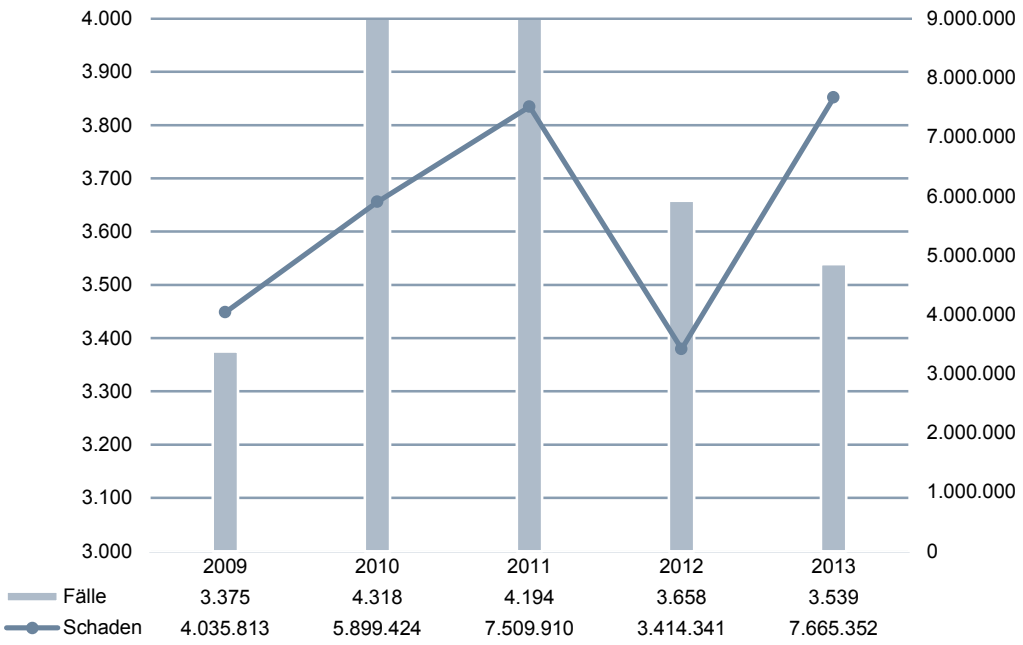
5 | CYBERCRIME IM ENGEREN SINNE (TABELLE) FÜNFJAHRESVERGLEICH (2009-2013)

Berichtsjahr	2009	2010	2011	2012	2013
Computerbetrug	3.375	4.318	4.194	3.658	3.539
Computerbetrug Schadenssumme in €	4.035.813	5.899.424	7.509.910	3.414.341	7.665.352
Fälschung beweiserheblicher Daten/Täuschung im Rechtsverkehr	672	638	618	649	692
Datenveränderung/ Computersabotage	141	194	236	292	392
Ausspähen von Daten	1.242	1.444	1.343	1.346	1.334
Computerkriminalität gesamt	8.363	9.755	9.048	8.907	8.893
Computerkriminalität gesamt Schadenssumme in €	6.201.261	9.374.777	9.575.267	5.843.142	10.254.150

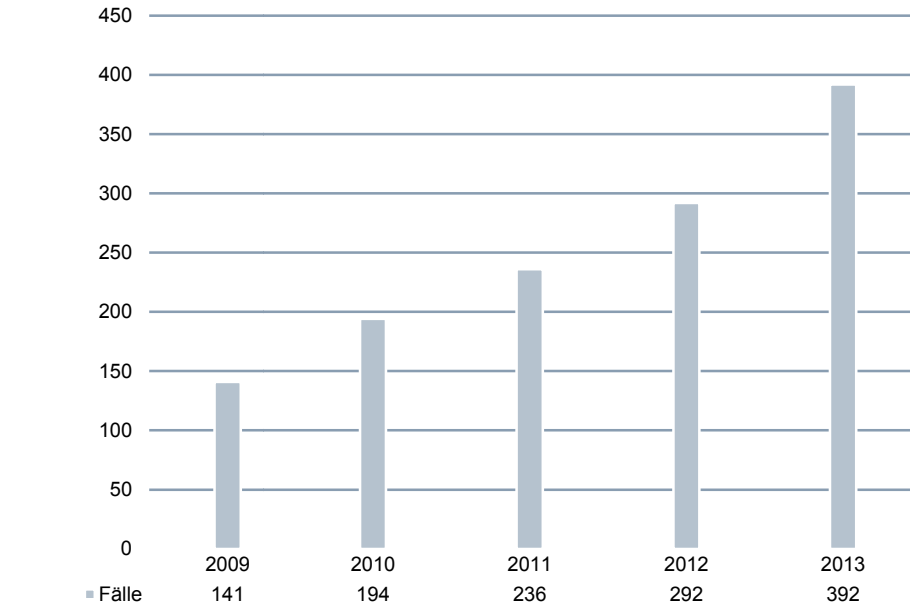
6 | AUSSPÄHEN VON DATEN FÜNFJAHRESVERGLEICH (2009-2013)



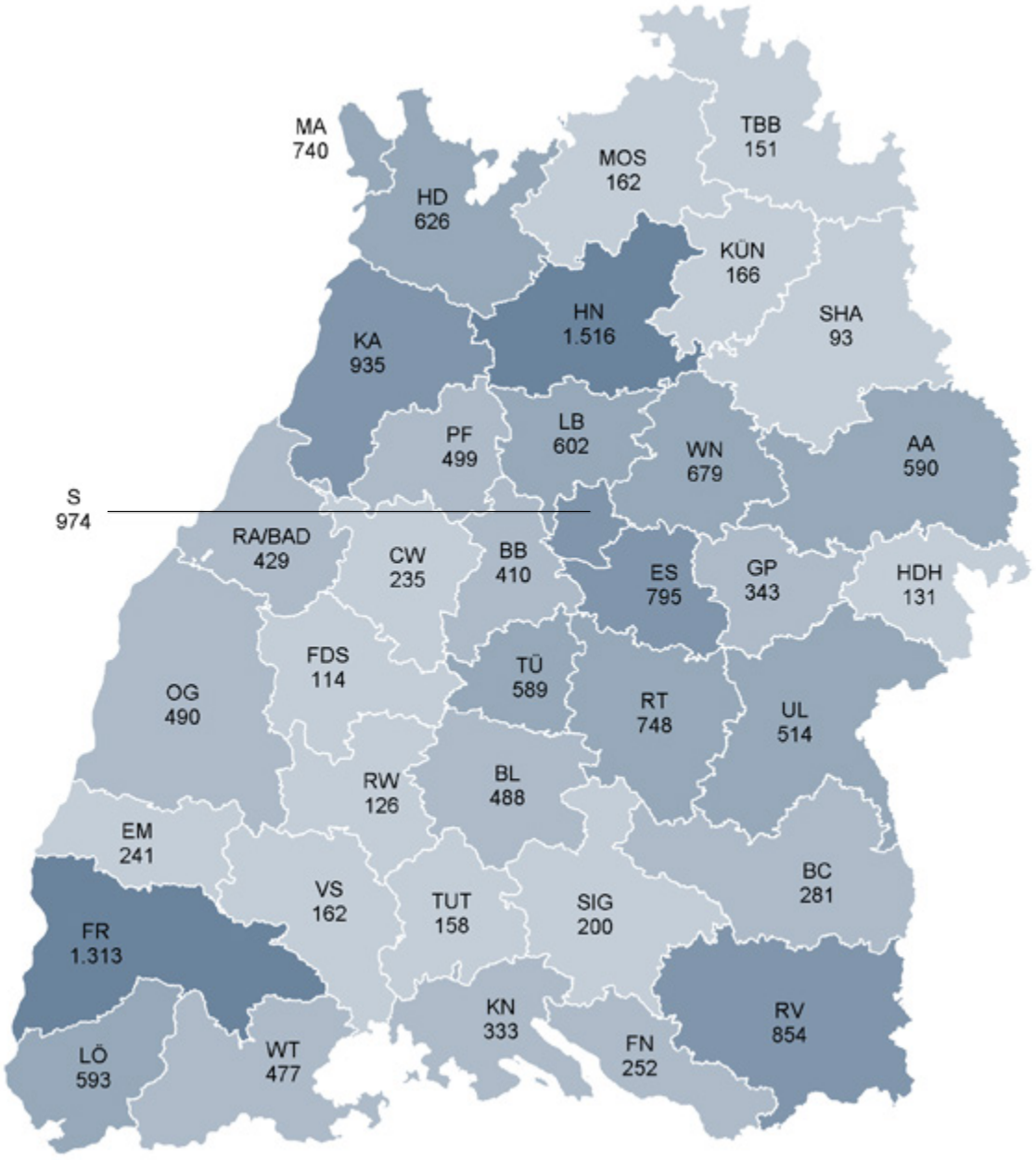
7 | COMPUTERBETRUG FÜNFJAHRESVERGLEICH (2009-2013)



8 | DATENVERÄNDERUNG / COMPUTERSABOTAGE FÜNFJAHRESVERGLEICH (2009-2013)



9 | **CYBERCRIME TATMITTEL – STRUKTUR BIS 2013**

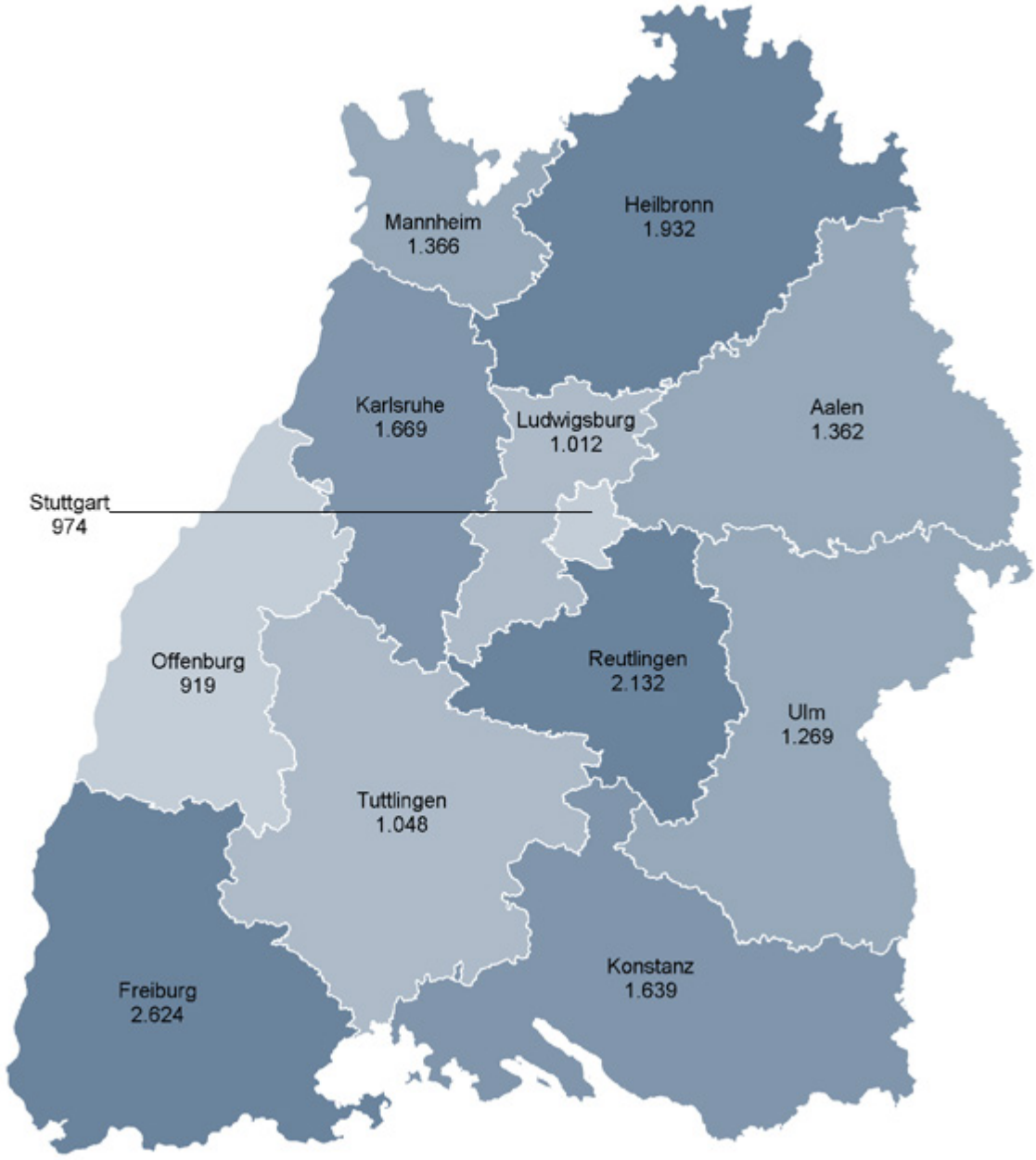


Topografisch nicht darstellbare Dienststellen

LKA BW	LPD S	LPD KA	LPD FR	LPD TÜ	andere Bundesländer
26	2	0	0	0	767

≤ 250
≤ 500
≤ 750

10 | CYBERCRIME TATMITTEL – STRUKTUR AB 2014



Topografisch nicht darstellbare Dienststellen

LKA BW	LPD S	andere Bundesländer
26	2	767

≤ 1.000
≤ 1.250
≤ 1.500
≤ 1.750
≤ 2.700

11 | PKS-BAROMETER CYBERCRIME TATMITTEL (2012 / 2013)

PKS-Hauptschlüssel	2012	2013	+/- absolut	+/- in %	Barometer
Internetkriminalität gesamt	16.912	18.804	+1.892	+11,2	↗
0000 (Straftaten gegen das Leben)**	1	0	-1	-100,0	↘
1000 (Straftaten gegen die sexuelle Selbstbestimmung)**	637	851	+214	+33,6	↗
2000 (Rohheitsdelikte, Straftaten gegen die persönliche Freiheit)**	339	354	+15	+4,4	↗
3***, 4***** (Diebstahl mit und ohne erschw. Umstände)**	4	1	-3	-75,0	↘
5000 (Vermögens- und Fälschungsdelikte)**	12.219	13.593	+1.374	+11,2	↗
6000 (Sonstige Straftatbestände gem. StGB)**	3.021	3.341	+320	+10,6	↗
7000 (Strafrechtliche Nebengesetze)**	691	664	-27	-3,9	↘

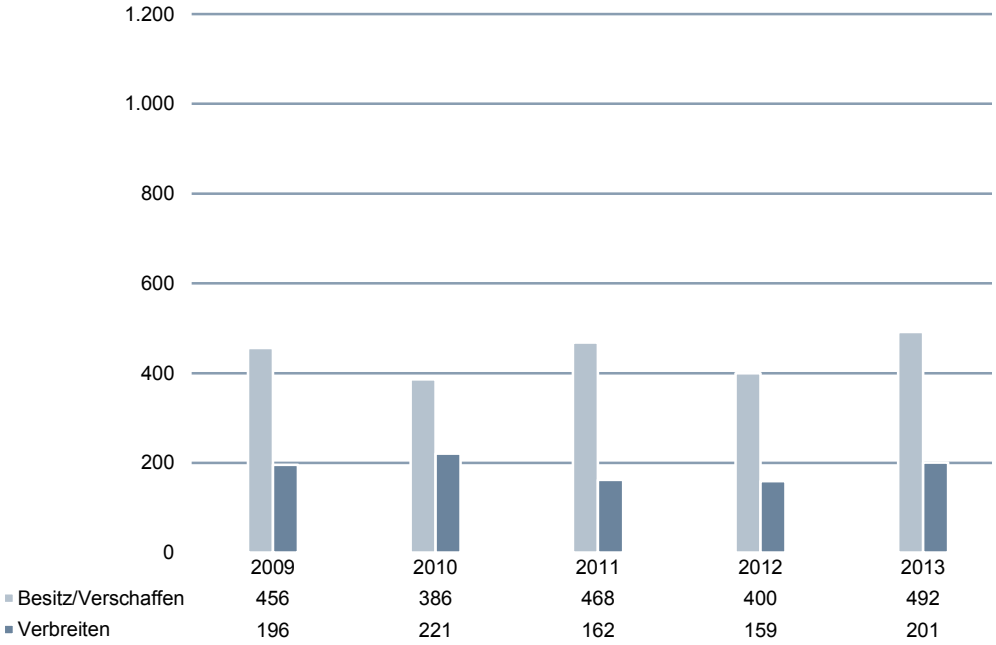
12 | CYBERCRIME TATMITTEL FÜNFJAHRESVERGLEICH (2009 - 2013)

	2009	2010	2011	2012	2013
Erfasste Fälle	21.505	22.494	20.988	16.912	18.804
Erfasste Fälle Differenz	+1.330	+989	-1.506	-4.076	+1.892
Erfasste Fälle Diff. in %	+6,6	+4,6	-6,7	-19,4	+11,2
Versuch	1.113	1.859	1.756	1.578	2.211
Aufgeklärte Fälle	17.115	16.247	14.667	11.028	12.631
Aufgeklärte Fälle Differenz	+817	-868	-1.580	-3.639	+1.603
Aufgeklärte Fälle Diff. in %	+5,0	-5,1	-9,7	-24,8	+14,5
AQ in %	+79,6	+72,2	+69,9	+65,2	+67,2
AQ Differenz in %	-1,2	-7,4	-2,3	-4,7	+2,0
Schaden in €	13.507.038	19.161.021	14.137.128	8.764.879	11.096.543
Schaden Differenz	+2.553.042	+5.653.983	-5.023.893	-5.372.249	+2.331.664

13 | PKS-BAROMETER KINDERPORNOGRAFIE (2012 / 2013)

	PKS-Schlüssel	2012	2013	in %	Tendenz
Besitz/Verschaffen von Kinderpornografie (§ 184b StGB)	1433**	400	492	23,0	↗
Verbreitung von Kinderpornografie (§ 184b StGB)	1434**	159	201	26,4	↗

14 | BESITZ / VERSCHAFFEN UND VERBREITEN VON KINDERPORNOGRAFIE FÜNFJAHRESVERGLEICH (2009-2013)



15 | DATENMENGEN KINDERPORNOGRAFIE AST KIPO FÜNFJAHRESVERGLEICH (2009-2013)

	2009	2010	2011	2012	2013
Anlieferungen	3	7	9	22	35
Bilder	646	5.092	753	25.137	1.346.194
Videos	106	32	77	704	30.041

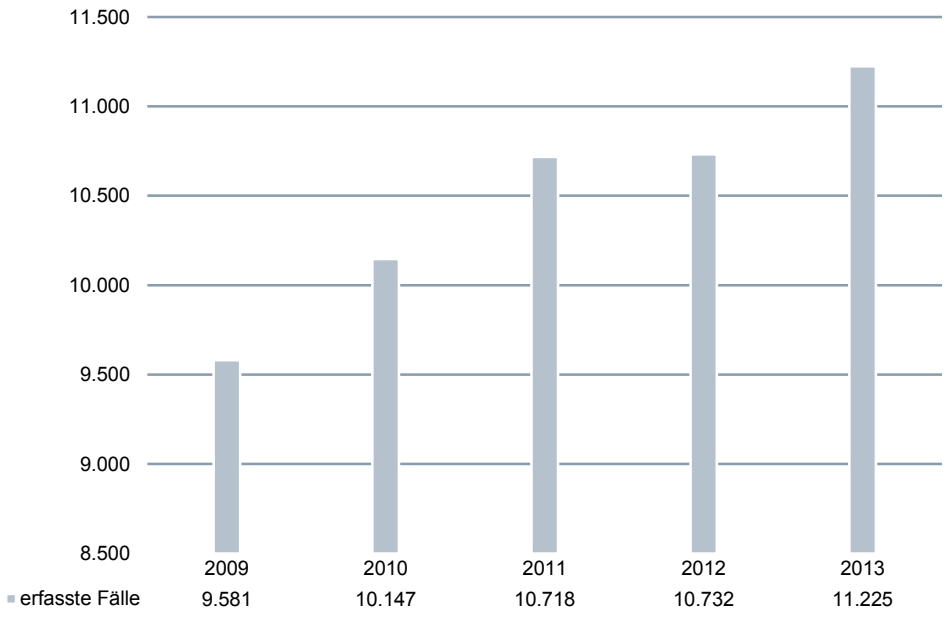
ARBEITSBEREICH INTERNETRECHERCHE (AIR)

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

16 | **STRAFVERFAHRENINITIIERUNGEN AIR FÜNFJAHRESVERGLEICH (2009-2013)**

Berichtsjahr	2009	2010	2011	2012	2013
Deutschland	338	66	420	40	297
davon Baden-Württemberg	30	3	24	4	25
International	2.305	1.045	7.720	636	5.419
Gesamt	**2.643**	**1.111**	**8.164**	**676**	**5.716**

17 | **IT-BEWEISSICHERUNG – ENTWICKLUNG NEUER AUFTRÄGE (LANDESWEITE ÜBERSICHT 2009-2013)**



BEGRIFFSBESTIMMUNGEN

Begriff	*Erläuterung*
Account	*Steht für Benutzerkonto, Zugangsberechtigung. Wird auch in Verbindung mit Diensten benutzt, zum Beispiel E-Mail-Account.*
Advertising, Ad, (Werbe-)Banner	*Werbung im Internet. Üblich sind Werbebanner, eingeblendete Info-Grafiken am Rand der Webseite oder auch als Pop-up-Fenster.*
Antivirenprogramm und Firewall	*Schutzmaßnahmen zur Absicherung des eigenen Rechners. Antivirenprogramme enthalten Virenscanner, spüren bekannte Malware auf und identifizieren unbekannte Malware beispielsweise anhand ihres Verhaltens im System. Antivirenprogramme blockieren und beseitigen Malware. Firewalls sichern Datenverbindungen im Netzwerk ab. Sie können mittels Regeln durch den Anwender justiert werden und helfen, unerwünschten Datenverkehr zu blockieren.*
App, Application	*Software für mobile Endgeräte wie Tablets und Smartphones.*
Bookmark	*Lesezeichen oder auch „Favoriten", die gespeichert werden (zum Beispiel im Browser), um das Wiederaufrufen oder -finden zu erleichtern.*
(Web-)Browser	*Software, mit der Internetseiten und Dokumente aufgerufen werden können.*
Brute Force Attack	*Brute Force steht für rohe Gewalt und bezeichnet eine Methode, bei der Rechenleistung und Wiederholungen eingesetzt werden, um beispielsweise den Zugang zu einer passwortgeschützten Datenbank zu erlangen oder einen Verschlüsselungscode zu knacken.*
Bots, Botnetze/Botnet, Command & Control-Server, Zombie-PC	*Unter einem Bot (vom englischen Begriff robot abgeleitet) versteht man ein Computerprogramm, das weitgehend selbständig sich wiederholende Aufgaben abarbeitet, ohne dabei auf eine Interaktion mit einem menschlichen Benutzer angewiesen zu sein. Der Rechner, auf dem die Bot-Software aktiv ist, wird dadurch Teil eines Netzwerks – eines sogenannten Botnet. Dieses Botnet kann im Weiteren gesteuert werden (durch den sog. Command & Control-Server/CC-Server), um z. B. Spam- oder Phishing-E-Mails zu versenden oder andere Rechner oder Server mittels einer DDoS-Attacke (Distributed Denial of Service) zu stören. Der infizierte Rechner wird häufig auch als Zombie-PC bezeichnet.*
Cache	*Zwischenspeicher in Rechnern, in dem Daten temporär abgelegt werden, die in nächster Zeit voraussichtlich öfters benötigt werden. Der Cache spielt auch beim Betrachten von Internetseiten oder Abspielen von Musik und Videofilmen eine Rolle, denn die Daten werden im Cache zunächst zwischengespeichert.*
Chat	*Chat steht für Unterhaltung, plaudern. Die Kommunikation findet in Echtzeit statt. Meist werden hierzu Chatrooms, also besondere Portale und Seiten im Internet benutzt, in denen sich Leute beispielsweise zu verschiedenen Themen treffen und austauschen. Die Kommunikation findet häufig mit mehreren Personen gleichzeitig statt. Es gibt verschiedene Techniken wie den (älte-*

	ren) Internet Relay Chat (IRC), der Zusatzsoftware benötigt oder den Webchat, der im Browser ablaufen kann. Im Chat (aber auch in Foren) wird üblicherweise eine Netiquette (Network-Etiquette) eingefordert, dies sind Benimmregeln im gegenseitigen Umgang.
Cloud Computing	*Cloud Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle.* *Die Spannbreite, der im Rahmen von Cloud Computing angebotenen Dienstleistungen, umfasst das komplette Spektrum der Informationstechnik und beinhaltet unter anderem Infrastruktur (zum Beispiel Rechenleistung, Speicherplatz), Plattformen und Software (Definition des BSI).*
Cyberwar	*Cyberwar ist aus den Wörtern Cyberspace und War zusammengesetzt und bedeutet zum einen die kriegerische Auseinandersetzung im und um den virtuellen Raum mit Mitteln vorwiegend aus dem Bereich der Informationstechnik. Zum anderen sind damit die hochtechnisierten Formen des Krieges im Informationszeitalter gemeint, die auf einer weitgehenden Computerisierung, Elektronisierung und Vernetzung fast aller militärischer Bereiche und Belange basieren. Übliche Zielrichtungen des Cyberwars sind Spionage, Sabotage und Manipulation.*
Datenarten (Bestandsdaten, Verkehrsdaten und Inhaltsdaten)	***Bestandsdaten*** *Daten eines Teilnehmers, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden (§ 3 Nr. 3 TKG). Daten, die Anwender bei Vertragsabschluss oder -änderung beim Provider hinterlegen (zum Beispiel Adresse, Kontoverbindungen, Kopien, Personalausweisdaten etc.). Welche Auskünfte der Provider geben muss, ist in § 11 TKG geregelt.* ***Inhaltsdaten*** *Alle tatsächlich übertragenen Daten, die nicht lediglich reine Verbindungs- und Steuerungsfunktion haben, zum Beispiel der Inhalt von Telefongesprächen.* ***Verkehrsdaten*** *Daten nach § 3 Nr. 30 TKG, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden (zum Beispiel Telefonnummern und Verbindungszeiten, Standortdaten von Mobiltelefonen, IP-Adressen und Zeitraum der Zuweisung zu einem Anschluss bei der Nutzung von Rechnern). Welche Verkehrsdaten durch den Verpflichteten gespeichert werden dürfen, ergibt sich aus § 96 TKG.*
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 Cybercrime kann in vielerlei Ausprägungen stattfinden. Strafrechtlich relevant ist vor allem das „Ausspähen von Daten" (§ 202a StGB).*
Domain, Top-Level-Domain	*Eine Domain ist eine weltweit gültige und eindeutige Kennung, die bestimmten Regeln unterliegt. Ein Beispiel ist www.polizei-bw.de. Die sogenannte Top-Level-Domain oder auch Länderkürzel genannt, kennzeichnet in der Regel das Land (DE steht zum Beispiel für Deutschland), wobei es auch Top-Level-Domains gibt, die thematisch sind wie .com für commercial.*
Domain Name Service (DNS)	*Der DNS-Server wandelt die eindeutige IP-Adresse (numerisch) in den gewählten Domainnamen (zum Beispiel polizei-bw.de) um (auch Namensauflösung). Es handelt sich um einen zentralen Dienst im Internetverkehr. Deswegen ist er auch potentielles Ziel für Angriffe und Manipulationen.*
DoS- und DDoS-Attacken	*Als Denial of Service (kurz DoS, englisch für: Dienstverweigerung) wird in der digitalen Datenverarbeitung die Nichtverfügbarkeit eines Dienstes bezeichnet, der eigentlich verfügbar sein sollte. Obwohl es verschiedene Gründe für die Nichtverfügbarkeit geben kann, spricht man von DoS in der Regel als die Folge einer Überlastung von Infrastruktursystemen. Dies kann durch unbeabsichtigte Überlastungen verursacht werden oder durch einen mutwilligen Angriff auf einen Server, einen Rechner oder sonstige Komponenten in einem Datennetz. Wird die Überlastung von einer größeren Anzahl anderer Systeme verursacht, so wird auch von einer verteilten Dienstblockade oder englisch Distributed Denial of Service (DDoS) gesprochen.*
Download, Upload	*Download bedeutet das Herunterladen einer Datei auf den lokalen Rechner. Im Gegenteil dazu bezeichnet der Upload das Hochladen von Daten, zum Beispiel in eine über das Internet zugängliche Datenbank oder Anwendung.*
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 werden (drive-by bedeutet im Vorbeifahren).*
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. Besonders gefährlich sind Zero-Day-Exploits, die über Jahre hinweg nicht bemerkt werden.*
Filehoster	*Als Filehoster werden Internetdienstanbieter bezeichnet, bei denen der Anwender Dateien unmittelbar mit oder ohne vorherige Anmeldeprozedur speichern oder herunterladen kann.*

Flatrate	*Leistungen wie bspw. Internetzugang oder Telefonie zu einem Pauschalpreis, der nicht von Häufigkeit oder Datenverbrauch abhängt.*
(Internet-)Forum/ Message Board	*Internetforen bieten die Möglichkeiten, Fragen und Antworten sowie Gedanken und Anregungen auszutauschen. Die Kommunikation läuft hier asynchron, das heißt zeitversetzt und unterscheidet sich damit von Chats. Bereits kommentierte, das heißt fortgeschriebene, beantwortete Einträge werden Threads (englisch: Faden, Strang) genannt.*
FTP	*FTP bedeutet File Transfer Protocol (Datenübertragungsverfahren) und ist ein Netzwerkprotokoll zur Übertragung von Dateien über IP-Netzwerke.*
Hacker	*Sammelbegriff für IT-Spezialisten, im Regelfall negativ belegt. Zur weiteren Unterscheidung gibt es die Bezeichnungen „White-Hat", „Grey-Hat" oder „Black-Hat", welche die jeweilige Motivation und Loyalität zu Gesetzen und strafbaren Handlungen aufzeigt. „Black Hats" begehen Straftaten, um ihre meist kriminellen Ziele zu erreichen, sie stehen demnach auch im Fokus der Ermittlungsbehörden.*
Hacktivismus	*Das Wort besteht aus den Bestandteilen Hack und Aktivismus. Hacktivisten setzen Rechner und Netzwerke als Protestmittel ein, um politische Ziele zu erreichen. Übliche Formen sind DDoS-Angriffe, um Webseiten lahmzulegen, Defacement (Verändern/Verunstalten von Webseiten, nach erfolgreichem Hacking), Spamming (z. B. durch das massenhafte Verschicken von sinnlosen oder sehr großen E-Mails). Regelmäßig übersteigen die Handlungen reine Protestformen und erfüllen Straftatbestände.*
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.*
Hoax	*Moderner Kettenbrief, Scherz-Mail oder Falschmeldung, häufig auch mit vermeintlich ernsthaftem Hintergrund wie einem Hilferuf, angeblichem Warnhinweis der Polizei oder einer Unterstützungsanfrage sowie der Verbreitung von sog. urbanen Legenden. Die Verbreitung ähnelt der Verbreitung von Malware, geschieht allerdings aktiv durch die Nutzer selbst. Auf der Seite der TU Berlin kann man prüfen, ob eine Meldung ein bekannter Hoax ist: http://hoax-info.tubit.tu-berlin.de/hoax/*
HTML	*HTML steht für Hypertext Markup Language. Mittels HTML können Dokumente und Webseiten aufgebaut werden. Mittels Webbrowser können diese Seiten dargestellt werden.*
HTTP	*HTTP bedeutet Hypertext Transfer Protocol. Es handelt sich um ein Hypertext-Übertragungsprotokoll und stellt ein nachrichtenorientiertes Kommunikationsprotokoll für Netzwerke dar. HTTP wird zur Übertragung von HTML-Webseiten und Daten in Netzwerken verwendet.*

Hyperlink, Link	*Sprungmarken, die zu einer bestimmten Textstelle, Datei oder im Internet zu einer Seite führen.*
IMEI	*IMEI steht für International Mobile Station Equipment Identity und ist die 15-stellige individuelle Seriennummer eines Mobiltelefons.*
IMSI	*IMSI steht für International Mobile Subscriber Identity. Mittels der IMSI können Geräte in GSM- und UMTS-Mobilfunknetzen eindeutig identifiziert werden. Die IMSI wird auf der SIM-Karte (Subscriber Identity Module) gespeichert. Sie werden durch die Mobilfunknetzbetreiber jeweils nur einmalig vergeben.*
Internet Protocol Versionen – IPv4 und IPv6	*Der Standard IPv4 benutzt 32-Bit-Adressen, wodurch, „nur" etwa 4,3 Milliarden eindeutige Adressen möglich sind. Dieser Bedarf ist zwischenzeitlich überschritten, die letzten freien Adressen wurden vergeben. Der neue Standard IPv6 besteht hingegen aus 128-Bit-Adressen. Dadurch gibt es zukünftig etwa 340 Sextillionen (eine Sextillion hat 36 Nullen) eindeutige Adressen.* *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.*
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 (zum Beispiel für den Datentransport). Meist werden Geräte automatisch konfiguriert und erhalten eine sogenannte dynamische IP-Adresse. Dynamisch bedeutet dabei, dass sie nicht dauerhaft durch das gleiche Gerät genutzt. Das Gegenteil sind statische IP-Adressen, die beispielsweise für Server oder Netzwerkdrucker üblich sind. Der aktuelle Standard zur Adressierung ist IPv4.*
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 ärztliche 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.*

Keylogger	*Die Aufgabe eines Keyloggers ist die im Regelfall heimliche Protokollierung sämtlicher Eingaben des Benutzers am Rechner. Die Software kann eingesetzt werden, um Passwörter auszuspionieren.*
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 Diensten, verschlüsselte Daten, die während der Laufzeit entschlüsselt sind oder bestehende Verbindungen des Systems innerhalb eines Netzwerks.*
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 for Mobile Communications)*** *GSM ist ein Standard für Mobilfunknetze. Er wird hauptsächlich für Telefonie genutzt. Zudem ermöglicht er die Übertragung von Kurzmitteilungen.* ***UMTS (Universal Mobile Telecommunications 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.*
NAPT-Technik	*Mit der Verwendung der Network-Adress-Port-Translation-Technik (NAPT) wird einer IP-Adresse eine Vielzahl von Nutzern zugeordnet. Damit soll erreicht werden, dass nicht zu viele IP-Adressen verbraucht werden.*
Netzjargon	*Im Internet hat sich in Chats, Messengerdiensten, Foren aber auch in versandten Nachrichten wie SMS und E-Mail sowie Computerspielen eine eigene Sprache entwickelt, die aus Abkürzungen und Akronymen besteht. Einige davon sind bekannter wie „lol" für „laughing out loud", lautes Lachen oder „cu" für „see you" für bis bald oder Tschüss, andere weniger wie „afk" – „away from keyboard" für bin kurz weg.*
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.*
Nickname	*Pseudonym oder Fantasiename, der einmal oder mehrfach bei Spielen, in Foren oder Chats oder auch bei der Anmeldung zu Diensten benutzt wird. Das Gegenteil zum Begriff Nickname ist der Realname, also der echte Namen der Person.*
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")*
Patch, Update	*Ein Patch (englisch Flicken) behebt einen festgestellten Fehler. Alle eingesetzten Programme sollten regelmäßig „gepatcht" werden, damit zumindest bekannte Fehler im Programm korrigiert werden. Ein Update ist im Wesentlichen dasselbe, kann jedoch auch Optimierungen am Programm vornehmen (zum Beispiel Verbesserung der Ausführungsgeschwindigkeit).*

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 E-Mails, wie Rechnungen, Sicherheitshinweise oder Benutzerinformationen, die es verleiten sollen, dem Täter vertrauliche Informationen, vor allem Benutzernamen und Passwörter oder PIN und TAN von Online-Banking-Zugängen, preiszugeben. Mit den gestohlenen Zugangsdaten kann der Phisher die Identität seines Opfers übernehmen und in dessen Namen Handlungen ausführen. Im Internet werden so gestohlene Daten in ganzen Paketen zum Kauf angeboten.*
Plug-In, Add-On	*Zusatzprogramme oder Softwaremodule, die in ein Programm eingebunden werden können, um z. B. bestimmte Zusatzfunktionalitäten zu erreichen (beispielsweise um Dateiformate zu öffnen, die nicht im Standardprogramm enthalten sind). Browser lassen sich mit Plug-Ins und Add-Ons häufig mit hilfreichen Zusatzfunktionen ausstatten.*
Pop-up-Fenster	*Pop up bedeutet im Englischen etwa plötzlich auftauchen und bezieht sich insbesondere auf Fenster, die gewünscht (zum Beispiel Kontextmenü, das mittels rechter Maustaste in vielen Programmen aufgerufen werden kann) oder unerwünscht (zum Beispiel Werbung im Internet beim Aufrufen einer Webseite) erscheinen. Viele Browser bieten inzwischen Pop-up-Blocker an, die diesen Vorgang beim Internetsurfen verhindern.*
Posting (auch abgekürzt Post)	*Das erstellen von Beiträgen, Kommentaren oder Anmerkungen in Foren, Newsgroups oder Anwendungen. Das Verb wird als „posten" bezeichnet.*

Provider	*Provider bedeutet Anbieter und wird meist nur verkürzt benutzt. Übliche Langbegriffe sind Mobilfunkprovider, Telekommunikationsdienstprovider oder Internet-Service-Provider. Provider (auch Access-Provider genannt) bieten beispielsweise einen Zugang zum Internet gegen eine monatliche Gebühr an.*
Proxy	*Ein Proxyprogramm ist eine Kommunikationsschnittstelle in einem Netzwerk und steht als Mittelsmann zwischen anfragendem Rechner und Zielrechner. Proxys können zu verschiedenen Zwecken eingesetzt werden, zum Beispiel zur Anonymisierung oder zur Filterung.*
Ransomware, Digitale Erpressung	*Als Ransomware werden Schadprogramme bezeichnet, mit deren Hilfe ein Eindringling eine Zugriffs- oder Nutzungsverhinderung der Daten sowie des gesamten Computersystems erwirkt. Dabei werden private Daten auf einem fremden Computer verschlüsselt oder der Zugriff auf diese wird verhindert, um für die Entschlüsselung oder Freigabe ein Lösegeld zu fordern. Es handelt sich folglich um eine digitale Form einer Erpressung. Die Bezeichnung „Ransomware" setzt sich aus der Zugehörigkeit zur Klasse der Malware sowie der englischen Bezeichnung für Lösegeld (= „ransom") zusammen.*
Scareware	*Bei Scareware, alternativ auch „Fake-AV" (AV steht für Antivirus) genannt, handelt es sich um Software, die darauf ausgelegt ist, Computernutzer zu verunsichern (scare bedeutet Schrecken). Dies erfolgt durch ein kostenlos zur Verfügung gestelltes angebliches Antivirenprogramm oder aber durch Anzeigen bzw. Animationen über Webseiten im Internet. Der Schaden für den Nutzer kann darin bestehen, dass er aus Angst ein nutzloses Programm erwirbt oder dass er erst durch das Aufspielen der Software Schadsoftware auf seinen Rechner bringt.*
Schadprogramme, Malware	*Sammelbegriff für Computerprogramme, die unerwünschte, schädliche oder zerstörende Funktionen haben. Der Begriff Malware ist dabei eine Wortschöpfung aus den englischen Begriffen malicious (boshaft) und Software. Der Sammelbegriff umfasst insbesondere Viren, Würmer, Trojanische Pferde, Scareware, Spyware und Ransomware.*
Smartphones	*Smartphones sind Mobiltelefone, die den Fokus auf die Nutzung des Internets und dessen Dienste legen, während klassische Mobiltelefone den Schwerpunkt auf Telefonie und Dienste zur einfachen Nachrichtenübermittlung (zum Beispiel SMS) legen.*
Social Engineering	*Methode, um mit zwischenmenschlichen Kontakten (unmittelbar oder mittelbar) bestimmte Verhaltensweisen auszulösen, zum Beispiel Herausgabe von vertraulichen Informationen oder Passwörtern. Erfolgreiches Social Engineering basiert häufig auf falschem Vertrauen und greift im Bereich Cybercrime nicht die technische Komponente, sondern die menschliche Komponente an. Beispiele sind der gefälschte Anruf eines Technikers aus der Firma, der den Passwortzugang zur Wartung benötigt, oder die Nutzung einer gefälschten E-Mail-Adresse oder falscher Identitäten (zum Beispiel in sozialen Netzwerken).*

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

Thumbnail	*Englischer Begriff für Daumennagel, bezieht sich auf die Größe und ist eine kleine Grafik, die ein Vorschaubild darstellt. Damit lassen sich beispielsweise Bildergalerien übersichtlich darstellen.*
TOR	*TOR (The Onion Routing) ist ein Netzwerk zur Anonymisierung von Verbindungsdaten, das seine Nutzer vor der Analyse des Datenverkehrs schützt. Die dabei angewendete Technik ist die kaskadierte Verschlüsselung. Als Kaskadierung wird das Hintereinanderschalten mehrerer Systeme bezeichnet (deswegen auch der Bezug zu einer Zwiebel, englisch onion).*
Trojanische Pferde (kurz Trojaner)	*Ein Trojanisches Pferd besteht aus zwei Bestandteilen, einem in der Regel nützlichen Programmteil, das einen Zweck erfüllt, den der Nutzer erzielen möchte und einem versteckten Programmteil, der im Hintergrund arbeitet und unerwünschte Software aufspielt oder Veränderungen am Computersystem vornimmt. Häufig wird Spyware oder eine sogenannte Backdoor (eine „Hintertür", durch die der Täter später ungesehen in das System eindringen kann) aufgespielt, mit deren Hilfe der Täter Daten erlangt oder Veränderungen vornehmen kann.*
Troll, Trollen	*Trolle sind eine Erscheinung des Internets, die im Regelfall ohne einen Mehrwert zu erzeugen in Kommunikationsvorgängen (Chats, Foren, Newsgroups, Kommentierungen et cetera) sinnlose, destruktive, provozierende, störende oder anders nutzlose Beiträge verfassen. Die „Tätigkeit" wird trollen genannt. Trollen widerspricht im Regelfall der gültigen Netiquette. Es ist zudem nicht angebracht, Trolle zu „füttern" („Do not feed the troll" DNFTT), das bedeutet auf deren Beiträge einzugehen.*
URL	*URL steht für Uniform Resource Locator und bedeutet einheitlicher Quellenanzeiger. Mit URL werden Adressen beschrieben, die eine bestimmte Ressource in einem Netzwerk lokalisieren. Dazu werden das verwendete Netzwerkprotokoll (z. B. HTTP, FTP et cetera) und der Ort der Ressource angegeben.*
(Computer)Virus	*Computerviren sind die älteste Art der Malware. Sie verbreiten sich, indem sie Kopien von sich selbst in Programme, Dokumente, Datenträger oder den Bootbereich schreiben. Dabei finden Manipulationen statt, die der Benutzer nicht kontrollieren kann. Die Folgen reichen dabei von einfachen Manipulationen bis hin zum kompletten Systemabsturz. 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.*
Voice over IP (VoIP)	*Bezeichnet Internettelefonie also das Telefonieren über das Internet oder andere Computernetzwerke.*

Ware, Warez	*Ware (englisch) bezeichnet einen Überbegriff und wird meist mit Präfix wie Malware (s. o.), Freeware (im Regelfall kostenfrei nutzbare Software) oder Shareware (Testversionen mit Beschränkungen) benutzt. Warez umfasst hingegen illegal beschaffte oder verbreitete Software. Die Endung „z" wird zudem auch für andere Bereiche wie Gamez (Spiele), Moviez (Filme) oder Appz (Anwendungen) verwendet. Seiten mit entsprechenden Angeboten bieten in der Regel illegale Waren an, zudem sind die Seiten bzw. die Daten oft mit Malware verseucht.*
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 (zum Beispiel 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 (sog. user generated content) 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-Netzwerken aber auch Wechselmedien. Zielrichtung eines Wurms ist dabei die schnelle (weltweite) Verbreitung.*

ANSPRECHPARTNER

ANSPRECHPARTNER

ÖFFENTLICHKEITSARBEIT

Telefon 0711 5401-2012 und -3012

Fax 0711 5401-1012

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

IMPRESSUM

CYBERCRIME / DIGITALE SPUREN

JAHRESBERICHT 2013

HERAUSGEBER

Landeskriminalamt Baden-Württemberg
Taubenheimstraße 85
70372 Stuttgart

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

GESTALTUNG

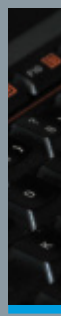
Liane Köhnlein, LKA BW

DRUCK

e. kurz + co, Stuttgart

BILDQUELLEN

LKA BW, fotolia.com



2013