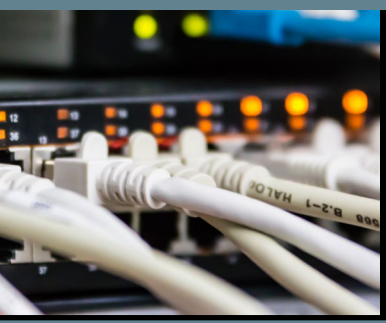
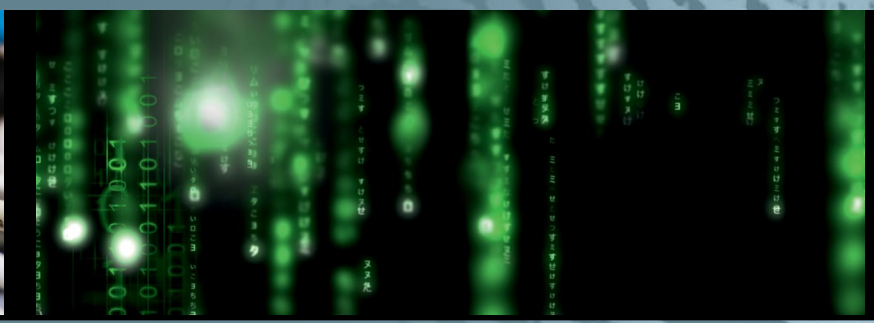
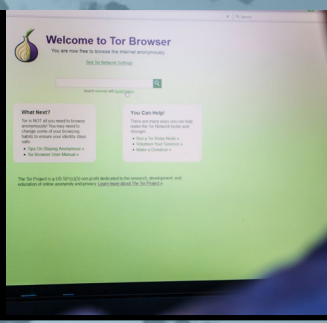




LKA BW

Cybercrime und Digitale Spuren

JAHRESBERICHT 2016

Baden-Württemberg

LANDESKRIMINALAMT

AUF EINEN BLICK

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

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

BIG DATA BEI DER POLIZEI. DIE SICHERGESTELLTEN DATENMENGEN STEIGEN WEITER AN.

	2015	2016	IN %	
GESAMT	**22.133**	**21.744**	**-1,8 %**	↘
COMPUTERKRIMINALITÄT	6.547	7.113	8,6 %	↗
INTERNETKRIMINALITÄT	18.676	18.005	-3,6 %	↘
GESAMTBEREICH KINDERPORNOGRAFIE KINDERPORNOGRAFISCHE SCHRIFTEN	599	703	17,4 %	↗
VERFAHRENSINITIIERUNGEN AIR	921	664	-27,9 %	↘
NEUE AUFTRÄGE ITB	10.071	10.683	6,1 %	↗

INHALT

1 ANALYSE

KRIMINALITÄT IM NEUEN ZEITALTER

Ein 19-jähriger Drogenhändler wurde im November 2016 in Wien festgenommen. Unter dem Pseudonym Hedon war der Student als Powerseller im Darknet aktiv und verkaufte große Mengen an Rauschgift und suchtmittelhaltige Medikamente bis er ins Visier der Ermittler des LKA geriet. Er soll knapp 1.800 Verkäufe im Darknet getätigt haben. Die Drogen verschickte er per Post, bezahlt wurde mittels Bitcoin – einer digitalen Währung.

Die Polizei ist immer öfter mit Tätern und Tätergruppierungen konfrontiert, die mit neuen Ideen und hochtechnischer Ausrüstung ihr Unwesen im Internet treiben. Es ist eine zentrale Aufgabe der Ermittlungsbehörden, dieser Entwicklung entgegenzutreten und die Kriminellen zu ermitteln, sodass sich der Bürger auch in der virtuellen Welt sicher fühlen kann. Die Reaktion auf die Entwicklung Kriminalität 2.0 muss Kriminalistik 2.0 und Kriminaltechnik 2.0 lauten. Dafür steht die Abteilung Cybercrime und Digitale Spuren des LKA.

Allerdings werden die Ermittlungen gegen Cyberkriminelle zusätzlich erschwert, da diese zunehmend aus dem Darknet – der dunklen Seite des Internets – heraus agieren. In diesem Bereich des Internets können die Täter mittels spezieller Tools und Verschlüsselungstechnologien ein Höchstmaß an Anonymisierung ihres Datenverkehrs erreichen.

Dies führte dazu, dass sich in den letzten Jahren eine Parallelwelt im Internet mit sogenannten Kryptomärkten – hierbei handelt es sich um Marktplätze, auf denen insbesondere illegaler Handel mit Waffen, Kinderpornographie und Betäubungsmitteln betrieben wird – entwickelt hat. Spätestens seit dem Amoklauf in München im Juli 2016 ist das Darknet einer größeren Öffentlichkeit bekannt, da sich der Täter im Schatten-Netzwerk seine Waffe und die passende Munition besorgt hatte.

Einen Einblick in das Darknet und in die polizeilichen Ermittlungsmaßnahmen zur Aufdeckung von Käufern und Händlern illegaler Waren erhielten der Bundesinnenminister, Dr. Thomas de Maiziere, sowie der Innenminister des Landes Baden-Württemberg, Thomas Strobl, bei ihrem Besuch am 18. August 2016 im Landeskriminalamt Baden-Württemberg. „Die besondere Brisanz des Darknets liegt darin, dass der Zugang zum illegalen Markt für jedermann einfach möglich ist. Uns ist es wichtig, im Darknet präsent zu sein. Es muss klar sein, dass man hier nicht unbeobachtet tätig sein kann. Unser Anspruch ist, die scheinbare Anonymität der Kriminellen zu lüften“, so Ralf Michelfelder, Präsident des LKA im Interview mit der Heilbronner Stimme.

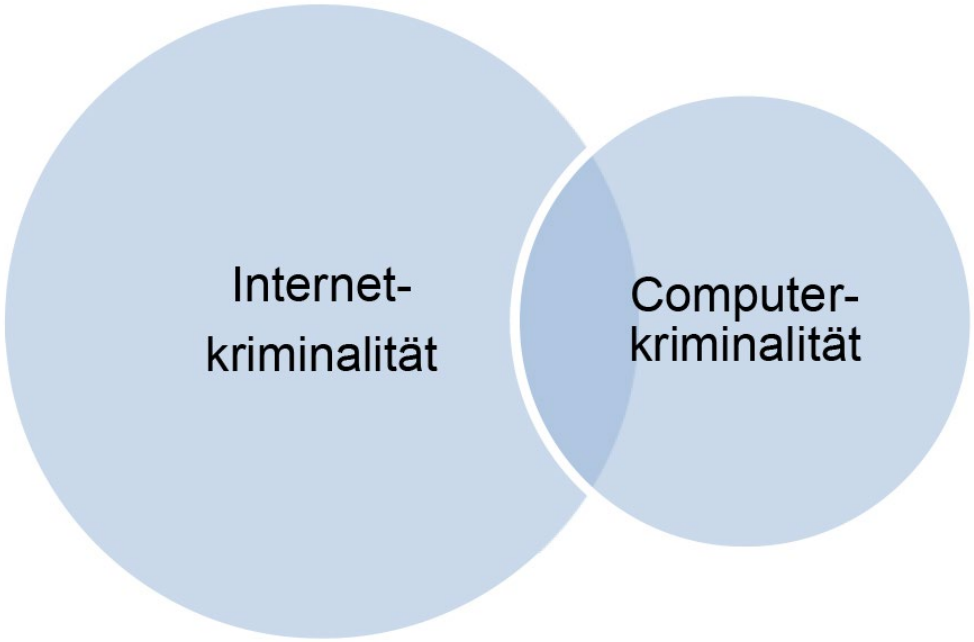
Reinhard Tencz, Leiter der Abteilung Cybercrime und Digitale Spuren.

Bei allen kriminellen Aktivitäten in der virtuellen Welt gibt es eine Schnittstelle in die reale Welt. Dies ist der Schlüssel zum Ermittlungserfolg des LKA. Vor dem Hintergrund, dass sich die Täter im Netz modernster und hochkomplexer Technologien bedienen ist es unabdingbar, dass die Polizei ihr Personal stetig weiterbildet und ebenfalls neuartige Technologien im Rahmen der digitalen Verbrechensbekämpfung einsetzt.

Die Polizei Baden-Württemberg hat bereits vor einigen Jahren die Sonderlaufbahn Cyberkriminalist eingeführt. Die besonders qualifizierten IT-Spezialisten verrichten ihren Dienst in der Abteilung Cybercrime und Digitale Spuren beim LKA sowie bei den entsprechenden Kriminalinspektionen der zwölf regionalen Polizeipräsidien.

Da die meisten Cybercrime-Delikte lokal nicht eingrenzbar sind, ist es erforderlich, dass die Behörden auf Bundes- und Landesebene aber auch im internationalen Kontext enger zusammenarbeiten.

Baden-Württemberg zählt zu den sichersten Bundesländern Deutschlands. In einer globalen Welt wird sich die Polizei jedoch angesichts zunehmender Bedrohungen – insbesondere durch Cyberangriffe, Terrorismus und Extremismus – besonderen Herausforderungen stellen müssen, um das hohe Sicherheitsniveau aufrecht zu erhalten.



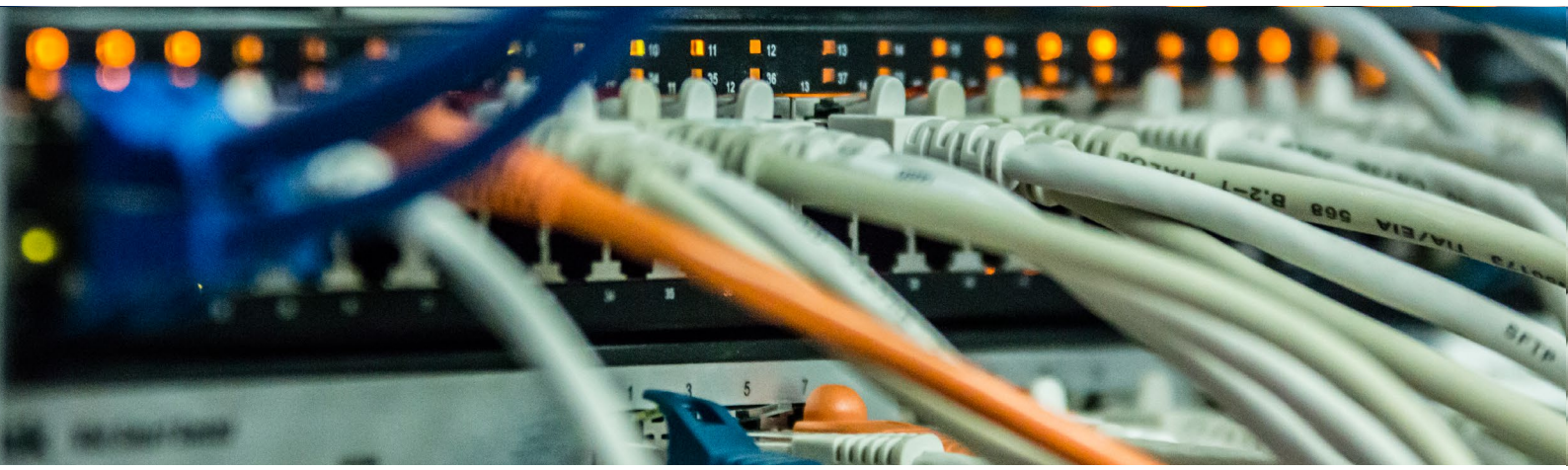
DARSTELLUNG UND BEWERTUNG DER KRIMINALITÄTSLAGE

In der Polizeilichen Kriminalstatistik (PKS) werden die Begriffe Internetkriminalität und Computerkriminalität verwendet. Diese werden im Folgenden näher erläutert. Es gilt zu beachten, dass die in der PKS erfassten Fallzahlen nicht dem tatsächlich zu bearbeitenden Fallaufkommen im Bereich Cybercrime entsprechen. Eine Begründung hierfür ergibt sich aus den Erfassungsrichtlinien, die keine Erfassung von Straftaten mit Handlungsort im Ausland oder weltweit ungeklärtem Handlungsort vorsehen. Diese Umstände sind bei Cyber-Ermittlungen regelmäßig gegeben, so dass diese Fälle abschließend keinen Eingang in die PKS finden. Betrachtet man die Entwicklung der Auslandsstraftaten oder die Fälle, deren Tatort nicht auf Deutschland eingegrenzt werden kann, in der Eingangsstatistik POLAS BW, so sieht man seit dem Jahr 2007 kontinuierlich Anstiege. Entsprechende Anpassungen werden aktuell umgesetzt, so dass diese Fälle ab dem Jahr 2018 ausgewiesen werden können.

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

- das Internet
- weitere Datennetze
- informationstechnische Systeme oder
- deren Daten richten.

Cybercrime umfasst aber auch solche Straftaten, die mittels dieser Informationstechnik begangen werden.



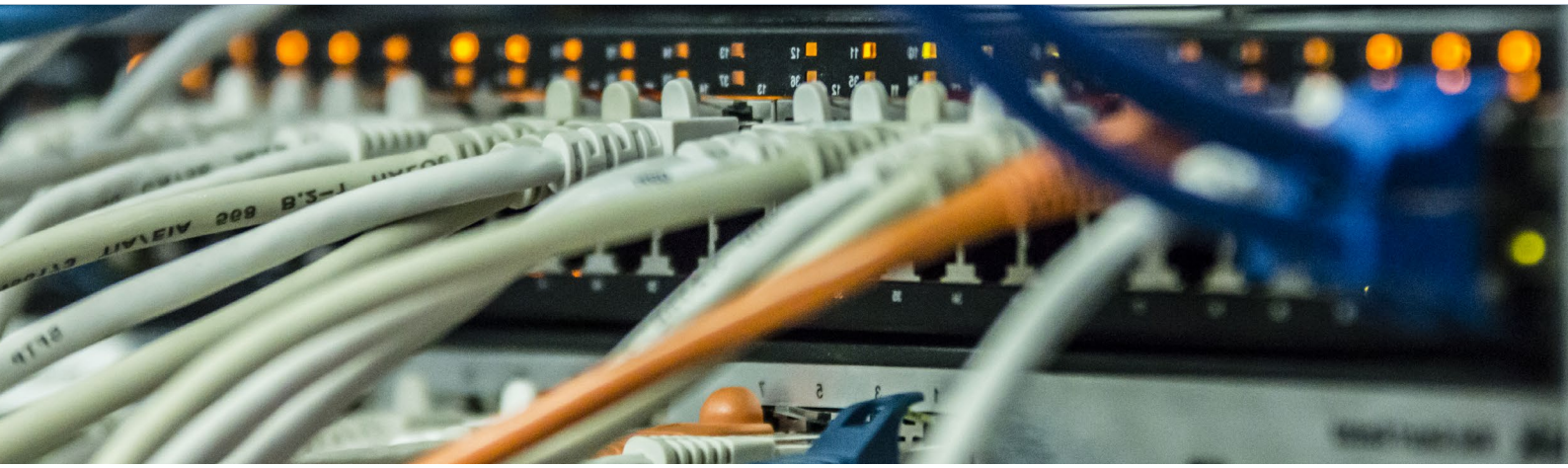
INTERNETKRIMINALITÄT (CYBERCRIME TATMITTEL)

Unter Internetkriminalität sind grundsätzlich alle Straftaten in der PKS erfasst, bei denen das Medium Internet als Tatmittel verwendet wird. Hier kommen sowohl Straftaten in Betracht, bei denen das bloße Einstellen von Informationen in das Internet bereits strafbar ist (sogenannte Äußerungs- beziehungsweise Verbreitungsdelikte), als auch solche Delikte, bei denen das Internet als Kommunikationsmedium bei der Tatbestandsverwirklichung eingesetzt wird. Auf besondere Fähigkeiten des Täters oder dessen Tatbegehungsweise kommt es dabei nicht an.

Bei der Internetkriminalität ist entgegen dem Vorjahrestrend ein leichter Rückgang um 3,6 Prozent auf 18.005 Fälle festzustellen. Verantwortlich hierfür zeichnet sich zu einem Großteil der Warenbetrug, welcher im Vergleichszeitraum um 15,6 Prozent auf 4.859 Fälle abgenommen hat.

Der Gesamtschaden hingegen hat im Vergleich zum Vorjahr um 50,5 Prozent auf 20.247.579 Euro zugenommen. Diese hohe Summe resultiert aus einem Verfahren der Inspektion 310 (Wirtschaftskriminalität) des LKA wegen Anlagebetrugs mit mehreren hundert Fällen, welches mit einem Schaden von 10.285.680 Euro in der PKS erfasst worden ist.

Die Vermögens- und Fälschungsdelikte haben im Jahr 2016 um 4,5 Prozent auf 12.610 Fälle abgenommen. Den größten Anteil hatte der Betrug mit 12.349 Fällen. Beim Waren und Warenkreditbetrug, welcher unter der Gesamtzahl des Betrugs zu subsumieren ist, gingen die Zahlen um 10,2 Prozent auf 7.844 Fälle zurück. Auch beim sonstigen Betrug haben die Fälle analog zu den Vorjahren einen Rückgang um 12,2 Prozent auf 3.204 Fälle zu verzeichnen. Die Strafrechtlichen Nebengesetze spiegeln mit einer Abnahme um 32,6 Prozent auf 839 Fälle die rückläufige Entwicklung der Internetkriminalität des Jahres 2016 wieder. Maßgeblich hierfür sind vor allem die Straftaten gegen Urheberrechtsbestimmungen, welche einen Rückgang um 32,8 Prozent auf 319 Fälle aufweisen. Auch die Rauschgiftdelikte nach dem Betäubungsmittelgesetz (BtMG) gingen um 19,8 Prozent auf 416 Fälle zurück. Im Jahr 2016 gab es nur noch drei Straftaten nach dem Datenschutzgesetz (-97,8 Prozent). Verantwortlich für den Rückgang zeichnen mehrere Verfahren des Polizeipräsidiums Mannheim aus dem Jahr 2015. Die Beschuldigten hatten Kurzzeitkennzeichen mit missbräuchlich erlangten Identitäten beantragt und anschließend gewinnbringend an Dritte verkauft.

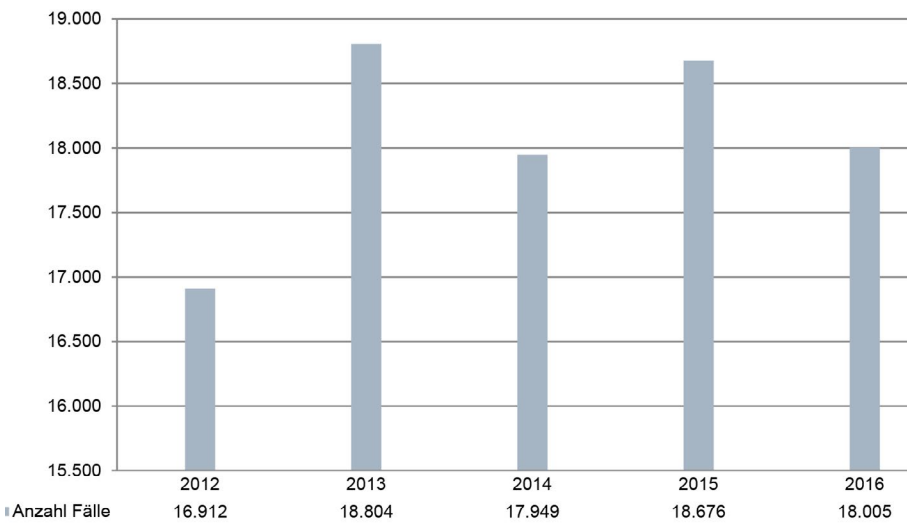


Straftaten gegen die sexuelle Selbstbestimmung hatten im Jahr 2015 einen Höchststand im Fünfjahresvergleich erreicht. Im Berichtsjahr ist die Anzahl der Fälle (773) wieder rückläufig, was einer Abnahme um 16,2 Prozent entspricht.

Maßgeblich hierfür ist vor allem die Verbreitung pornographischer Schriften mit einem Rückgang um 15,0 Prozent auf 651 Fälle. Innerhalb der Sonstigen Straftatbestände des Strafgesetzbuches (StGB) haben die Fälle der Geldwäsche nach Paragraf 261 StGB einen bemerkenswerten Zuwachs zu verzeichnen. Dieser ist mit 1.041 Fällen auf einem Höchststand im Fünfjahresvergleich und hat allein im Vergleich zum Vorjahr einen Zuwachs um 90,7 Prozent erfahren.

Ursächlich hierfür sind ein Anstieg der Fallzahlen bei der Bundespolizei im Zusammenhang mit betrügerisch erlangten Bahnfahrkarten, deren Verkaufserlöse durch Finanzagenten gewaschen wurden, sowie erhöhte Sorgfalts- und Meldepflichten der Banken.

CYBERCRIME TATMITTEL (2012 BIS 2016)



COMPUTERKRIMINALITÄT

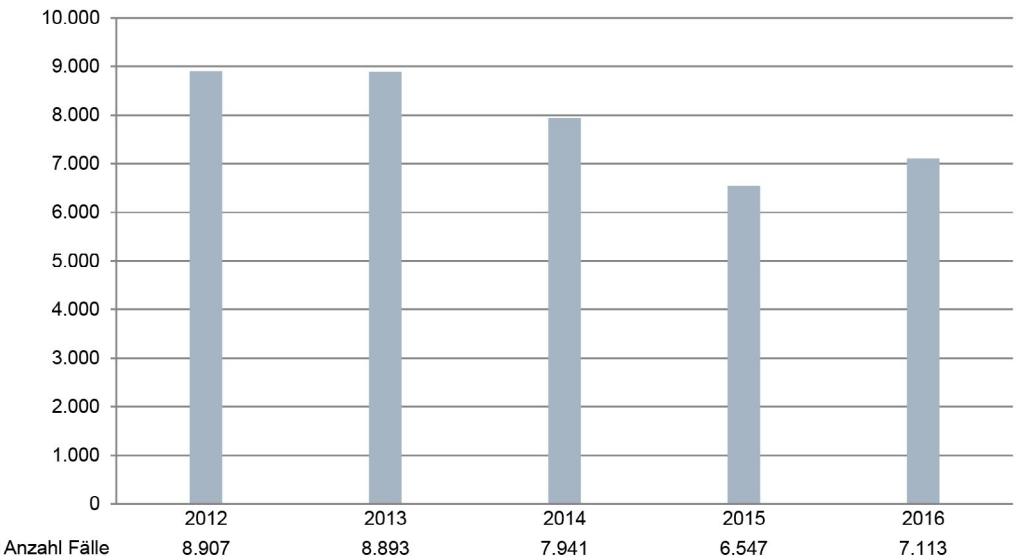
In Abgrenzung zur Internetkriminalität ist bei der Computerkriminalität die Informationstechnik nicht ausschließlich Tatmittel, sondern es geht hierbei meist um Angriffe gegen die Informationstechnik oder auf deren Daten.

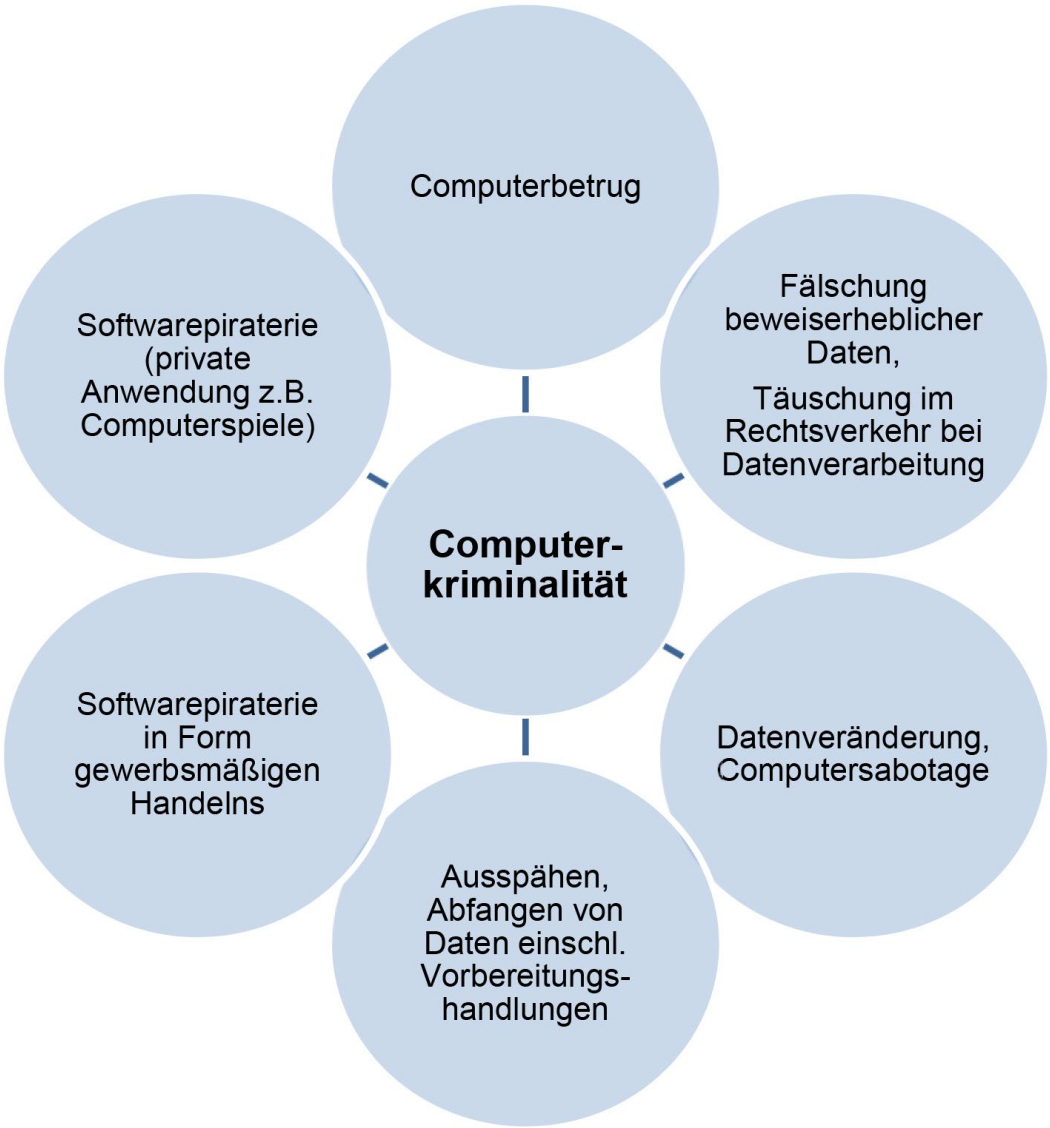
Bei der Computerkriminalität ist eine Zunahme um 8,6 Prozent auf 7.113 Fälle zu verzeichnen. Den größten Anteil bildet der Computerbetrug mit 5.813 Fällen. Durch die Überarbeitung der Erfassung der Betrugsdelikte zum 1. Januar 2016, zu welchen der Computerbetrug zählt, sind noch keine Vergleichszahlen aus den Vorjahren verfügbar.

Auch die Straftaten der Computerkriminalität, welche über das Internet begangen werden, zeigen sich rückläufig. Diese haben einen Rückgang um 9,2 Prozent auf 3.374 Fälle zu verzeichnen. Beim Computerbetrug ist hierbei ebenfalls eine Abnahme um 36,9 Prozent auf 1.356 Fälle festzustellen, wobei dieser hohe Prozentsatz seine Ursache vor allem in der Überarbeitung der Erfassungsrichtlinien hat.

Die Fallzahlen des Delikts Datenveränderung/ Computersabotage mit einer Tatbegehung über das Internet haben ihr Niveau gehalten und eine Zunahme um nur einen Fall auf 143 Fälle zu verzeichnen. Die Anzahl der Fälle bei Ausspähen von Daten sind leicht um 6,9 Prozent auf 363 Fälle zurückgegangen.

COMPUTERKRIMINALITÄT (2012-2016)




Computerbetrug
Softwarepiraterie (private Anwendung z.B. Computerspiele)
Fälschung beweiserheblicher Daten,
Täuschung im Rechtsverkehr bei Datenverarbeitung
Computer-kriminalität
Softwarepiraterie in Form gewerbsmäßigen Handelns
Datenveränderung, Computersabotage
Ausspähen, Abfangen von Daten einschl. Vorbereitungs-handlungen

2 ERMITTLUNGEN CYBERCRIME

Die Abteilung Cybercrime und Digitale Spuren des LKA bearbeitet in erster Linie sogenannte Pilot- und Mehrwertverfahren der Cybercrime im engeren Sinne[3]. Pilotverfahren sind Verfahren mit neuartigen Sachverhalten oder Aufklärungsmöglichkeiten in kriminologischer, kriminalistischer oder rechtlicher Hinsicht. Darunter fallen zum Beispiel neue Kriminalitätsphänomene und Begehungsweisen, die innovative kriminaltaktische und neue kriminaltechnische Maßnahmen erfordern. Mehrwertverfahren sind Verfahren, die starke Ressourcen oder Spezialkenntnisse und nach Bewertung der Gesamtumstände eine zentrale Ermittlungsführung erfordern. Die Ermittlungsverfahren können auf Grund eigener Feststellungen bekannt werden oder vom Bundeskriminalamt (BKA) beziehungsweise den Polizeipräsidien des Landes an das LKA herangetragen werden.

Die Kriminalinspektionen 5 (K5) der zwölf regionalen Polizeipräsidien bearbeiten ebenfalls Fälle der Cybercrime im engeren Sinne, insbesondere, wenn eine banden- oder gewerbsmäßige Begehungsweise festgestellt wird. Darüber hinaus sind sie für Fälle von Internetkriminalität zuständig, wenn zu deren Bearbeitung besonderes informationstechnisches Fachwissen und beziehungsweise oder besondere technische Beweisführungsmethoden erforderlich sind. Auch wenn auf Seiten der Täter ein hohes Maß an informationstechnischem Know-how zu erkennen ist, wird der Fall von der regionalen K5 bearbeitet, sofern er nicht in herausragenden Fällen in die Zuständigkeit des LKA fällt.

Auf Grund der faktischen und rechtlichen Komplexität sowie der rasanten Entwicklungszyklen im Bereich der Informationstechnik besteht bei den Ermittlungseinheiten der Polizeipräsidien sowie beim LKA hoher Beratungs- und Unterstützungsbedarf. Die spezialisierten Dienststellen Cybercrime und Digitale Spuren nehmen in diesem Zusammenhang ermittlungsunterstützende und beratende Tätigkeiten wahr.

1 Cybercrime im engeren Sinne umfasst bestimmte Delikte der Computerkriminalität. Eine detaillierte Auflistung der Delikte findet sich in der Polizeilichen Kriminalstatistik.

RANSOMWARE

Schadsoftware in Form sogenannter Ransomware (ransom = englisch Lösegeld) wird täterseitig bereits seit dem Jahr 1989 über verschiedene Angriffsvektoren, wie zum Beispiel Spam-Mails, über das Internet verbreitet. Zwischenzeitlich hat sich Ransomware zu einer der größten Bedrohungen für Internetnutzer entwickelt. Kennzeichnend für dieses Kriminalitätsphänomen sind die immer wieder neu erscheinenden Abwandlungen von bereits bestehenden Varianten. Unterschieden wird dabei zwischen Locker-Ransomware und Crypto-Ransomware.

Locker-Ransomware zielt darauf ab, den Zugriff eines berechtigten Nutzers auf ein infiziertes System und die darauf gespeicherten Daten zu unterbinden. Die Schadsoftware ist somit darauf ausgelegt, grundsätzlich den Zugriff auf ein Rechnersystem zu verhindern. Dabei ist es im überwiegenden Teil der Fälle nicht die Motivation der Täterseite, nachhaltige Veränderungen am Betriebssystem oder den gespeicherten Daten vorzunehmen. Um den angestrebten Zweck, das heißt die Sperrung eines infizierten Systems sowie die Zahlung einer Strafe durch das Opfer zu erreichen, blendet die Locker-Ransomware einen sogenannten Sperrbildschirm mit entsprechenden Anweisungen ein.

Im Gegensatz zu Locker-Ransomware steht bei Crypto-Ransomware die Verschlüsselung von Nutzerdaten im Vordergrund. Eine Verschlüsselung von Betriebssystemdateien findet in der Regel nicht statt, so dass das angegriffene System grundsätzlich funktionsfähig und vom Nutzer bedienbar bleibt. Lediglich ein Zugriff auf die betroffenen Nutzerdaten wird unterbunden. Crypto-Ransomware verschlüsselt Dateien verschiedenster Formate, wie beispielsweise Office-Dokumente, Bilder, Videos oder Datenbankdateien. Dabei sind häufig Dateien, welche insbesondere für Unternehmen geschäftskritisch sind, wie zum Beispiel Konstruktionszeichnungen, betroffen. Die derzeit existierenden Varianten von Crypto-Ransomware werden meist über E-Mails (deren Anhänge oder integrierte Links) unter den verschiedensten Vorwänden verbreitet. Nach Auslösung der Schadsoftware wird gleichzeitig die Zahlung von Lösegeld, meist in Form von Bitcoins, gefordert.

Nach eher rückläufigen Fallzahlen von Locker-Ransomware, wie dem sogenannten BKA-Trojaner, nahmen die Fallzahlen durch Crypto-Ransomware weiter zu. Für das Jahr 2016 wurden 1.140 Fälle von Ransomware in Baden-Württemberg bekannt, 2015 waren es dagegen noch circa 400. Von einem äußerst hohen Dunkelfeld ist auszugehen.

ERMITTLUNGSVERFAHREN GEGEN DIGITALE ERPRESSER

Derzeit führt das LKA ein Ermittlungsverfahren gegen eine international agierende Tätergruppierung im Bereich Crypto-Ransomware.

Die vom LKA verfolgte Tätergruppierung hat damit im Jahr 2016 weltweit Daten von tausenden Privatpersonen, Behörden und Unternehmen verschlüsselt und auf diese Weise Lösegeldsummen im zweistelligen Millionen-Bereich erpresst. Allein in Baden-Württemberg wurden Erpressungsfälle dieser Gruppierung im dreistelligen Bereich registriert. Der wirtschaftliche Schaden, der weltweit durch die Verschlüsselung der Nutzerdaten und die folglich notwendigen IT-Maßnahmen zur Wiederherstellung entstanden ist, liegt um ein Vielfaches höher.

ERMITTLUNGEN IN ZUSAMMENHANG MIT ÜBER 250 MILLIONEN INFIZIERTEN RECHNERN

Das LKA ermittelt seit dem Jahr 2013 gegen eine Tätergruppierung, welche weltweit verschiedene Varianten von Locker-Ransomware verbreitet. Mit dieser Schadsoftware wurden nachweislich Millionen Rechner infiziert. Die dabei von den Geschädigten geforderte Lösegeldsumme beläuft sich auf jeweils 100 Euro beziehungsweise einen ähnlich hohen Betrag in der entsprechenden Landeswährung. Durch umfangreiche technische Maßnahmen konnte nachgewiesen werden, dass die Tätergruppierung damit bislang einen knapp zweistelligen Millionenbetrag an Geldern eingenommen hat.

Die Gruppierung konnte inzwischen im Ausland lokalisiert werden. Weitere polizeiliche Maßnahmen werden aktuell mit dem entsprechenden Staat abgestimmt.

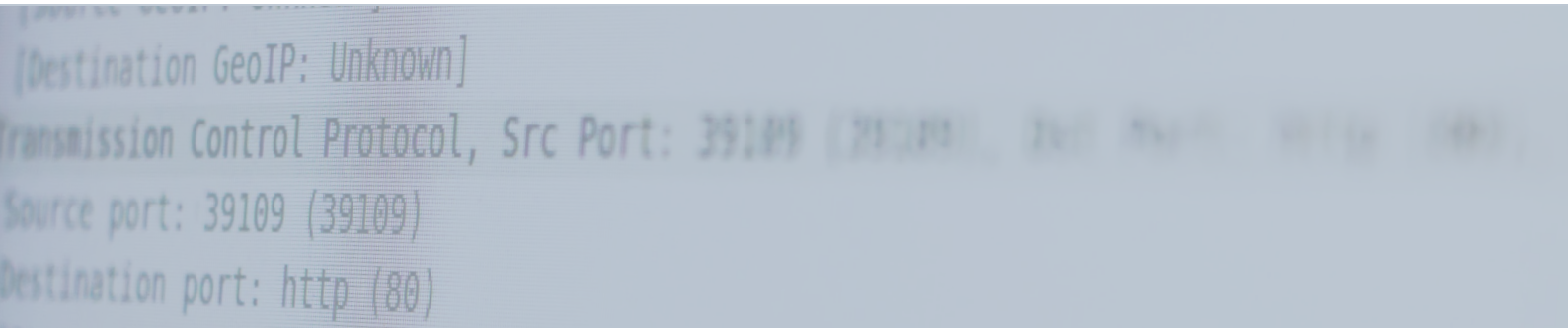
Beschlagnahmebanner (auch veröffentlicht in der Pressemitteilung der GenStA Frankfurt am Main vom 29.02.2016), der noch unter http://fato.me abrufbar ist. Die Domains faking.cc und comlync.cc sind nicht mehr erreichbar (Stand Januar 2017).

GEMEINSAME AKTION GEGEN BETREIBER ILLEGALER MARTKPLÄTZE IM NETZ

Gemeinsam mit dem Bundeskriminalamt und anderen Landeskriminalämtern beteiligte sich das LKA auch im Jahr 2016 im Kampf gegen die Mitglieder illegaler Foren im Internet sowie im Darknet. Dabei wurden in einer bundesweiten Aktion die deutschsprachigen Foren faking.cc, comlync.cc sowie fato.me durch das Bundeskriminalamt abgeschaltet und deren Betreiber festgenommen.

In diesen Foren wurde ein schwunghafter Handel mit illegalen Gütern wie Waffen, Betäubungsmitteln, Falschgeld, gefälschten Ausweisdokumenten und ausgespähten Daten betrieben. Darüber hinaus umfasste die Angebotspalette der Foren auch kriminelle Dienstleistungen, wie beispielsweise die Herstellung oder Verteilung von Schadsoftware.

Trotz Anonymisierung der Forenmitglieder im Darknet gelang es dem LKA durch intensive Ermittlungen, Tatverdächtige im Alter zwischen 18 und 31 Jahren zu identifizieren. Allein in Baden-Württemberg wurden im Rahmen einer bundesweiten eintägigen Durchsuchungsaktion Wohnungen von zehn Beschuldigten durchsucht und verschiedenste Beweismittel sichergestellt. Darunter befanden sich Computer, Smartphones, Tablets und andere elektronische Datenträger sowie schriftliche Unterlagen.



INTERNETRECHERCHE

Der Arbeitsbereich Internetrecherche (AIR) befasst sich mit der brennpunktorientierten, nicht extern initiierten Suche nach Inhalten im Internet zum Zwecke der Gefahrenabwehr und Verfolgung von festgestellten strafrechtlich relevanten Sachverhalten. Dies schließt die Beweissicherung bis zur Feststellung der Verantwortlichen und der örtlichen Zuständigkeiten von Polizei und Justiz mit ein. Außerdem werden neue Recherche- beziehungsweise Beweissicherungsmethoden sowie notwendige Recherche- und Sicherungstools entwickelt. Diese werden den Polizeipräsidien bei Bedarf zur Verfügung gestellt. Der AIR unterstützt darüber hinaus anlassbezogen die Polizeipräsidien bei Sonderlagen, wie beispielsweise der Fußballweltmeisterschaft, aber auch anlassbezogen bei Ermittlungen zu Kapitaldelikten.

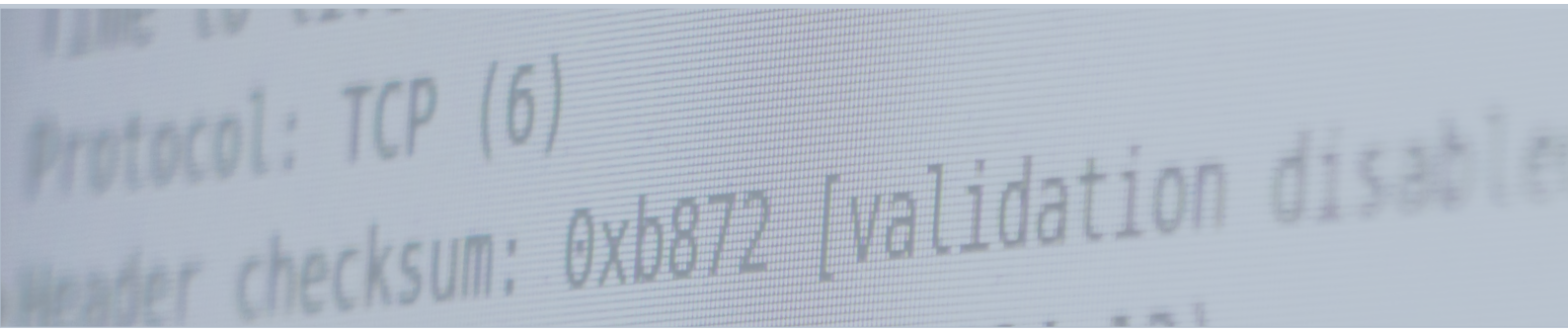
Zum Aufgabengebiet gehört auch die Beobachtung neu entstehender Internetdienste, zu welchen gegebenenfalls neue gerichtsfeste Beweissicherungsverfahren zu entwickeln sind.

INITIIERUNG VON ERMITTLUNGSVERFAHREN

Im Jahr 2016 führte der AIR sieben Operationen wegen der Verbreitung von Kinderpornografie in dezentralen Netzwerken (Tauschbörsen) durch. Infolgedessen konnten weltweit 11.746 Strafverfahren initiiert werden. Hierbei konnten 34 Tatverdächtige aus Baden-Württemberg und insgesamt 664 Tatverdächtigen bundesweit festgestellt werden.

Durch den Rücklauf der mit den Operationen verbundenen Erkenntnisanfragen wurde festgestellt, dass zahlreiche Tatverdächtige bereits einschlägige Erkenntnisse im Bereich der Sexualstraftaten hatten. In mehreren Fällen waren sie zudem bereits in Operationen des AIR aus den vergangenen Jahren als Besitzer beziehungsweise Verbreiter von kinderpornografischen Dateien aufgefallen. Der Anteil der Verfahren mit deutschen Tatverdächtigen, bei denen die Provider die angefragten Verbindungsdaten nicht beauskunfteten, lag im Berichtszeitraum bei rund 32 Prozent (unzureichende Vorratsdatenspeicherung). Andere Möglichkeiten zur Identifizierung der Täter bestanden nicht, so dass der Staatsanwaltschaft eine Strafanzeige gegen Unbekannt vorgelegt werden musste.

Berichtsjahr	2012	2013	2014	2015	2016
Deutschland	40	297	731	921	664
davon Baden-Württemberg	4	25	69	59	34
International	676	5.716	10.387	13.550	11.746

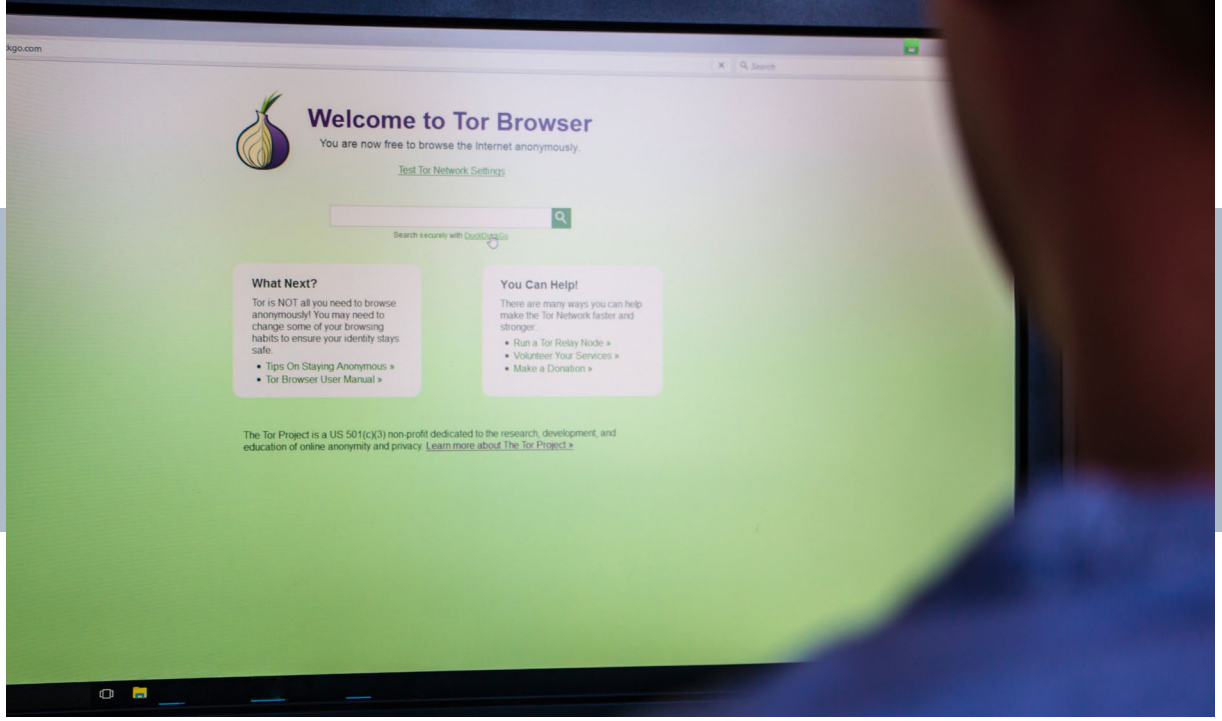


BEENDIGUNG ANDAUERNDER MISSBRAUCHSHANDLUNGEN

Immer wieder können im Rahmen von Operationen anhaltende Missbrauchsfälle beendet werden. So konnte auch im Februar 2016 durch den AIR ein Verbreiter von kinderpornografischen Dateien identifiziert und in der Folge weitere Missbrauchshandlungen zum Nachteil eines Kindes unterbunden werden. Die Auswertung der sichergestellten Hard- und Software ergab Hinweise auf einen schweren sexuellen Missbrauch des Kindes, der durch den identifizierten Mann und seine Lebensgefährtin, die Mutter des Kindes, begangen wurde.

GEFÄHRDUNGSLAGEN

Der AIR war im Berichtszeitraum in 18 Gefährdungslagen eingebunden. Darunter fielen 13 Suizidankündigungen. Fünf weitere Gefährdungslagen betrafen Hinweise auf sonstige Bedrohungslagen, wie beispielsweise Amok- oder Morddrohungen. Bezüglich einer Suizidankündigung konnte die betroffene Person durch den AIR identifiziert werden. Die Person wurde nach Informationen der örtlich zuständigen Polizei auf freiwilliger Basis in die Psychiatrie verbracht.



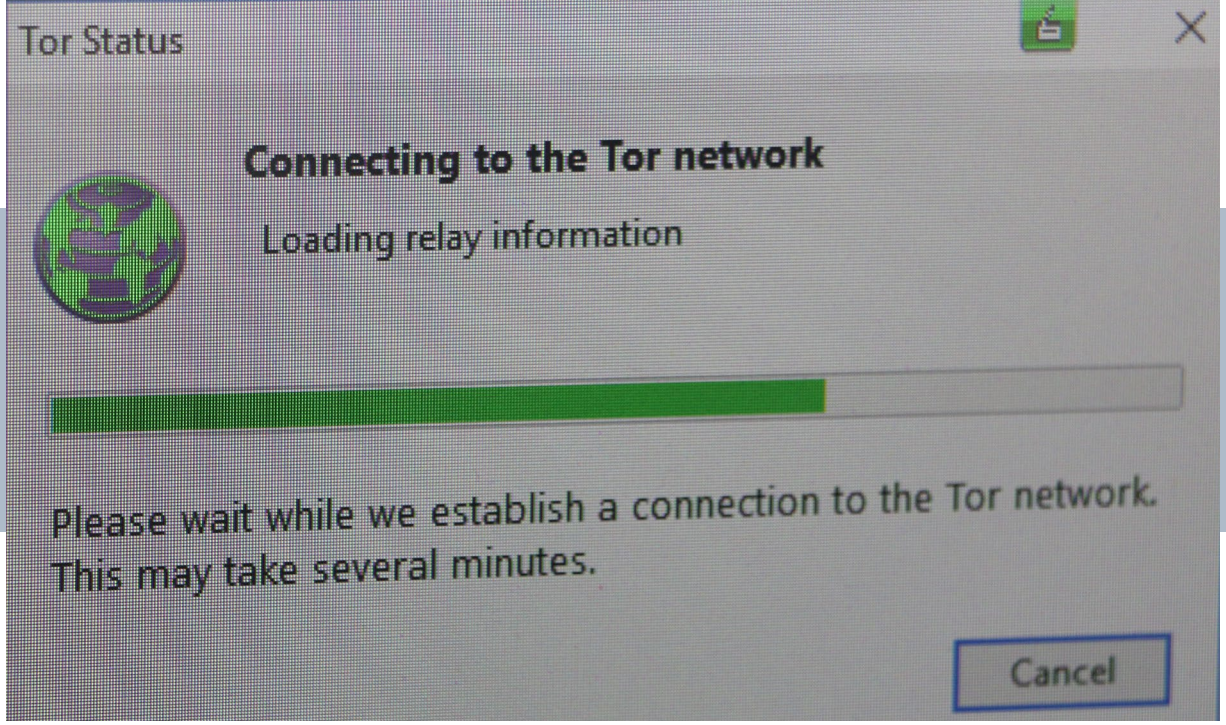
Ein Weg ins Darknet: Der Tor Browser baut eine anonyme Verbindung ins Netz auf.

DARKNET

Das Darknet ist der Teil des Internets, welcher für den konventionellen Nutzer ohne entsprechende Software sprichwörtlich im Dunkeln verborgen bleibt. Der bekannteste Teil des Darknets ist das sogenannte TOR-Netzwerk. Mittlerweile besteht ein bedeutender Teil des Darknets aus Marktplätzen, bei denen inkriminierte Güter anonym gehandelt werden. Diese beinhalten beispielsweise Waffen, Betäubungsmittel, Arzneimittel, Falschgeld, gefälschte Dokumente sowie Kinderpornografie. Außerdem werden unter dem Schlagwort Crime-as-a-Service zunehmend kriminelle Dienstleistungen und Schadsoftware angeboten.

Seit der polizeilich erwirkten Schließung des Darknet-Forums Silk Road im Oktober 2013, dem bis dahin größten Drogenumschlagplatz im TOR-Netzwerk, gewannen andere, bereits bestehende und neu gegründete Markplätze zunehmend an Popularität. Gemäß einer im August 2015 veröffentlichten Studie der Carnegie Mellon University und einer im August 2016 veröffentlichen Studie der RAND Corporation hat sich das Umsatzvolumen an Angeboten aller Art seit Schließung von Silk Road bis Januar 2016 verdoppelt, die Anzahl an Transaktionen verdreifacht und die Angebotsliste um das 5,5-Fache vergrößert. Der rasante Anstieg zeigt die Brisanz der prinzipiell für jedermann zugänglichen Handelsmöglichkeiten. Ein Beispiel hierfür stellt der Amoklauf von München im Juli 2016 dar, zu dessen Durchführung der Täter seine Waffe über das Darknet bezogen hatte.

Die Techniken des Darknet beziehungsweise die Aktivitäten der Nutzer sind auf größtmögliche Anonymität ausgelegt. Entsprechend widerstandsfähig sind die Marktplätze bislang gegen staatliche beziehungsweise polizeiliche Eingriffe. Neben anonymen Zugangsmöglichkeiten betrifft dies auch die Bezahlung der bestellten Waren. Transaktionen erfolgen in der Regel mit der virtuellen Währung Bitcoin, der aktuell populärsten Krypto-Währung.



Tor schützt seine Nutzer vor der Analyse des Datenverkehrs.

Bitcoin ist ein weltweit verfügbares dezentrales Zahlungssystem. Überweisungen werden von einem Zusammenschluss von Rechnern über das Internet und mithilfe einer speziellen Peer-to-Peer-Anwendung abgewickelt, sodass dabei keine zentrale Abwicklungsstelle wie im herkömmlichen Zahlungsverkehr über Banken benötigt wird.

Möglichkeiten zur Identifizierung von Straftätern, welche sich das Darknet zunutze machen, ergeben sich dennoch. Die Schnittstellen zwischen der realen und der virtuellen Welt, wie zum Beispiel der Versand inkriminierter Güter sowie die Zahlungsströme, spielen dabei eine große Rolle. Im Berichtszeitraum konnten durch den AIR mehrere sogenannter Powerseller ermittelt werden. Ermittlungen des LKA führten beispielsweise im August 2016 zu einem Drogen-Händler in Österreich. Die dortigen Strafverfolgungsbehörden haben im Rahmen von Durchsuchungsmaßnahmen neben einem Labor zur Herstellung von Amphetaminen verschiedene Betäubungsmittel und verschreibungspflichtige Arzneimittel mit einem Nettogewicht von 13 Kilogramm sichergestellt.

ANSPRECHSTELLE KINDERPORNOGRAFIE

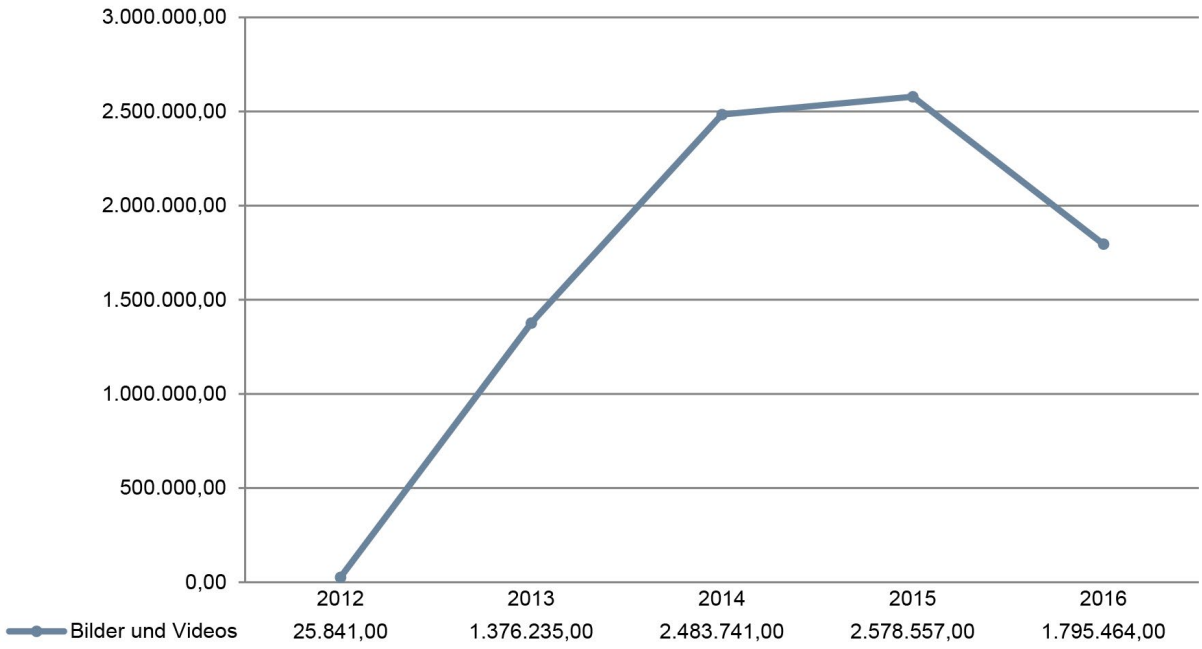
Die Ansprechstelle Kinderpornografie (ASt KiPo) ist die zentrale Ansprech- und Koordinierungsstelle des Landes im Zusammenhang mit Besitz, Verschaffen und Verbreitung kinderpornografischer Schriften. Hauptaufgabengebiete sind die Aufnahme und Bearbeitung von Bürgerhinweisen auf kinder- und jugendpornografische Inhalte im Internet, die Koordinierung von Umfangsverfahren im Deliktsbereich Kinderpornografie und die Kategorisierung von deliktsspezifischen Dateien, welche von den Landesdienststellen angeliefert werden.

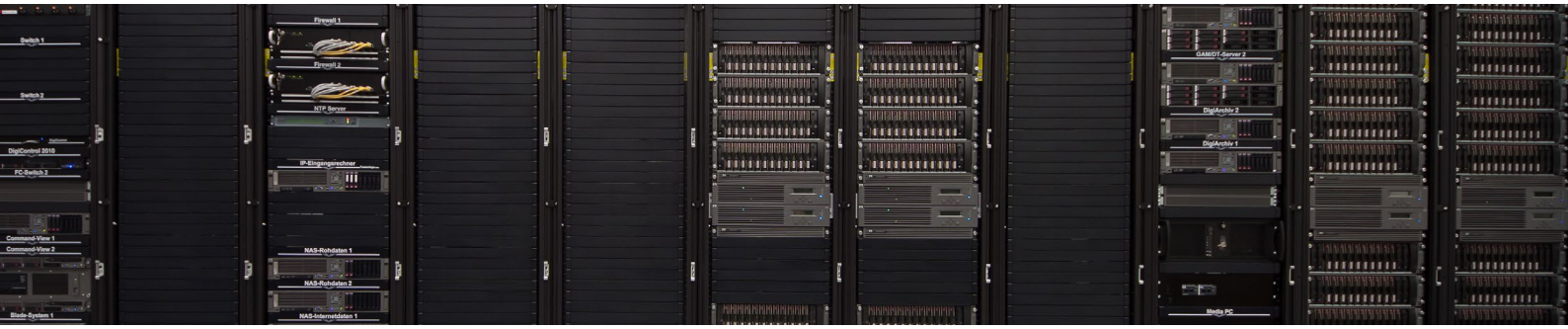
Der Deliktsbereich Verbreitung, Erwerb, Besitz und Herstellung von Kinderpornografie erfuhr mit 703 Fällen eine Steigerung um 17,4 Prozent zum Vorjahr. Die Aufklärungsquote betrug in diesen Fällen 77,5 Prozent. Seit dem Jahr 2016 wird in der PKS nicht mehr zwischen Verbreitung und Besitz/Verschaffen pornografischer Schriften unterschieden.

Bei der Ansprechstelle Kinderpornografie (ASt KiPo) des LKA wurden insgesamt 71 Umfangsverfahren mit 139 Tatverdächtigen in Baden-Württemberg koordiniert. Davon wurden allein 27 Verfahren in Baden-Württemberg initiiert.

Durch die Mitarbeiter der ASt KiPo wurden im Jahr 2016 über 1,3 Millionen Dateien kategorisiert. Hierbei werden Bilder und Videos bewertet, ob sie anhand ihrer Darstellung die Kriterien für die strafrechtliche Verfolgung aufgrund Kinder- oder Jugendpornografie erfüllen. Alle bewerteten relevanten Hashwerte werden dem BKA zur Eingabe in die Hash-Datenbank Pornografische Schriften übermittelt, welche dann bundesweit für polizeiliche Sachbearbeiter abrufbar sind. Bereits nach nur zweijähriger Nutzungszeit des landesweit eingeführten Auswertesystems ZiuZ konnte der bis zu diesem Zeitpunkt vorliegende bundesweite Datenbestand durch Zulieferungen aus Baden-Württemberg mehr als verdoppelt werden. Der Einsatz dieser Hashwerte führt zu einer deutlichen Reduzierung der manuell zu bewertenden Dateien in laufenden Ermittlungsverfahren. Zudem wird die psychische Belastung der Sachbearbeiter deutlich reduziert, da Bilder und Videos nicht mehrfach bewertet werden müssen.

ANLIEFERUNGEN DER POLIZEIDIENSTSTELLEN DES LANDES ZUR KATEGORISIERUNG





IDENTIFIZIERUNGSVERFAHREN UND SCHULFAHNDUNG

Identifizierungsverfahren werden anhand eines bundesweiten Stufenmodells zur polizeilichen Fahndung nach Tätern und Opfern des sexuellen Missbrauchs an Kindern und Jugendlichen durchgeführt. Das BKA leitete im Jahr 2016 insgesamt 31 Identifizierungsverfahren ein. Hiervon konnten in 18 Verfahren Täter und Opfer identifiziert werden, in vier Fällen war Baden-Württemberg betroffen.

Bei Fällen, in denen das polizeiinterne Identifizierungsverfahren nicht zum Erfolg führt, wird die Durchführung einer sogenannten Schulfahndung geprüft. Bei dieser Maßnahme werden Bilder eines mutmaßlich in Deutschland wohnenden minderjährigen Opfers eines sexuellen Missbrauchs an die Schulleitungen im Land zur Fahndung unter Mitwirkung der Lehrkräfte übermittelt. Die seit einigen Jahren unter Koordination der ASt KiPo praktizierte Fahndungsart hat sich als Mindermaßnahme zur Öffentlichkeitsfahndung bewährt. Ziel ist die Identifizierung des Opfers, um einen möglicherweise noch andauernden sexuellen Missbrauch zu beenden und die Straftat aufzuklären.

Im Jahr 2016 wurden zwei Schulfahndungen durchgeführt. Insgesamt wurde nach sechs Kindern gefahndet. Bei der Ast KiPo gingen in beiden Fällen zahlreiche Hinweise ein. Die in der Frühjahrsfahndung gesuchten vier Kinder konnten inzwischen alle identifiziert und außerhalb Baden-Württemberg zugeordnet werden. Die Herbstfahndung ist dagegen noch nicht in allen Bundesländern abgeschlossen (Stand Januar 2017). Sowohl diese als auch weitere zurückliegende Ermittlungserfolge verdeutlichen die Bedeutung des Instruments der zielgruppenorientieren Öffentlichkeitsfahndung in Form der Schulfahndung.

TECHNIKER-WORKSHOP 2016

Der diesjährige Techniker-Workshop des LKA fand vom 6. bis 8. Dezember 2016 statt. Informatiker sowie Polizeibeamte mit Programmieraufgaben aus den jeweiligen Cybercrime-Abteilungen aller Bundesländer, aus Österreich und der Schweiz tauschten sich bei dieser Veranstaltung über aktuelle Entwicklungen im Bereich der IT sowie eigenentwickelte Software aus. Schwerpunkt der diesjährigen Veranstaltung war die Sicherung von Inhalten in sozialen Netzwerken.

Frank Winterhalter, Inspektionsleiter bei der Abteilung Cybercrime und Digitale Spuren eröffnet den Techniker-Workshop.

3 DIGITALE FORENSIK

IT-FORENSIK – WAS IST DAS?

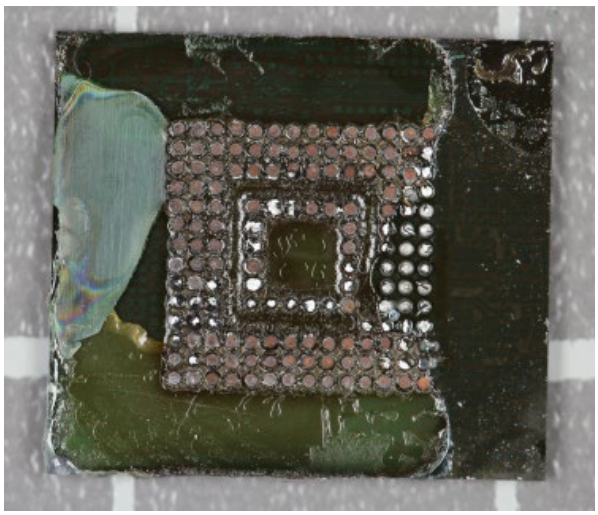
Die Spurensuche, deren anschließende Sicherung und inhaltliche Auswertung sind seit jeher wesentliche Bestandteile in den polizeilichen Arbeitsprozessen. Die digitalen Spuren haben ergänzend zu den klassischen Spurenarten, wie Finger-, Schuhlaufflächen-, Werkzeug- oder DNA-Spuren, in den zurückliegenden Jahren an Verbreitung zugenommen und damit einhergehend weiter an Bedeutung für polizeiliche Ermittlungen gewonnen. Sie umfassen nicht nur vom Benutzer selbst erzeugte Inhalte wie Bilddateien, Videos, E-Mails, SMS-Nachrichten oder Office-Dokumente.

In einer immer enger vernetzten Welt, in der nicht nur Menschen sondern zunehmend Maschinen und Systeme miteinander kommunizieren, fallen auch fortlaufend Spuren ohne menschliches Zutun an. Insbesondere diese kaum manipulierbaren Spuren sind auch in der Digitalen Forensik von besonderem Interesse. Digitale Spuren spielen nicht nur bei der Bekämpfung der Cyberkriminalität eine Rolle, sie können in nahezu jedem Deliktsbereich von Bedeutung sein. Gerade in Wirtschaftsdelikten, Rauschgiftverfahren und in Staatsschutzangelegenheiten werden zahlreiche Asservate sichergestellt, um sie auf ihre digitalen Spurenlagen untersuchen zu lassen. So hat die IT-Forensik auch im Jahr 2016 in nahezu allen pressebekannten Ermittlungsverfahren beratend oder direkt durch die Untersuchung digitaler Spurenträger unterstützt.

SMARTPHONE IN FLAMMEN

Bei einem Wohnungsbrand starben im letzten Jahr zwei Menschen. Um die Brandursache zu ermitteln wurde neben weiteren Gegenständen ein Smartphone sichergestellt. Trotz des Feuerschadens konnten die Forensiker des LKA die auf dem Gerät gespeicherten Daten auslesen und den Ermittlern zur Verfügung stellen.

Das Smartphone ist nur schwer als ein solches zu erkennen.



Auch der interne Speicher war stark beschädigt.

Analog zu Sicherungsmethoden der klassischen Kriminaltechnik (wie beispielsweise DNA-, Werkzeug- oder Fingerabdruckspuren) unterstützt die IT-Forensik die polizeilichen Ermittler beim Umgang mit digitalen Spuren. Die Arbeit der IT-Forensik beginnt meist mit der forensischen Sicherung der Spuren aus allen denkbaren Arten von Geräten der IT- und Kommunikationstechnik. Forensische Sicherungen können dabei entweder direkt vor Ort, zum Beispiel im Rahmen von Durchsuchungen beziehungsweise an Tatorten, oder aber in den IT-forensischen Laboren der Polizeipräsidien erfolgen und erfordern tiefgehende Fachkenntnisse bezüglich der Funktionsweise der zu sichernden Geräte und Systeme.

Bei der forensischen Sicherung digitaler Spuren ist analog zur Arbeit in anderen kriminaltechnischen Disziplinen insbesondere darauf zu achten, dass keine Veränderungen an den Originalasservaten oder am Originaldatenbestand durchgeführt werden. Eine lückenlose Dokumentation der einzelnen Arbeitsschritte ist bereits in dieser Phase unabdingbar, um eine größtmögliche Verwertbarkeit der gesicherten Daten im anschließenden Ermittlungsverfahren sowie später vor Gericht zu gewährleisten.

Nach erfolgter forensischer Sicherung werden die vorliegenden Daten untersucht und aufbereitet, sodass diese durch den polizeilichen Ermittler weiterverwendet werden können. Jede einzelne digitale Spur – hierzu zählen zum Beispiel Dateien, aber auch durch Betriebssystem und Programme für den Nutzer unbewusst erzeugte Aktivitäts- und Ereignisprotokolle – ist (unter Umständen auch nach deren Löschung) zu lokalisieren, lesbar zu machen, gegebenenfalls zu entschlüsseln, zu klassifizieren, technisch zu interpretieren und für die weitere Verwendung und Bewertung durch den polizeilichen Ermittler aufzubereiten und diesem in geeigneten Formaten zur Verfügung zu stellen.

Die Untersuchung und Aufbereitung digitaler Spuren erfordert ein hohes Maß an Fachwissen, Zeit und Rechenleistung. Nur durch stetige Weiterentwicklung der Untersuchungsmethoden und Investitionen in die eingesetzte Technik kann eine Aufrechterhaltung der aktuellen Leistungsfähigkeit in der IT-Beweissicherung gewährleistet werden.

DATEN NACH WASSERSCHADEN WIEDERHERGESTELLT

An einem Tatort wurde im vergangenen Jahr eine SD-Speicherkarte in einer Wasserpfütze aufgefunden. Die Karte war durch Feuchtigkeitseinwirkung und nachfolgende Korrosion stark beschädigt, so dass diese mit herkömmlichen Methoden nicht mehr ausgelesen werden konnte. Den Spezialisten der IT-Forensik des LKA gelang es, die durch Korrosion unterbrochenen Leiterbahnen im Zehntel-Millimeter-Bereich wiederherzustellen und die auf der Karte enthaltenen und für das Tatgeschehen relevanten digitalen Spuren zu sichern und den polizeilichen Ermittlern zur Verfügung zu stellen.

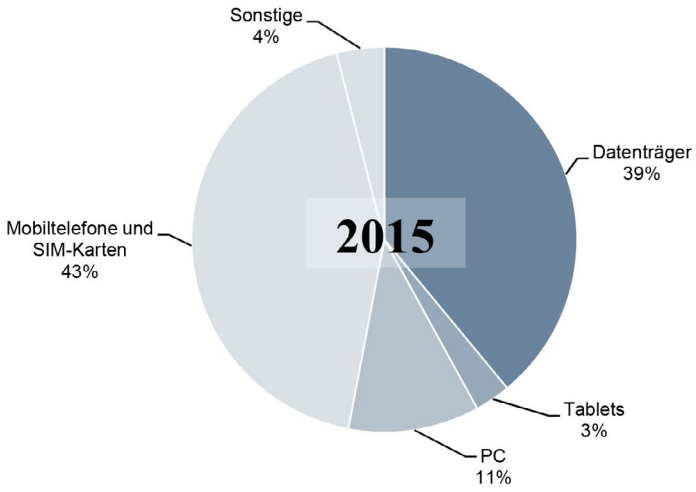
AUFTRAGSLAGE IT-FORENSIK

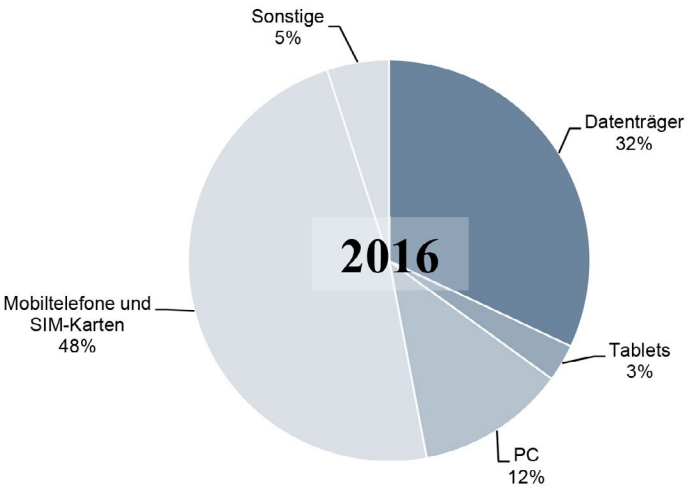
Bei den IT-Forensik-Dienststellen sind im Jahr 2016 insgesamt 10.683 Aufträge zur Untersuchung digitaler Spuren eingegangen. Dies entspricht einer moderaten Steigerung von 442 Aufträgen im Vergleich zum Vorjahr. Die Anzahl der in diesem Zusammenhang übergebenen Asservate ist von 29.669 im Jahr 2015 auf 28.987 im Jahr 2016 leicht zurückgegangen. Diese Zahlen sind aufgrund unterschiedlicher Schwerpunktsetzungen im Ermittlungsbereich Fluktuationen unterworfen. So wurden beispielsweise im Jahr 2015 im Rahmen eines einzigen Untersuchungsauftrags aus dem Deliktsbereich Kinderpornographie 1.851 CDs und DVDs zur Untersuchung und Aufbereitung übergeben.

ASSERVATENMIX

Im Vergleich zum Vorjahr ist ein Anstieg des Anteils der untersuchten Mobiltelefone und SIM-Karten zu beobachten. 13.792 Mobiltelefone und SIM-Karten wurden im Jahr 2016 untersucht, im Jahr 2015 waren es 12.902.

Aufgrund der kontinuierlich zunehmenden Speicherkapazitäten von Smartphones, Festplatten und anderen digitalen Spurenträgern, nimmt jedoch auch bei gleichbleibender Anzahl der zu untersuchenden Geräte der Aufwand für Sicherung und Aufbereitung der digitalen Spurenbefunde stetig zu.





UNTERSUCHUNG VON MASSENDATEN

Die Polizei unterscheidet bei der Untersuchung von großen Datenmengen zwischen strukturierten und unstrukturierten Massendaten. Daten, die bereits im Vorfeld in definierte Strukturen mit festgelegter Bedeutung überführt wurden, werden als strukturierte Massendaten bezeichnet. So handelt es sich beispielsweise bei Funkzellendaten, die in einem bestimmten Daten-Format vorliegen, um strukturierte Massendaten, welche durch die Datenanalyse bearbeitet werden. Bei der Kombination von Daten verschiedenster Art – zum Beispiel Bilddateien, Videos, E-Mails, Office-Dokumente – wie sie normalerweise auf IT-Systemen (zum Beispiel auf PCs oder in Smartphones) vorhanden sind, spricht man von unstrukturierten Massendaten.

Es sind daher auch mehrheitlich unstrukturierte Massendaten, welche bei der IT-Forensik untersucht und aufbereitet werden müssen. Stetig steigende Kapazitäten der in Smartphones, PCs, Laptops und Tablets verbauten Speichermedien sowie kontinuierlich steigende Gerätezahlen führen folglich zu steigenden Anforderungen an die Kapazitäten und Leistungsfähigkeit der zur forensischen Untersuchung und Aufbereitung dieser Daten genutzten Hard- und Softwaresysteme.

Hierbei stellt nicht nur die Zunahme der Datenmenge ein Problem dar, sondern auch die Integration von Daten aus unterschiedlichen Asservatentypen. Um die inhaltliche Auswertung von relevanten Spurenlagen möglichst effizient gestalten zu können, ist es erstrebenswert, die Anzahl der Prozessschritte möglichst gering zu halten. Auch im Jahr 2016 wurden umfangreiche Investitionen getätigt, um die Leistungsfähigkeit der eingesetzten Systeme zu verbessern und für zukünftige Anforderungen gewappnet zu sein.

INTERNET DER DINGE

Inzwischen finden wir in sämtlichen Lebensbereichen die unterschiedlichsten Informations- und Kommunikationstechnologien. Hierdurch entstehen für die polizeiliche Ermittlungsarbeit neue Spurenquellen. Vernetzte Geräte aus dem Bereich Smart Home können Informationen über An- und Abwesenheitszeiten von Tatverdächtigen liefern. Moderne Unterhaltungselektronik bietet oftmals Kommunikationsfunktionen und kann so im Rahmen von Ermittlungsverfahren eine Quelle relevanter Informationen sein.

Die IT-forensische Untersuchung derartiger Geräte unterscheidet sich oftmals grundlegend von der Untersuchung klassischer Träger digitaler Spuren wie PCs oder Mobiltelefonen. Die forensische Sicherung erfordert zumeist hardware-nahes Arbeiten, so dass im Gegensatz zur bisherigen IT-forensischen Tätigkeit zunehmend auch tiefere elektrotechnische Kenntnisse benötigt werden. Erschwerend kommt hinzu, dass sich bedingt durch eine hohe Anzahl verschiedener Modelle sowie kurze Produktzyklen eine Entwicklung standardisierter Sicherungs- und Untersuchungsmethoden als äußerst schwierig erweist, so dass oftmals erst bei Vorliegen des Untersuchungsauftrags entsprechende Methoden für den jeweiligen Einzelfall entwickelt werden müssen. Die Polizei reagiert auf diese Entwicklungen unter anderem durch Einstellung von Experten mit abgeschlossenem elektrotechnischem Ingenieursstudium.

DATEN IN DER CLOUD

Für Ermittlungsverfahren relevante Spuren befinden sich trotz wachsender Speicher immer häufiger nicht nur auf lokalen IT- und Kommunikationsgeräten, sondern sind, mit zunehmender Verbreitung von Cloud-Diensten, auf räumlich dislozierten Serversystemen – das heißt in der Cloud – gespeichert. Aufgrund der räumlichen Distanz sowie der eingesetzten Technologien erfordert die forensische Sicherung von digitalen Spuren in der Cloud spezielle Sicherungsmethoden, welche sich stark von den Sicherungsverfahren für herkömmliche IT- und Kommunikationsgeräte unterscheiden. Die IT-Forensik der Polizei reagiert auf diese Herausforderung durch stetige Weiterentwicklung der Sicherungsmethoden sowie deren Anpassung an die im Markt der Cloud-Dienste kontinuierlich stattfindenden Veränderungen.

MULTIMEDIAFORENSIK

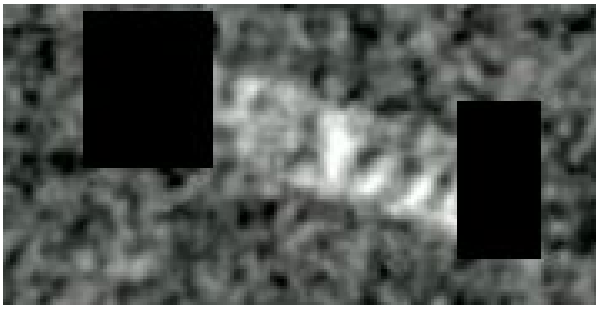
Das Aufgabenfeld der Multimediaforensik umfasst unter anderem:

- die Sicherung von Multimediadaten aus proprietären Systemen (zum Beispiel aus Videoüberwachungsanlagen)
- die Verbesserung von Multimediadaten bei unzureichender Qualität
- die Konvertierung in andere Dateiformate
- die forensische Untersuchung auf Manipulation der Daten
- die Feststellung des digitalen Endgerätes, mit dem die Daten aufgenommen oder erstellt wurden
- die Untersuchung versteckt eingebetteter Inhalte innerhalb einer Multimediadatei (Steganografie)

UNLESBARES KENNZEICHEN

Im Rahmen von Ermittlungen bezüglich Landfriedensbruchs wurde von den Ermittlern ein Überwachungsvideo sichergestellt. Das Kennzeichen eines verdächtigen Fahrzeugs war zunächst nicht lesbar, konnte jedoch durch die Multimediaforensik erfolgreich aufbereitet werden. Teile des Kennzeichens wurden für den Bericht wieder unkenntlich gemacht:

vorher:



nachher:

Das Arbeitsfeld der Multimediaforensik befasst sich mit der Aufbereitung und Untersuchung von digitalen Bild-, Video- und Audiodateien. Neben einem ansteigenden Fallaufkommen erlangt die Thematik Multimediaforensik eine zunehmende Bedeutung bei der Terrorismusbekämpfung.

Die Daten stammen beispielsweise aus Videoüberwachungen von öffentlichen Plätzen und Einrichtungen oder werden durch Zeugen zugeliefert, die einen relevanten Vorfall mittels Smartphone aufgezeichnet haben. Um die inhaltliche Auswertung vorzubereiten, bedarf es mitunter einer Aufbereitung der übermittelten Daten, um sie an die Anforderungen der Ermittler anzupassen. Die Bandbreite der Delikte umfasst den einfachen Diebstahl, bis hin zur Unterstützung von Sonderkommissionen oder Ermittlungsgruppen bei Schwerstkriminalität. Auch die Entwicklung von Algorithmen zur automatischen Bewegungserkennung in umfangreichen Videobeständen ist Bestandteil der Multimediaforensik.

Je nach Komplexität des Auftrags beträgt der Zeitaufwand für die Bearbeitung eines Falles zwischen wenigen Tagen und mehreren Monaten. Inzwischen konnte der Bereich, der bislang durch drei Polizeibeamte betreut wurde, personell mit zwei weiteren Mitarbeitern mit wissenschaftlicher Ausbildung verstärkt werden. Durch die Bündelung von forensischem Wissen der Polizeibeamten und technischen Fachwissen der Mitarbeiter mit wissenschaftlichen Hintergrund werden Synergieeffekte erzielt und im Ergebnis häufig aussagekräftige Untersuchungsergebnisse erreicht. Die Beschäftigung von Personal mit technisch wissenschaftlichem Hintergrund ist einem Spezialbereich, wie der Multimediaforensik, nicht mehr wegzudenken. Im Jahr 2017 wird die Multimediaforensik durch weiteres Personal verstärkt.

DATENANALYSE

Die Datenanalyse hat sich zu einem wichtigen Instrument für die Gewinnung von Ermittlungsansätzen entwickelt. Im Mittelpunkt des nachfolgenden Beispiels steht die Aufbereitung und ermittlungsorientierte Analyse von Personendaten.

DER TATHERGANG:

EINE RAUBSERIE AUF ÖRTLICHE TANKSTELLEN

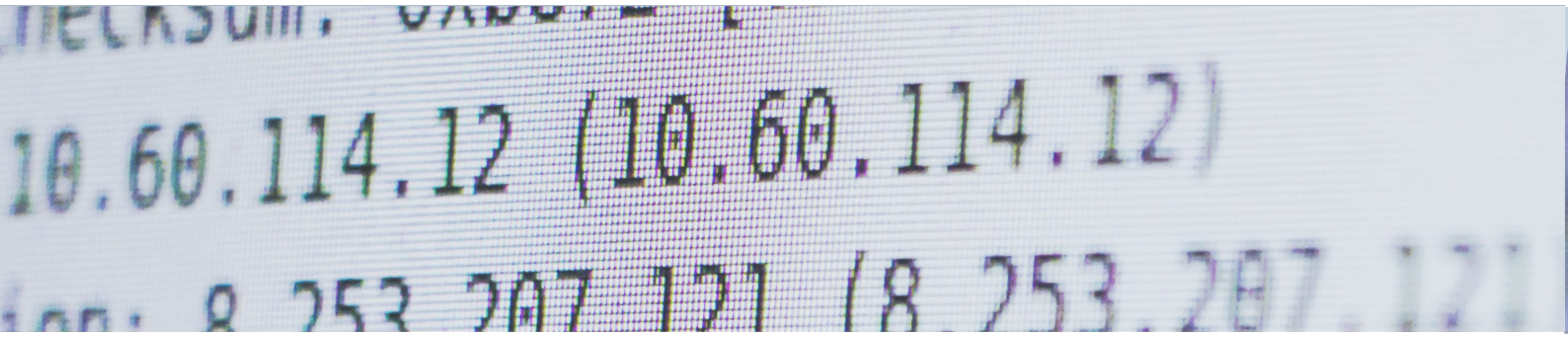
Erneut kam es in der Region in den Abendstunden an einer Tankstelle zu einem bewaffneten Raubüberfall. Das Vorgehen des Täters gleicht einer Vielzahl vorangegangener Taten. Die Ermittler gehen von einer Tatserie aus. Konkrete Täterhinweise liegen nicht vor. Jedoch führen zahlreiche Zeugenvernehmungen und die Auswertung von Videoaufzeichnungen zu einer Täterhypothese.

DIE TÄTERHYPOTHESE:

AUSGANGSLAGE FÜR DIE DATENANALYSE

Die Auswertung der verschiedenen Ermittlungs- und Untersuchungsergebnisse bieten eine wichtige Grundlage für die Entwicklung einer Tat-/Täter-Hypothese. Wie kann der Täter unter Berücksichtigung aller bisher bekannten Informationen beschrieben werden – welcher Umgebung kann er möglicherweise zugeordnet werden? Die Ermittler kommen zu folgender Täterhypothese:

- Männlich; dunkle, kurze Haare, schlanke Statur.
- Circa 25 bis 35 Jahre.
- Circa 180 cm groß.
- Vermutlich deutsch (gemäß Aussehen und schwäbischem Akzent).
- Der Täter drohte mit einer Schusswaffe, die anhand von Videoaufzeichnungen einem Hersteller und Typ zugeordnet werden kann.
- Die Mitarbeiter des Arbeitsbereiches Multimediaforensik des LKA konnten in gesicherten Videoaufzeichnungen, an einer vom Täter getragenen Jacke, ein Firmenlogo identifizieren. Dieses Logo gehört zu einem örtlichen Großunternehmen. Die Jacke wurde in drei Fällen getragen.
- In einem Fall wurden im Rahmen der Flucht im erweiterten Außenbereich der Tankstelle Videoaufzeichnungen gesichert. Die Aufzeichnungen zeigen, wie der Täter mit einem roten Klein-Pkw flüchtete – der Pkw-Hersteller und -Typ waren erkennbar. Das Kennzeichen wurde vom Täter abgedeckt, jedoch nicht vollständig. Die Buchstaben des Zulassungskreises waren sichtbar, aber auf Grund Unschärfe nicht lesbar. Durch die speziellen Untersuchungsmethoden der Multimediaforensik konnte der Zulassungskreis identifiziert werden.



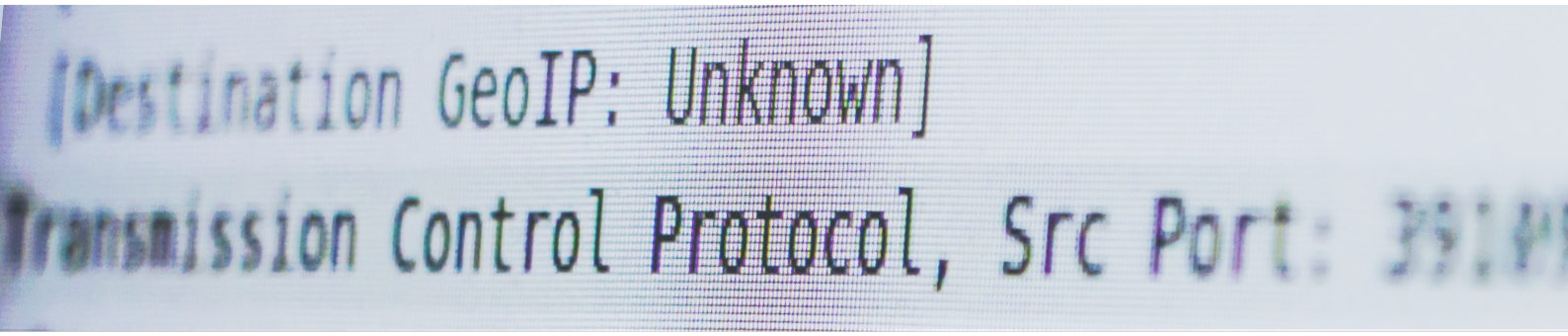
DER ANALYSEANSATZ – WELCHE DATEN WERDEN ERHOBEN UND WONACH WIRD GESUCHT?

In Abstimmung zwischen Ermittlern und den Sachbearbeitern Datenanalyse wird ein Konzept erarbeitet, wie anhand der beschriebenen Erkenntnislage eine Analyse der Daten durchgeführt werden kann. Danach beschließen die Ermittler folgende Datenerhebungen durchzuführen:

- Recherche in den polizeilichen Auskunftsdateien zu allen männlichen Personen, die in den vergangenen fünf Jahren in der erweiterten räumlichen Umgebung einen bewaffneten Raub mit der festgestellten Vorgehensweise begangen haben. Als weitere Eingrenzungskriterien werden die Merkmale der Personenbeschreibung verwendet. Die gefilterten Personendaten werden in einer Datentabelle bereitgestellt.
- Feststellung aller Inhaber der identifizierten Schusswaffe bei der örtlichen Waffenbehörde. Die Personendaten werden in einer Datentabelle bereitgestellt.
- Zum identifizierten Pkw-Hersteller und Typ (einschließlich Farbe) werden zum betreffenden Zulassungskreis Halterdaten erhoben. Die Personendaten werden in einer Datentabelle bereitgestellt.

Die erhobenen Daten werden der zuständigen Analysestelle zugeleitet und sollen durch die Sachbearbeiter Datenanalyse zusammengeführt und auf Schnittmengen untersucht werden. Die Frage lautet konkret:

GIBT ES IDENTISCHE PERSONENDATEN, DIE IN DEN VERSCHIEDENEN DATENBESTÄNDEN VORKOMMEN?



BEARBEITUNGSGRUNDSÄTZE

Zunächst gilt es, die Personendaten für den beabsichtigten Abgleich aufzubereiten. Die Daten müssen in ein für die Untersuchung einheitliches Format gebracht werden. Es ist auch zu berücksichtigen, dass nicht jede Stelle, von der Daten eingeholt werden, ihre Daten nach einem einheitlichen Standard erfasst. Die Erfassungsqualität ist bedeutsam und variiert erfahrungsgemäß sehr stark.

Um die Daten einer belastbaren Schnittmengenuntersuchung zuzuführen, ist von der Analysestelle ein Qualitätsniveau zu definieren. Sämtliche Datenbestände sind diesem Niveau anzupassen. Hierfür werden teilweise komplexe Regeln festgelegt. Beispielsweise müssen zu einem Familiennamen die vielfältigen Möglichkeiten einer fehlerhaften Schreibweise einbezogen werden. Hier sei beispielhaft der Familienname Schmidt angeführt, dessen Schreibeweise für die Datenerfassung ein hohes Fehlerpotential enthält (beispielsweise Schmid und Schmitt).

Erst wenn die qualitätsgeprüfte einheitliche Datenebene hergestellt wurde, wird der entscheidende Abgleich, nach fest definierten Regeln durchgeführt. Dieser Aufbereitungs- und Analyseprozess unterliegt einer sorgfältigen Dokumentationspflicht. Im Nachgang muss im Detail nachvollziehbar sein, wie die Daten verarbeitet wurden.

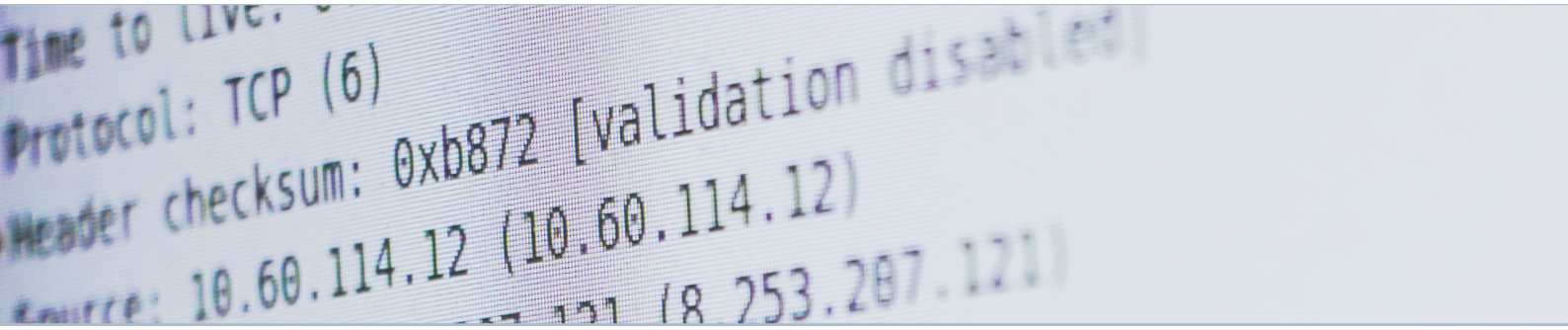
DAS ANALYSEERGEBNIS – DER ANSATZ FÜR WEITERE TÄTERORIENTIERTE ERMITTLUNGEN

Den Datenanalysten gelingt es, aus der großen Anzahl an Datensätzen wenige Personen herauszufiltern, die in den verschiedenen Datenbeständen erfasst sind. Der Analysebericht, der die gesamten Aufbereitungsschritte und das erzielte Ergebnis beinhaltet, wird den Ermittlern zugeleitet.

WEITERE ERMITTLUNGSMASSNAHMEN WERDEN EINGELEITET

Auf Grundlage der Analyseergebnisse und weiterführenden Ermittlungen konkretisiert sich ein Tatverdacht. Von den ermittelnden Beamten werden weitere gezielte Ermittlungsmaßnahmen gegen den identifizierten Tatverdächtigen eingeleitet. Dazu gehört auch, auf richterlichen Beschluss die Telekommunikationsverbindungsdaten gemäß § 100g Strafprozessordnung (StPO) zu erheben, die in Zusammenhang mit dessen Mobilfunkgerät in der Vergangenheit entstanden sind.

Die Aufbereitung und Analyse von Telekommunikationsverkehrsdaten liegt ebenfalls im Tätigkeitsbereich der Datenanalyse. Auch bei diesem Ansatz geht es unter anderem um die Erkennung von Schnittmengen.



WIE HAT SICH DIE DATENANALYSE IM JAHRESVERGLEICH ENTWICKELT?

Der dargestellte fiktive Fall entspricht grundsätzlich den Realbedingungen und gibt nur einen thematischen Teilbereich der Arbeit des Sachbearbeiters Datenanalyse wieder. Es sollen anhand des Beispiels die wesentlichen Prozessschritte im Rahmen einer Datenanalyse abgebildet werden. Die Aufgaben der Datenanalysten beziehen sich neben der Verarbeitung von Personendaten zudem auf weitere analysefähige Datenfelder, wie zum Beispiel Telekommunikationsverkehrsdaten, Kraftfahrzeugdaten oder georeferenzierte Informationen, die im Rahmen von Ermittlungsverfahren zu untersuchen sind.

Die aufgeführten Kerndaten beziehen sich auf alle bearbeiteten Datentypen. Die regionalen Analysestellen, die den zwölf örtlichen Kriminalpolizeidirektionen angegliedert sind und die zentrale Analysestelle beim Landeskriminalamt wurden am 1. Januar 2014 neu eingerichtet. Das erste Jahr galt vornehmlich dem strukturellen Aufbau. Die Disziplin der Datenanalyse in den dezentralen Analysestellen der Regionalpräsidien ist, wie oben dargestellt, erst wenige Jahre präsent, sodass keine weiteren vergleichbaren Daten vorliegen. Es ist dennoch festzustellen, dass unter Bezugnahme auf die Kennzahlen 2015 im vergangenen Jahr in den landesweit begleiteten Ermittlungskomplexen (Vorgänge) die Anzahl der bearbeiteten Fälle um 23 Prozent angestiegen ist. Ein Anstieg dieser Größenordnung lässt auch bei der verfügbaren knappen Datenbasis darauf schließen, dass die Serviceleistungen der Analysestellen zunehmend in Anspruch genommen werden. Dies ist maßgeblich in erfolgreichen Unterstützungsleistungen für die Ermittlungseinheiten begründet.

	2015	2016	Tendenz
Vorgänge	2.090	2.116	↗
Fälle	5.151	6.351	↗

Die Begriffe erklären sich wie folgt:

	Beschreibung
Vorgänge	Anzahl der Ermittlungskomplexe, die von den Analysestellen unterstützt wurden
Fälle	Anzahl der Einzelfälle, die innerhalb der Ermittlungskomplexe bearbeitet wurden. Einzelfälle sind die eigentlichen „Datenpools“ die aufbereitet und untersucht werden. Das können z.B. TK-Verbindungsdatenbestände, Personendatenbestände, Kraftfahrzeugdatenbestände, georeferenzierte Datenbestände sein

4 TELEKOMMUNIKATIONSÜBERWACHUNG (TKÜ)

Telekommunikationsüberwachung liefert auch unter zunehmend schwierigeren Rahmenbedingungen weiterhin unverzichtbare Ermittlungsansätze. Übertragungsgeschwindigkeiten, Bandbreiten und Datenmengen nehmen stark zu. Darüber hinaus zeichnet sich eine zunehmende Verschlüsselung der Kommunikationsinhalte, technisch bedingte oder absichtlich erzeugte Anonymisierung von Teilnehmeranschlüssen, Internationalisierung und die Einführung neuer technischer Standards ab. Herkömmliche Kommunikations- und Telemediendienste verschmelzen miteinander und führen zu einer steigenden Anzahl von Kommunikations- und vielfältigen Nutzungsmöglichkeiten. Die Nutzerzahlen von interaktiven Informations- und Kommunikationsplattformen sowie mobilen Endgeräten wachsen rasant. Die Anforderungen an eine moderne Telekommunikationsüberwachung haben sich in den letzten Jahren drastisch verändert.

Bis vor einigen Jahren wurde fernmündlich ausschließlich „über den Draht“ kommuniziert. Durch Vorlage eines richterlichen Beschlusses konnten berechtigte Stellen auf diese Inhalte mittels einer Providerausleitung zugreifen. Durch die mittlerweile vollzogene Digitalisierung der Telekommunikation wurde es jedoch für den Endbenutzer sehr einfach und kostenneutral möglich, sämtliche digitalen Kommunikationsvorgänge zu verschlüsseln.

Die Nutzung moderner Verschlüsselungstechnik setzt dabei keine weitergehenden technischen Fertigkeiten voraus. Durch diese Entwicklung wird die klassische Telekommunikationsüberwachung erheblich erschwert oder sogar unmöglich gemacht. Eine auch weiterhin erfolgsversprechende Überwachung der Telekommunikation bedarf der Entwicklung geeigneter technischer Ausgleichsmaßnahmen seitens der Sicherheitsbehörden. Aus diesem Grund wurde beim LKA ein Projekt für künftige TKÜ-Maßnahmen eingerichtet.

KONVENTIONELLE TKÜ

Die landesweite TKÜ-Zentrale setzt Beschlüsse nach den Paragraphen 100a StPO (Telekommunikationsüberwachung) i.V.m. 100b StPO (Verfahren bei der Telekommunikationsüberwachung) und Verkehrsdatenanfragen nach § 100g StPO beziehungsweise § 23a Polizeigesetz (PolG BW) um. Verkehrsdaten sind beispielsweise Datum, Uhrzeit und Nummer eines beteiligten Telefonanschlusses oder bei mobilen Anschlüssen die Standortdaten der genutzten Funkzelle. Lediglich die technische Umsetzung wird hierbei im Landeskriminalamt realisiert. Die Inhalte werden im Folgenden landesweit an den jeweiligen Sachbearbeiter beziehungsweise an polizeiliche Datenanalysten ausgeleitet. Kernstück der technischen Plattform für die Telekommunikationsüberwachung ist die leistungsfähige TKÜ-Anlage. Statistische Daten zu Maßnahmen nach §§ 100a und 100g StPO sind über das Bundesamt für Justiz im Internet abrufbar.[2]

Neben den oben genannten technischen Unterstützungen beraten die Mitarbeiterinnen und Mitarbeiter des LKA Polizeibeamte des Landes und Angehörige der Justiz bei Maßnahmen beziehungsweise Sonderlagen mit TKÜ-Bezug zu Themen wie Festnetz, Mobilfunk, und digitaler Telefonie/Voice over IP (VoIP). Standortfeststellungen von mobilen Endgeräten werden im Bedarfsfall ebenfalls durchgeführt.

Beispielsweise kann bei einer suizidgefährdeten Person der Funkmast festgestellt werden, in welchen ein Mobiltelefon eingebucht ist. Zur Sicherstellung einer 24/7-Erreichbarkeit ist außerhalb der Kernarbeitszeit ein Bereitschaftsdienst verfügbar. Um die oben genannten Maßnahmen durchzuführen, sorgen die Mitarbeiterinnen und Mitarbeiter der TKÜ-Technik für die nötigen Hard- und Softwarekomponenten.

AUS- UND FORTBILDUNGSANGEBOTE

Das Feld der Telekommunikation unterliegt einem ständigen Wandel, der auch Auswirkungen auf die Hard- und Software der TKÜ-Anlage und somit auf die Arbeit der Ermittler hat. Das TKÜ-Zentrum bietet daher unter dem Motto „aus der Praxis für die Praxis“ Aus- und Fortbildungsveranstaltungen für Ermittler, die Justiz und andere Bedarfsträger an. Im Jahr 2016 wurden insgesamt 56 Veranstaltungen durchgeführt.

2 https://www.bundesjustizamt.de/DE/Themen/Buergerdienste/Justizstatistik/Telekommunikation/Telekommunikationsueberwachung.html

OPERATIVE IT/ NETZWERKFORENSIK

Die Polizeivollzugsbeamten und IT-Spezialisten des Arbeitsbereichs Operative IT/Netzwerkforensik (OIT) unterstützen landesweit im Bereich IT-bezogener Ermittlungen. Neben individuellen Beratungen in Ermittlungsverfahren und Einsatzlagen jeglicher Art werden auf den konkreten Einzelfall abgestimmte besondere technische Maßnahmen entwickelt und umgesetzt. Im Jahr 2016 wurden die Dienstleistungen der OIT in über einhundert Fallkonstellationen in Anspruch genommen. Schwerpunkte waren die Identifizierung und Lokalisierung von Beschuldigten über das Internet, die Überwachung von Internet-Servern und die Sonderauswertung von TKÜ-Maßnahmen.

Im Jahr 2016 traten verstärkt die Phänomene Ransomware und CEO-Fraud mit einer Vielzahl von Unterstützungsanfragen zu Tage. Die beiden Delikte werden an späterer Stelle näher erläutert. Aufgrund ihrer langjährigen Erfahrung und dem kontinuierlichen professionellen Ausbau der technischen Infrastruktur war die OIT auch 2016 ein gefragter Ansprechpartner bei anderen Behörden auf Bundesebene und in anderen Bundesländern. In mehreren Fällen wurde technische Amtshilfe bei der Realisierung besonderer Maßnahmen gewährt.

MOBILFUNKAUFKLÄRUNG (MFA)

Zentrales Einsatzmittel der Mobilfunkaufklärung stellt der IMSI-Catcher dar. Dabei handelt es sich um ein Messsystem welches die IMSI (International Mobile Subscriber Identity) von Mobilfunkgeräten – dient der Identifikation von Netzteilnehmern – abfragen und den Standort eines eingeschalteten mobilen Endgerätes bestimmen kann.

Neben weiterer Messtechnik zur Funkzellenbestimmung hält der Arbeitsbereich MFA auch WLAN-Catcher bereit, die über WLAN geführte Kommunikation, einschließlich der anfallenden verbindungsbegleitenden Daten erfasst. IMSI-Catcher dienen unter anderem dazu, unbekannte Mobilfunkgeräte zu identifizieren oder den Standort von mobilen Endgeräten festzustellen, die beispielsweise von verunglückten Personen mitgeführt werden.

Der Arbeitsbereich Mobilfunkaufklärung führt IMSI-Catcher-, WLAN-Catcher-Einsätze sowie Funkzellenbestimmungen und -vermessungen (gem. § 23a Polizeigesetz BW oder § 100i beziehungsweise § 100a StPO) durch. Mit der Funkzellenbestimmung wird die Abfrage einer Funkzelle gemäß § 100g StPO vorbereitet. Die Funkzellvermessung dient der Bestimmung des konkreten Ausmaßes einer Funkzelle, insbesondere zur Alibiüberprüfung und für gutachterliche Aussagen vor Gericht.

EINE TYPISCHE FALLGESTALTUNG

In einer Funkleitzentrale geht ein Notruf einer zunächst unbekannten Frau ein: „Hallo mein Name ist Müller (Name und Örtlichkeit geändert). Wir sind in Radolfzell irgendwo. Mein Mann war früher ein Nazi und wir werden in letzter Zeit verfolgt. Ich weiß nicht wo wir sind, Friedhof irgendwo, sie kommen, ich muss auflegen."

Erste Ermittlungen lassen darauf schließen, dass es sich tatsächlich um eine bedrohliche Situation handeln könnte. Sofort wird mit der Suche im Bereich Radolfzell begonnen. Diese verläuft erfolglos. Am Abend des gleichen Tages meldete die Schwester der Anruferin diese als vermisst. Frau Müller hätte ihr dreijähriges Kind bei der Großmutter gegen 18 Uhr abholen sollen, war aber nicht erschienen. Ein solches Verhalten sei für sie völlig ungewöhnlich. Die Familie machte sich daher ernsthaft Sorgen. Die mitgeführten Handys von Frau und Herrn Müller waren aktiv, jedoch konnte bei Anrufversuchen niemand erreicht werden. Erste Standortbestimmungen, die von dem örtlichen Polizeipräsidium veranlasst wurden, ergaben einen Suchbereich mit einem Radius von circa 15 Kilometern. Fahndungsmaßnahmen durch die örtliche Dienststelle verliefen erneut negativ.

Neben den eingeleiteten örtlichen Suchmaßnahmen alarmierte die Funkleitzentrale auch die Mobilfunkaufklärung des LKA. Durch deren Unterstützung konnten im Bereich des Friedhofs die beiden gesuchten Mobiltelefone und persönliche, teilweise blutverschmierte Gegenstände der gesuchten Personen aufgefunden werden. Aufgrund der Spurenlage wurde von einem Kapitaldelikt ausgegangen. Die Kriminalpolizei richtete eine Sonderkommission ein. Im Rahmen der weiteren Ermittlungen ergab sich der Verdacht, dass die Straftat nur vorgetäuscht sein könnte. Dieser Verdacht bestätigte sich wenige Wochen später, nachdem die spanische Polizei Frau und Herrn Müller angetroffen hatte und diese festnehmen konnte.

Im Zusammenhang mit suizidgefährdeten und vermissten Personen wurden die Fachkräfte des Arbeitsbereichs Mobilfunkaufklärung im Jahr 2016 insgesamt 55 Mal angefordert (2015: 34 Mal). Darüber hinaus wurden in 1.067 Fällen Funkzellenbestimmungen durchgeführt. Seit April 2015 leisten die Mitarbeiter der Mobilfunkaufklärung einen 24/7 Bereitschaftsdienst, um bei Gefahr für Leib oder Leben auch außerhalb der regulären Dienstzeiten ihre Einsatzfähigkeit zu gewährleisten. Da derartige Einsatzlagen stetig zunehmen, wurde der Arbeitsbereich personell aufgestockt.

5 ZENTRALE ANSPRECHSTELLE CYBERCRIME

Die Zentrale Ansprechstelle Cybercrime (ZAC) dient als Single Point of Contact für Wirtschaftsunternehmen, Behörden sowie Forschungseinrichtungen in allen Belangen des Themenfeldes Cybercrime. Die Mitarbeiterinnen und Mitarbeiter der ZAC nehmen in diesem Zusammenhang eine Vermittler- und Beraterrolle wahr. Im Jahr 2016 nahmen die Kontaktaufnahmen der Zielgruppe im Vergleich zum Vorjahr deutlich zu. Insgesamt gingen 620 Hinweise und Anfragen bei der ZAC ein (2015: 481).

Die Mitarbeiterinnen und Mitarbeiter der Ansprechstelle können auf ein bundesweites Netzwerk von ZAC-Dienststellen, die beim Bundeskriminalamt und den Landeskriminalämtern eingerichtet sind, zurückgreifen. Um einen bundesweiten Wissenstransfer sicherzustellen, finden regelmäßige Treffen im ZAC-Verbund statt. Dem Wunsch kleiner und mittelständischer Unternehmen (KMU) nach Präventionsaktivitäten kam die ZAC im Jahr 2016 in Form von zahlreichen Awarenessvorträgen nach. In der Regel wurden Veranstaltungen in Zusammenarbeit mit Unternehmensverbänden durchgeführt. Hierbei wurden aktuelle Gefahren im Cyberraum aufgezeigt und konkrete Handlungsempfehlungen genannt. Aufgrund von zwei Personalabgängen in der zweiten Jahreshälfte mussten die Vortragstätigkeiten reduziert werden. Die ZAC wird im Frühjahr 2017 durch weiteres Personal verstärkt.

Zu herausragenden Kriminalitätsphänomenen veröffentlichte die ZAC anlassbezogen Warnmeldungen, welche sowohl über die Industrie- und Handelskammern den 650.000 zugehörigen Unternehmen in Baden-Württemberg sowie über andere Kooperationspartner, wie beispielsweise Unternehmensverbände, als auch über die Internetseite der ZAC zur Verfügung gestellt wurden.

Auch polizeiintern übernimmt die ZAC zunehmend eine Vermittlerrolle. Bei Cybercrime-Ermittlungen oder bei der Sicherung beziehungsweise Auswertung von digitalen Spuren werden Ermittler häufig mit Fragestellungen konfrontiert, welche nur die Fachinspektionen beantworten können. Die ZAC ist beim LKA in der Führungsgruppe der Abteilung Cybercrime und Digitale Spuren angesiedelt. Diese gleichnamigen Themen werden von der Abteilung landesweit koordiniert und einheitlich umgesetzt. Daher sind die Mitarbeiterrinnen und Mitarbeiter der ZAC mit sämtlichen polizeilichen Einrichtungen, die sich mit digitalen Themen beschäftigen, vernetzt.

Im Jahr 2016 meldeten sich zahlreiche Institutionen bei der ZAC, da sie Opfer einer sogenannten Ransomware wurden. Als Ransomware werden Schadprogramme bezeichnet, die den Zugriff auf Daten und Systeme einschränken oder verhindern und diese Ressourcen nur gegen Zahlung eines Lösegeldes wieder freigeben.

Wie auch im Jahr zuvor wurden diverse Methoden genutzt, um Rechner mit der Schadsoftware zu infizieren. Häufig wurden an Personalabteilungen vermeintliche Bewerbungen per E-Mail übersandt. Beim Öffnen der Bewerbungsmappe wurde jedoch kein Lebenslauf dargestellt, stattdessen wurden Dateien auf dem betroffenen Rechner und unter Umständen die mit dem Client verbundenen Netzlaufwerke verschlüsselt.

Zur Entschlüsselung wurde eine Zahlung in Form von Bitcoins[3] erpresserisch gefordert. Um die Wahrscheinlichkeit zu erhöhen, dass durch den Angeschriebenen die beigefügte Datei mit der Schadsoftware ausgeführt wird, wurde der Bewerbungstext häufig auf tatsächlich veröffentlichte Stellenanzeigen angepasst.

Ein weiteres Kriminalitätsphänomen, das sehr häufig zur Anzeige gebracht wurde ist bekannt unter dem Begriff CEO-Fraud beziehungsweise Fake President. Es handelt sich um eine Betrugsmasche, bei der meist Mitarbeiter der Finanzabteilung vom vermeintlichen Vorgesetzten oder Geschäftsführer per E-Mail angeschrieben werden, um eine Finanztransaktion durchzuführen.

Häufig wird als Grund eine streng vertrauliche Firmenübernahme im Ausland vorgegeben. Tatsächlich stammt die Mail jedoch nicht von der Geschäftsführung sondern vom Täter. Nicht selten wurde so eine Zahlung in sechsstelliger Höhe auf fernöstliche Konten getätigt.

Eine Rückbuchung gezahlter Beträge ist dann meist nicht oder nur erschwert möglich. Durch diverse Präventions- und Awarenesskampagnen unterstützte das LKA im Berichtszeitraum zahlreiche Firmen bei der Mitarbeitersensibilisierung im Hinblick auf die Gefahren im Cyberraum. Die Maßnahmen trugen dazu bei, dass eine Vielzahl betrügerischer Mails bereits zu einem frühen Zeitpunkt von betroffenen Firmen erkannt wurden. Für die zum Teil kleinen und mittelständischen Unternehmen aus der Region sind die beiden oben genannten Kriminalitätsphänomene nicht selten existenzgefährdend.

3 Bitcoin ist eine digitale Währung.
Der Wert eines Bitcoin lag im Dezember 2016 bei circa 900 Euro.

KOOPERATIONEN

Die rasante Entwicklung der IT und die damit verbundenen neuen Möglichkeiten für Straftäter, diese Technologie einzusetzen, machen es stärker als in anderen Kriminalitätsfeldern erforderlich, mit Unternehmen und Unternehmensverbänden der IT-Branche, aber auch mit Forschung und Lehre Kooperationen einzugehen. Die Geschäftsführungen dieser Kooperationen sind in der ZAC angesiedelt. Im Folgenden werden exemplarisch drei elementare Kooperationen dargestellt. Kerngedanken der Mitgliedschaften in Kooperationen und Allianzen sind unter anderem:

- die Förderung des stetigen Erfahrungsaustausches
- die Aufhellung des Dunkelfeldes
- die Durchführung von gemeinsamen Aktionen zum Beispiel im Bereich der Aus- und Fortbildung oder der Prävention und
- die gegenseitige Unterstützung bei Problemstellungen oder bei konkreten Ermittlungsverfahren der Polizei.

SICHERHEITSKOOPERATION CYBERCRIME

Hervorzuheben ist die Sicherheitskooperation Cybercrime, welcher das LKA im Jahr 2013 beigetreten ist. Zusammen mit dem Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) und den Landeskriminalämtern Niedersachsen, NordrheinWestfalen, Sachsen und Hessen ist zwischen Polizei und IT-Unternehmen ein Netzwerk entstanden, welches die Grundlage zur Intensivierung eines erfolgreichen Wissenstransfers bildet.

Im Rahmen verschiedener Ermittlungsverfahren waren die Kontakte zu den Partnern der Sicherheitskooperation Cybercrime bereits hilfreich. Die Kontaktaufnahme erfolgte hierbei über die ZAC. Als Ergebnisse konnten bislang unter anderem die Entwicklung von Ermittlungstools, die Optimierung des Anzeigeverhaltens sowie zielgerichtete Hospitationen mit ausgewählten Partnern erreicht werden. Cybersicherheitsstrategien müssen zudem über Landesgrenzen hinweg gedacht und von den vielen Akteuren im Bereich der Cybercrime-Bekämpfung gemeinsam entwickelt werden. Die Vertreter der Sicherheitskooperation Cybercrime waren daher im März 2016 auf der CeBIT in Hannover, der weltweit größten Messe für Informationstechnik, als Aussteller vertreten.

Zudem war die Sicherheitskooperation Cybercrime erstmalig bei der GPEC 2016 (Fachmesse für Polizei- und Spezialausrüstung) in Leipzig mit einem Informationsstand vertreten. Im September 2016 fand die jährliche Veranstaltung der Sicherheitskooperation Cybercrime in Dresden statt. Neben den Bestrebungen der Sicherheitskooperation Cybercrime, eine globale Vernetzung sicherzustellen, werden durch die ZAC weitere Kooperationen mit teils internationalen Bezügen betreut.

ALLIANZ FÜR CYBERSICHERHEIT

Die Allianz für Cyber-Sicherheit ist eine Initiative des Bundesamtes für Sicherheit in der Informationstechnik (BSI), die im Jahr 2012 gegründet wurde. Die Allianz hat sich das Ziel gesetzt, die Cyber-Sicherheit in Deutschland zu stärken. Dazu stellt die Initiative ein umfangreiches Informationsangebot für die Wirtschaft und andere professionelle Bedarfsträger wie Behörden sowie für Forschung und Wissenschaft zur Verfügung. Ein weiterer wesentlicher Bestandteil der Arbeit der Initiative ist die Förderung des Erfahrungsaustausches unter den Teilnehmern. Derzeit beteiligen sich 2062 teilnehmende Institutionen (2015: 1.553), über 96 aktive Partner und mehr als 45 Multiplikatoren an der Allianz (Stand: Januar 2017). Das Landeskriminalamt Baden-Württemberg fungiert als Multiplikator und erhält so ausführliche Informationen zu aktuellen Cyber-Bedrohungen, die an die jeweiligen Bedarfsträger weitergegeben werden.

HOCHSCHULE ALBSTADT-SIGMARINGEN

Die Hochschule Albstadt-Sigmaringen (HSAS) bietet zusammen mit der Goethe-Universität Frankfurt und der Friedrich-Alexander-Universität Erlangen-Nürnberg seit dem Jahr 2010 den Masterstudiengang Digitale Forensik an. Bereits mehrere hochmotivierte Angehörige des LKA haben das Studienangebot in der Freizeit in Anspruch genommen und sich, ohne dass hierfür von Seiten des Landes eine Kostenerstattung erfolgen konnte, weitergebildet. Neben dem Masterstudiengang wurden mittlerweile auch zahlreiche Zertifikatsmodule, welche die HSAS im Rahmen des Open C³S Programmes zusammen mit fünf weiteren Hochschulen anbietet, durch Beamte absolviert.

Zum Teil finden sich die Studienmodule zu Themen wie Sicherheit, Forensik, Kryptologie, Recht oder praktische Informatik auch im Curriculum des Masterstudiengangs Digitale Forensik wieder. Durch Vertreter der Polizei Baden-Württemberg im Fachbeirat der Hochschule Albstadt-Sigmaringen wird sichergestellt, dass die Studieninhalte auch auf die Belange der Sicherheitsbehörden angepasst werden. Im September 2016 fand in Frankfurt am Main die letzte Sitzung statt. Zudem war das Landeskriminalamt Baden-Württemberg zusammen mit Kollegen von der örtlichen Polizei, wie bereits in den Vorjahren, beim Tag der Technik an der Hochschule Albstadt-Sigmaringen mit einem Informationsstand vertreten.

DER MASTERSTUDIENGANG DIGITALE FORENSIK

- **Vermittlung von umfassendem technischen IT-Wissen, detailliertem Know-how über Computer, Betriebssysteme und Netzwerke.**
- **Genaue Methodenkenntnis der Digitalen Forensik inklusive spezifischer Vorgehensweisen bei der Identifikation, Sicherung und Analyse aller Arten digitaler Beweismittel.**
- **Juristische Grundlagen, sodass später in der Berufspraxis die möglichen rechtlichen Konsequenzen des Handelns bewusst sind.**
- **Die Regelstudienzeit beträgt sieben Semester in Teilzeit, in der sich regelmäßig Online-Selbstlernphasen und Präsenzphasen abwechseln.**

DAS ZERTIFIKATSPROGRAMM OPEN C³S

- **Wissenschaftliche Weiterbildung im Bereich Cyber-Sicherheit.**
- **Zahlreiche in sich abgeschlossene Studienmodule zu den Themenschwerpunkten Sicherheit, Forensik, Kryptographie, Recht und praktische Informatik.**
- **Mehrere spezifische Zertifikatsmodule aus dem Zertifikatsprogramm können zu einem Zertifikatsstudium kumuliert werden: Zum Beispiel Datenträgerforensiker oder Netzwerkforensiker.**
- **Die Studiendauer beträgt circa acht Wochen pro Modul.**

IMPRESSUM

JAHRESBERICHT 2016

CYBERKRIMINALITÄT UND DIGITALE SPUREN

HERAUSGEBER

Landeskriminalamt Baden-Württemberg
Taubenheimstraße 85
70372 Stuttgart

Telefon 0711 5401-0
Fax 0711 5401-3355
E-Mail Stuttgart.lka@polizei.bwl.de

ANSPRECHPARTNER

ANSPRECHSTELLE FÜR FACHFRAGEN

ZENTRALE ANSPRECHSTELLE CYBERCRIME

Jürgen Fauth
Telefon 0711 5401-2444
E-Mail cybercrime@polizei.bwl.de

ERMITTLUNGEN/AUSWERTUNG CYBERCRIME

INSPEKTION 510

Frank Winterhalter
Telefon 0711 5401-2510
E-Mail stuttgart.lka.abt5.i510@polizei.bwl.de

IT-BEWEISSICHERUNG /

ANALYSE STRUKTURIERTER MASSENDATEN

INSPEKTION 520

Martin Lühning
Telefon 0711 5401-2520
E-Mail stuttgart.lka.abt5.i520@polizei.bwl.de

TKÜ-ZENTRUM

INSPEKTION 530

Claus-Dieter Schiemann
Telefon 0711 5401-2530
E-Mail stuttgart.lka.abt5.i530@polizei.bwl.de

DAS LANDESKRIMINALAMT BADEN-WÜRTTEMBERG