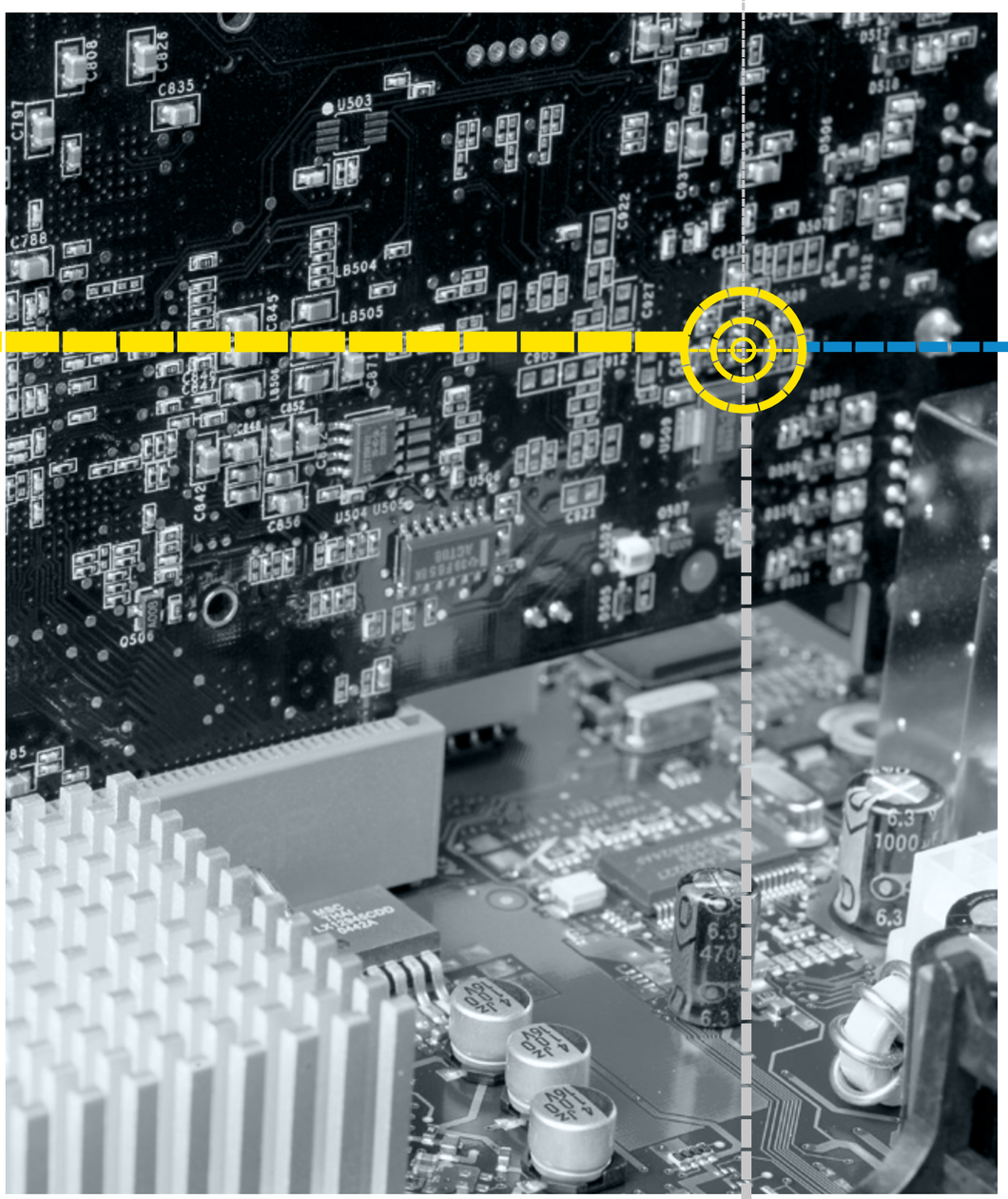
CYBERCRIME / DIGITALE SPUREN

JAHRESBERICHT 2015

LANDESKRIMINALAMT BADEN-WÜRTTEMBERG



LKA BW

Und wieder kam es zu einem Wohnungseinbruch in den frühen Abendstunden. Der Wert des Diebesgutes ist beträchtlich. Es verdichten sich die Hinweise, dass es sich um eine Tatserie handelt. Zeugen wollen beobachtet haben, wie eine unbekannte verdächtige Person das Gebäude über ein Fenster an der Gebäuderückseite telefonierend verließ.

Ein Fall für die Datenanalyse.

TENDENZEN

	2014	2015	IN %	
GESAMT	**21.898**	**22.133**	**+ 1,1**	→
COMPUTERKRIMINALITÄT	7.941	6.547	- 17,6	↘
INTERNETKRIMINALITÄT	17.949	18.676	+ 4,1	↗
GESAMTBEREICH KINDERPORNOGRAFIE				
KINDERPORNOGRAFISCHE SCHRIFTEN	578	599	+ 3,6	→
VERFAHRENSINITIIERUNGEN AIR	731	921	+ 26,0	↗
NEUE AUFTRÄGE ITB	10.339	10.071	- 2,6	→

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

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.

CYBERCRIME / DIGITALE SPUREN

JAHRESBERICHT 2015

1

13.550 initiierte Strafverfahren in Zusammenhang mit der Verbreitung von Kinderpornografie durch den Arbeitsbereich Internetrecherche

2.437.326 angelieferte Bilder bei der Ansprechstelle Kinderpornografie

13.450.079 Euro Schaden durch Internetkriminalität

141.231 angelieferte Videos bei der Ansprechstelle Kinderpornografie

fotolia.com

ANALYSE

NEUE TECHNOLOGIEN: FLUCH UND SEGEN

Auch im Jahr 2015 schreitet der digitale Wandel weiter voran. Mittlerweile sind nach einer Studie von ARD und ZDF mehr als die Hälfte der Bundesbürger ab 14 Jahren auch mobil im World Wide Web unterwegs.[1] Das Smartphone übernimmt hierbei eine zentrale Rolle. Doch nicht nur der unbescholtene Bürger nutzt die aktuellsten Technologien, auch die Täter wissen die neuen Möglichkeiten für ihre kriminellen Machenschaften einzusetzen.

Leitender Kriminaldirektor Reinhard Tencz, Leiter der Abteilung Cybercrime/Digitale Spuren beim LKA BW, Quelle LKA BW, C. Rottler

Für die Polizei sind die Geräte Fluch und Segen zugleich. Einerseits liefern sie Ermittlungsansätze, die es so vor einigen Jahren noch nicht gegeben hat, andererseits müssen sämtliche Daten von Gerätschaften eines Beschuldigten, die belastende, aber auch entlastende Hinweise liefern könnten, gerichtsverwertbar gesichert, aufbereitet und die Inhalte bewertet werden.

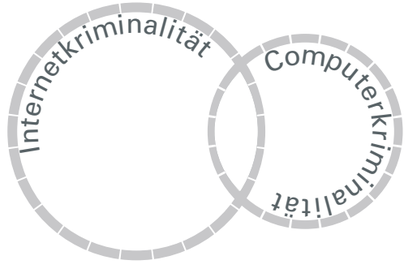
Neben den immer größeren Datenmengen werden auch die Ermittlungen im Cyberraum zunehmend komplexer. Da die virtuelle Welt keine Landesgrenzen kennt, ist die Überführung von Tätern häufig nur in Zusammenarbeit mit ausländischen Strafverfolgungsbehörden möglich. Die organisatorischen Veränderungen der Polizei des Landes tragen bei der Bekämpfung des Kriminalitätsfeldes Cybercrime und im Umgang mit digitalen Spuren erste Früchte. Die spezialisierte Abteilung beim Landeskriminalamt Baden-Württemberg (LKA BW), die Kriminalinspektionen Cybercrime/Digitale Spuren bei den Polizeipräsidien und ebenso der Institutsbereich Cybercrime/Digitale Spuren an der Hochschule für Polizei Baden-Württemberg (HfPol BW) haben sich bereits in der ersten Phase bewährt. Zunehmend entwickelt sich im Land ein Netzwerk hoch spezialisierter Mitarbeiter, das Bürgern und Unternehmen gleichermaßen für die Bekämpfung von Cybercrime zur Verfügung steht. Diese Entwicklung ist noch nicht am Ende angekommen und wird es wohl auch niemals sein.

[1] *http://www.ard-zdf-onlinestudie.de. Zugegriffen am 08.02.2016.*

Die Polizei stellt sich den Herausforderungen der digitalen Revolution.

DARSTELLUNG UND BEWERTUNG DER KRIMINALITÄTSLAGE

In der Polizeilichen Kriminalstatistik (PKS) werden die Begriffe Internetkriminalität und Computerkriminalität verwendet. Diese werden im Folgenden näher erläutert. Die Fallzahlen entsprechen jedoch nicht dem tatsächlich zu bearbeitenden Fallaufkommen im Bereich Cybercrime. Eine Begründung hierfür ergibt sich aus den Richtlinien der PKS, die eine Nichterfassung 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.

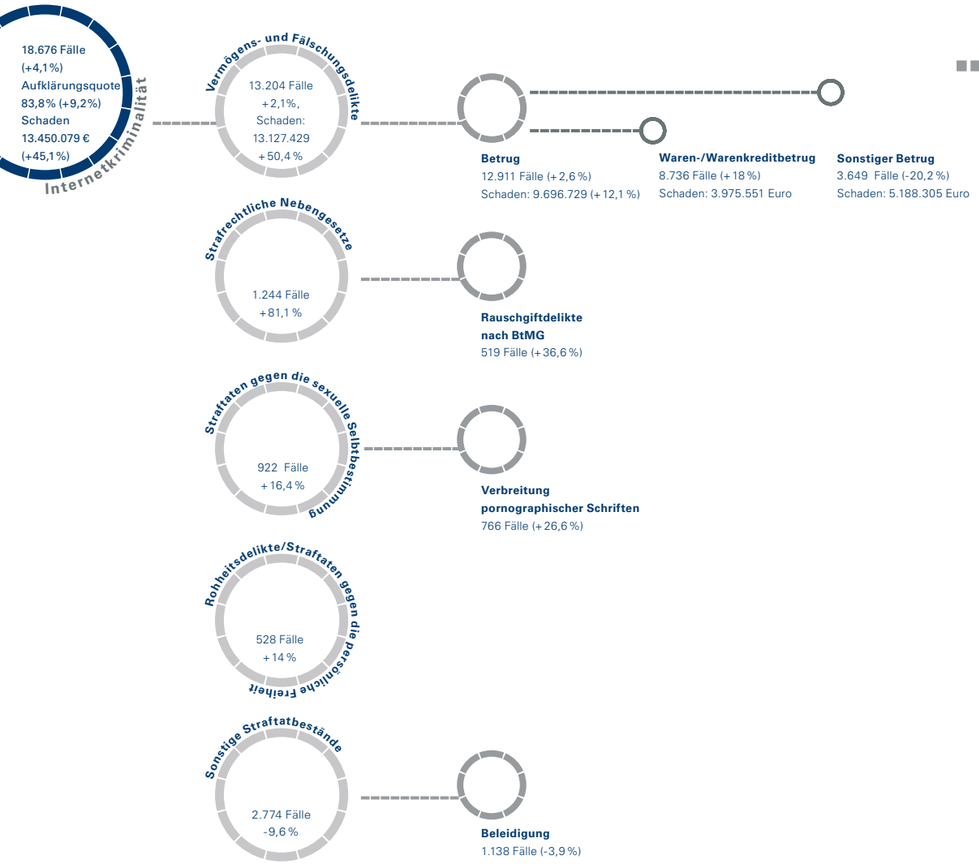


Verhältnis Internet- und Computerkriminalität

INTERNETKRIMINALITÄT (CYBERCRIME TATMITTEL)

Straftaten sind 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, bei denen das Medium Internet als Tatmittel verwendet wird. Der Einsatz eines Personal Computers (PC) oder Notebooks reicht allein nicht aus. 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 Delikte, bei denen das Internet als Kommunikationsmedium bei der Tatbestandsverwirklichung eingesetzt wird.

01



Bei der Internetkriminalität ist ein Anstieg um 4,1 % auf 18.676 Fälle festzustellen. Die Aufklärungsquote ist dabei ebenfalls um 9,2 % auf 83,8 % angestiegen, das heißt es wurden 15.645 Fälle aufgeklärt.

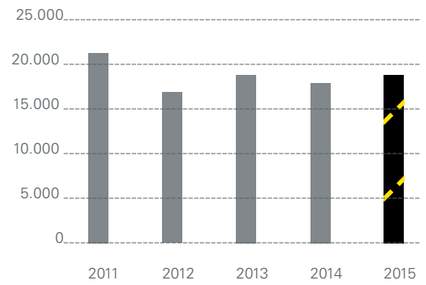
Die Vermögens- und Fälschungsdelikte haben um 2,1 % auf 13.204 Fälle zugenommen. Der Betrug mit 12.911 Fällen hat dabei den größten Anteil an der Zahl der Straftaten in diesem Deliktsbereich. Innerhalb des Betrugs ist der Waren-/Warenkreditbetrug maßgeblich. Hier ist ein Anstieg um 18,0 % auf 8.736 Fälle festzustellen, wohingegen beim sogenannten sonstigen Betrug die Anzahl der Fälle um 20,2 % auf 3.649 zurückging.

Betrachtet man weitere Deliktsbereiche aus der Internetkriminalität, fallen vor allem die Strafrechtlichen Nebengesetze auf, welche mit einem Zuwachs von 557 Fällen eine Steigerung um 81,1 % auf 1.244 Fälle zu verzeichnen haben. Verantwortlich dafür sind hauptsächlich die Rauschgiftdelikte nach dem Betäubungsmittelgesetz (BtMG) mit einer Steigerung von 380 auf 519 Fälle. Die Straftaten gegen die sexuelle Selbstbestimmung sind im Jahr 2015 um 130 Fälle auf 922 Fälle angestiegen und befinden sich damit auf dem Höchststand im Fünfjahresvergleich. Grund hierfür ist vor allem der Deliktschlüssel Verbreitung pornographischer Schriften, welcher eine Steigerung um 26,6 % auf 766 Fälle zu verzeichnen hat. Die Rohheitsdelikte/Straftaten gegen die persönliche Freiheit haben im Jahr 2015 mit einem Plus von 14,0 % auf 528 Fälle ebenfalls zugenommen. Unter den „Sonstigen Straftaten gemäß StGB“ ist der Straftatbestand Beleidigung trotz einer Abnahme um 3,9 % mit 1.138 Fällen weiterhin auf einem anhaltend hohen Niveau.

Der Schaden, der durch die Internetkriminalität verursacht wurde, beläuft sich auf eine Summe von 13.450.079 Euro und nahm dabei im Vergleich zum Vorjahreszeitraum um 45,1 % zu. Ursächlich für diesen hohen Zuwachs ist zu einem Großteil die Erfassung eines Ermittlungsverfahrens des LKA BW wegen Untreue, bei welchem der monetäre Schaden mit 3.400.000 Euro beziffert wird. Beim Waren-/Warenkreditbetrug kam es zu einem Schaden von 3.975.551 Euro. Mit der ebenfalls beträchtlichen Summe von 5.188.305 Euro schlägt der „sonstige Betrug“ zu Buche.

02

CYBERCRIME TATMITTEL (2011-2015)



COMPUTERKRIMINALITÄT (CYBERCRIME IM ENGEREN SINNE)

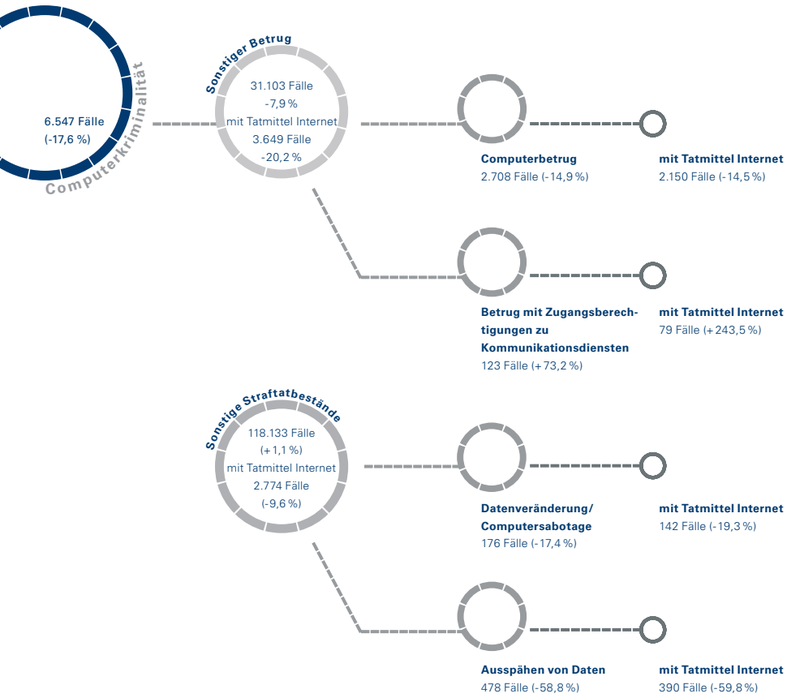
Cybercrime im engeren Sinne umfasst nach bundesweit gültiger Definition alle Straftaten, die sich gegen

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

richten.

In Abgrenzung zur Internetkriminalität ist die Informationstechnik also nicht nur Tatmittel.
Vielmehr geht es um Angriffe gegen die Informationstechnik oder auf deren Daten.

03

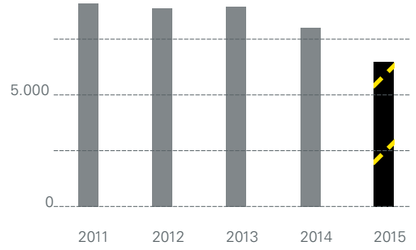


Bei der Computerkriminalität ist ein Rückgang um 17,6 % auf 6.547 Fälle zu verzeichnen. Mitverantwortlich für den Rückgang ist der Computerbetrug. Im Vergleichszeitraum sind die Fallzahlen um 14,9 % auf 2.708 Fälle gesunken. Damit ist der Tiefststand im Fünfjahresvergleich erreicht.

Beim Ausspähen von Daten ist prozentual der höchste Rückgang zu verzeichnen. Hier sind die Fallzahlen um 58,8 % auf 478 Fälle gesunken. Dafür legte der Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten um 52 auf 123 Fälle zu. Die Straftatbestände Computersabotage und Datenveränderung umfassen 176 Fälle und verzeichnen damit eine Abnahme um 17,4 %.

04

CYBERCRIME IM ENGEREN SINNE (2011-2015)



Auch die Straftaten der Computerkriminalität, welche über das Internet begangen werden, zeigen sich rückläufig. Diese haben einen Rückgang um 22,6 % auf 3.090 Fälle zu verzeichnen. Beim Computerbetrug ist hierbei ebenfalls eine Abnahme um 14,5 % auf 2.150 Fälle festzustellen. Die Fallzahlen des Delikts Ausspähen von Daten mit einer Tatbegehung über das Internet sind um 59,8 % auf 390 Fälle zurückgegangen und haben damit einen Tiefststand im Fünfjahresvergleich erreicht. Die Straftaten Computersabotage und Datenveränderung verzeichnen mit 142 Fällen eine Abnahme um 19,3 %.

ERMITTLUNGEN CYBERCRIME

2

Cyber-Dschihad Gekaperte Fernsehsender sind erst der Anfang– Die Welt 04/2015

Reparatur nach Cyberangriff: Der Bu ndestag zieht den Stecker Tagesschau 08/2015

Hacker übernehmen smartes Scharfschützengewehr–heise 07/2015

Falsche E-Mails –Wenn sich Betrüger als Chef ausgeben–Süddeutsche 08/2015

Hacker übernimmt Narkosegerät T-Online 08/2015

Wenn Cyberattacken in den Bankrott führen–Wirtschafts Woche 11/2015

2015 – das Jahr der Sicherheitslücken ZDNet 11/2015

Digitalisierung nimmt zu, IT-Sicherheit nimmt ab haufe 10/2015

shutterstock.com

ERMITTLUNGEN CYBERCRIME

Die Abteilung Cybercrime/Digitale Spuren des LKA BW bearbeitet in erster Linie sogenannte Pilot- und Mehrwertverfahren der Cybercrime im engeren Sinne. Pilotverfahren sind Verfahren mit neuartigen Sachverhalten oder Aufklärungsmöglichkeiten in kriminologischer, kriminalistischer oder rechtlicher Hinsicht. Darunter fallen zum Beispiel neue Kriminalitätsphänomene und Begehungsweisen sowie neue erforderliche innovative kriminaltaktische und kriminaltechnische Maßnahmen. 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 BW herangetragen werden.

Die Kriminalinspektionen 5 (K5) der zwölf regionalen Polizeipräsidien bearbeiten Fälle der Cybercrime im engeren Sinne, insbesondere, wenn eine banden- oder gewerbsmäßige Begehungsweise festgestellt wird. Darüber hinaus sind sie für die Cybercrime als Tatmittel und Cybercrime im engeren Sinne zuständig, wenn zu deren Bearbeitung besonderes informationstechnisches Fachwissen und/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 BW 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 BW hoher Beratungs- und Unterstützungsbedarf. Die spezialisierten Dienststellen Cybercrime/Digitale Spuren nehmen in diesem Zusammenhang ermittlungsunterstützende und beratende Tätigkeiten wahr.

ERMITTLUNGSVERFAHREN

Die im Jahr 2015 bei der Abteilung Cybercrime/Digitale Spuren bearbeiteten Ermittlungsverfahren umfassen unter anderem die Phänombereiche Hacking, Ransomware (digitale Erpressung), Underground Economy und Phishing. Die aus den Ermittlungsverfahren gewonnenen Erkenntnisse bestätigen die Erfahrungen aus den Vorjahren, dass die stetig fortschreitenden technischen Entwicklungen in der Informations- und Kommunikationstechnik viele potenzielle Gelegenheiten zur Begehung von Straftaten bieten. Die Vorgehensweisen der Täter im Phänomenbereich Cybercrime werden zunehmend massiver und komplexer. Gleichzeitig versprechen diese Straftaten hohe Erträge bei einem verhältnismäßig niedrigen Entdeckungsrisiko. Anonymisierungs- und Kryptierungstechnologien sowie die regelmäßig grenzüberschreitenden Begehungsformen der Straftaten erschweren die Ermittlungsarbeit der Strafverfolgungsbehörden. Die stetige Weiterentwicklung der Täter und ihrer Angriffsmethoden führt zu einer entsprechend hohen Bedrohungslage für die digitale Informationssicherheit. Im Rahmen der polizeilichen Ermittlungen wurde wiederholt festgestellt, dass die digitale Underground Economy eine große Bandbreite an Dienstleistungen zur Verfügung stellt, welche die Durchführung jeglicher Art von Cybercrime erleichtern. Kriminelle erhalten auch ohne ausgeprägte technische Kenntnisse und mit vergleichsweise geringem Aufwand Zugang zu umfangreichen Werkzeugen, mit denen eine Vielzahl von Cybercrime-Angriffen ausgeführt werden können. Im Hinblick auf die illegalen Machenschaften im Internet stellt sich im Zuge der Ermittlungsmaßnahmen heraus, dass auch die „klassischen“ Kriminalitätsfelder zunehmend von diesem Tatmittel durchdrungen werden.

Anonymisierungs- und Kryptierungstechnologien erschweren die Ermittlungarbeit

shutterstock.com

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.

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

INITIIERUNG VON ERMITTLUNGSVERFAHREN

Im Rahmen von sieben im Berichtsjahr durchgeführten Operationen wegen Verbreitung von Kinderpornografie in dezentralen Netzwerken (Tauschbörsen) wurden durch den AIR weltweit 13.550 Strafverfahren initiiert.

Davon konnten 59 Verfahren Baden-Württemberg und 921 bundesweit zugeordnet werden. Durch den Rücklauf der mit den Operationen verbundenen Erkenntnisanfragen wurde festgestellt, dass mehrere Tatverdächtige bereits Vorstrafen im Bereich des schweren sexuellen Missbrauchs zum Nachteil von Kindern hatten. Über die Strafverfahrensinitiierungen wurden häufig weitere Straftaten nach dem Strafgesetzbuch (StGB), dem BtMG oder Waffengesetz (WaffG) aufgeklärt. Das hierbei eigenentwickelte gerichtsfeste Beweissicherungsverfahren wurde im August 2015 dem Hessischen LKA zur Verfügung gestellt, so dass auch diese Dienststelle rund 1.200 Strafverfahren initiieren konnte.

13.550 Strafverfahren wurden initiiert

05

STRAFVERFAHRENINITIIERUNGEN AIR FÜNFJAHRESVERGLEICH (2011-2015)

Berichtsjahr	2011	2012	2013	2014	2015
Deutschland	420	40	297	731	921
davon Baden-Württemberg	24	4	25	69	59
International	7.720	636	5.419	9.656	12.629
Gesamt	**8.164**	**676**	**5.716**	**10.387**	**13.550**

BEENDIGUNG ANDAUERNDER MISSBRAUCHSHANDLUNGEN

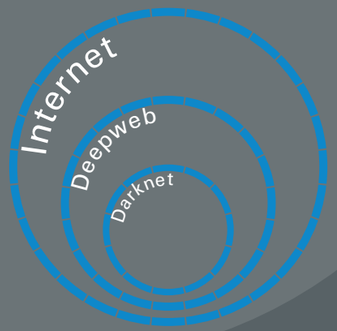
Jahr für Jahr können durch die Arbeit des AIR anhaltende sexuelle Missbrauchshandlungen von Kindern weltweit aufgedeckt und somit weitere Tathandlungen unterbunden werden. Im Jahr 2015 konnten alleine in Deutschland in sieben Fällen Täter identifiziert werden, durch welche acht Opfer im Alter zwischen 4 und 13 Jahren zum Teil noch bis zum Zeitpunkt der Identifizierung schwer missbraucht worden sind.

GEFÄHRDUNGSLAGEN

Der AIR bearbeitete im Berichtszeitraum 19 Gefährdungslagen. Hierbei handelte es sich um 17 Suizidankündigungen und 2 Amokandrohungen, die im Internet veröffentlicht und dem LKA über verschiedene Wege von Dritten übermittelt wurden. Die Zusammenarbeit mit den deutschen Diensteanbietern kann als weitgehend positiv bezeichnet werden. Bei den überwiegend amerikanischen Anbietern sozialer Netzwerke wird hingegen ein sehr unterschiedliches Auskunftsverhalten festgestellt. Die freiwillige Herausgabe von Daten erfolgt in aller Regel nach subjektiver Einschätzung dieser Unternehmen selbst und liegt oftmals konträr zur polizeilichen Bewertung der Gefahrenlage. In mehreren Fällen wurden dem LKA durch ausländische Diensteanbieter keine der angefragten Informationen übermittelt. So mussten Ermittlungsansätze durch zeitlich und personell aufwändige Internetrecherchen aus öffentlich zugänglichen Quellen gewonnen werden.

CYBERGROOMING

Das LKA BW führte im Berichtszeitraum Ermittlungs- und Identifizierungsmaßnahmen gegen Täter durch, welche in Kinder- und Jugendchats minderjährige Opfer mit sexuellem Hintergrund ansprechen („Cybergrooming“). Im Berichtszeitraum konnten so 28 Täter identifiziert werden.



DARKNET

Das Darknet ist eine Untersektion des Deep Web. Beim Deep Web, auch Hidden Web oder Verstecktes Web, handelt es sich um den Teil des Internets, der nicht über Standardsuchmaschinen auffindbar ist. Ein Teil der Informationen wird in passwortgeschützten oder mitgliedsbezogenen Bereichen vorgehalten. Es handelt sich sowohl um legale als auch illegale Inhalte. Die Schwierigkeiten für das Auffinden liegen darin, dass sie nicht durch Suchmaschinen indiziert werden.

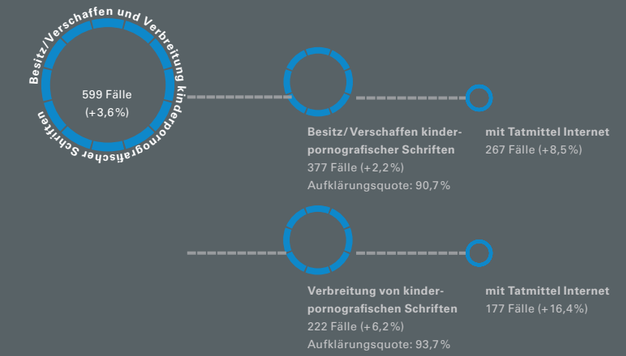
Seiten des Dark Web, auch Darknet bezeichnet, können nicht ohne Weiteres über konventionelle Internetbrowser erreicht werden, da die Informationen eher in Datenbanken vorgehalten werden, die durch Suchmaschinen nur schwer indiziert werden können. Nutzer müssen häufig eine spezielle Software installiert haben, um Zugang zu bestimmten Bereichen des Darknet zu erhalten. Zu den bekanntesten Softwarepaketen gehören The Onion Router (TOR) oder The Invisible Internet Project (I2P). Diese Programme sind separate Plattformen, über die ein spezieller Bereich des Webs mit Seiten, Foren und Peer-to-peer-Netzwerken erreichbar ist. Die Polizei stellt zunehmend sogenannte Marktplätze im Darknet fest, in welchen sich Täter zu Themen wie Betäubungsmittelhandel, Waffen, Falschgeld oder Cybercrime-Dienstleistungen austauschen und ihre Verkaufsgeschäfte tätigen. Der Arbeitsbereich Internetrecherche verstärkte seine Aktivitäten gegen solch illegale Angebote im Darknet, um rechtsfreien Räumen vorzubeugen und Straftäter zu überführen.

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, die von den Landesdienststellen angeliefert werden.

Im Jahr 2015 konnten bei Ermittlungen der Ansprechstelle Kinderpornografie (ASt KiPo) in einer Tauschbörse 39 Strafverfahren im In- und Ausland wegen des Besitzes und der Verbreitung kinderpornografischer Schriften initiiert werden.

06



Beim Besitz/Verschaffen kinderpornografischer Schriften kam es zu einer Zunahme der Fallzahlen um 2,2 % auf 377 Fälle, was sich auch auf die Fallzahlen mit Sonderkenner Internet übertragen hat. Diese haben um 8,5 % auf 267 Fälle zugenommen. Die Aufklärungsquote ist in diesem Bereich seit jeher hoch und beträgt 90,7 %. Die Anzahl der Straftaten der Verbreitung von kinderpornografischen Schriften erhöhte sich um 6,2 % auf 222 Fälle. Der Anteil der Fälle mit Tatmittel Internet nahm dabei um 16,4 % auf 177 Fälle zu. Der Gesamtbereich Besitz/Verschaffen und Verbreitung kinderpornografischer Schriften bewegt sich mit 599 Fällen in etwa auf dem Niveau der Vorjahre. Im Jahr 2015 hat die ASt KiPo 86 Umfangsverfahren mit 273 Tatverdächtigen im Land koordiniert. Hiervon hatten 32 Umfangsverfahren ihren Ursprung in Baden-Württemberg.

Im Jahr 2015 wurden 2.437.326 Bilder und 141.231 Videos durch die Polizeidienststellen des Landes an die ASt KiPo angeliefert. Hiervon konnten bereits 985.695 Dateien kategorisiert und 156.993 kinder- und jugendpornografische Dateien in die Übergangslösung zur Hash-Datenbank Pornographische Schriften (HashDB PS) eingestellt werden. Bei einem Hashwert handelt es sich um den digitalen Fingerabdruck einer Datei.

MD5 HASHWERT DES BILDES: CDE45FDE8E3A6FAFE5258D7D543D4A9B

Mit der HashDB PS ist eine zentrale kriminalpolizeiliche Sammlung von Hashwerten aller bekannten kinder- und jugendpornografischen Dateien geplant. Der Einsatz dieser Hashwerte in laufenden Ermittlungsverfahren führt zu einer deutlichen Reduktion der manuell zu bewertenden Dateien und damit zu einer Beschleunigung der Auswertung von digitalen Asservaten. Durch die daraus resultierende Verringerung der Auswertezeit wird die psychische Belastung der mit der Bewertung befassten Sachbearbeiter erheblich reduziert. In einer Übergangslösung werden die von den Bundesländern angelieferten Hashwerte seit dem 2. Juni 2014 über ein Portal des Bundeskriminalamtes zum Download zur Verfügung gestellt. Die Einführung der HashDB PS ist zum 1. Juli 2016 geplant.

LKA BW, M. Lühning

CDE45FDE8E3A6FAFE5258D7D543D4A9B

SCHULFAHNDUNG

Im Rahmen der Schulfahndung werden Lehrkräften Bilder zur Identifizierung von Kindern gezeigt. Diese Form der zielgruppenorientierten Öffentlichkeitsfahndung stellt eine Mindermaßnahme zur allgemeinen Öffentlichkeitsfahndung dar. Die ASt Kipo koordiniert in diesem Zusammenhang die landesweiten Fahndungsmaßnahmen.

In einem Identifizierungsverfahren des BKA wurden Videodateien festgestellt, die den sexuellen Missbrauch eines Jungen und eines Mädchens dokumentieren. Nach erfolgloser Durchführung polizeiinterner Fahndungsmaßnahmen erfolgte im Oktober 2015 eine Schulfahndung in Baden-Württemberg. Hierbei konnten beide Kinder von deren Lehrern innerhalb von zwei Tagen identifiziert und somit die Fahndung beendet werden. Dieser Fall sowie weitere zurückliegende Ermittlungserfolge verdeutlichen erneut die Bedeutung der zielgruppenorientierten Öffentlichkeitsfahndung in Form der Schulfahndung.

SOFTWAREENTWICKLUNGEN

EINSATZ EIGENENTWICKELTER SOFTWARE IN HESSEN

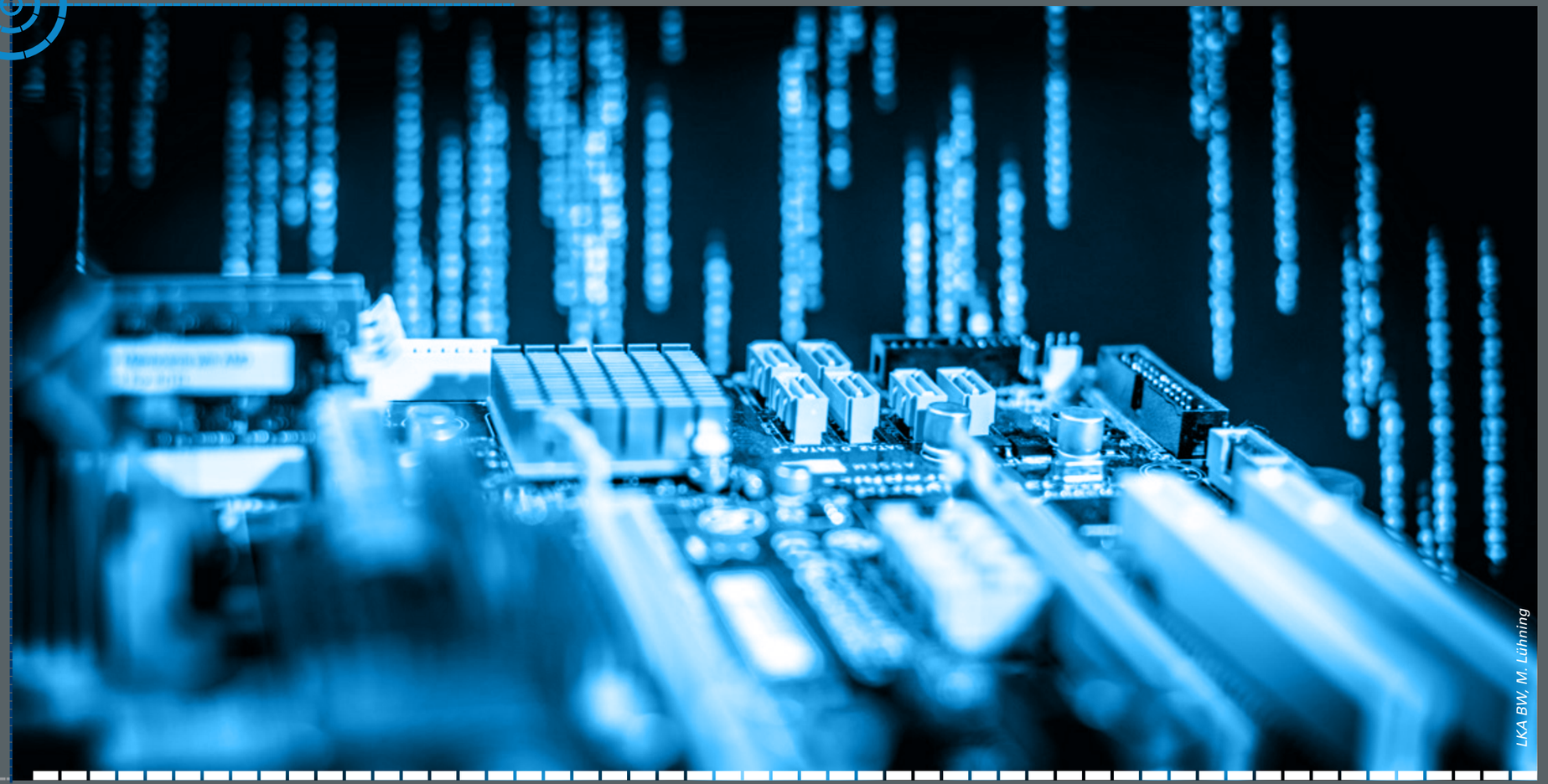
Die von den Informatikern der Inspektion 510 (Teilbereich der Abteilung 5 Cybercrime/Digitale Spuren) beim LKA BW entwickelte Software für das gerichtsfeste Beweissicherungsverfahren bei der Verbreitung von Kinderpornografie über Tauschbörsen wurde dem LKA Hessen zur Verfügung gestellt. Das Entwicklerteam befand sich dazu über mehrere Tage in Hessen. Die Software wurde in die bestehende Infrastruktur integriert und an die dortigen Bedürfnisse anpasst.

TECHNIKER-WORKSHOP 2015

Vom 6. bis 8. Oktober 2015 fand beim LKA BW der vierte Techniker-Workshop statt. Teilnehmer des Workshops sind Informatiker sowie Polizeibeamte, auch aus anderen Bundesländern, Österreich und der Schweiz, welche mit Programmieraufgaben betraut sind. Beim diesjährigen Workskhop wurden eigenentwickelte Softwarelösungen für Ermittlungen in sozialen Netzwerken und zu Handy-Messengern vorgestellt. Außerdem wurden Informationen zu Webseiten-Sicherungen und allgemeinen Entwicklungen im Bereich der Forensik vorgestellt.

DIGITALE FORENSIK

3



LKA BW, M. Lühning

DIGITALE FORENSIK

Die Sicherung und Auswertung von Spuren ist seit jeher wesentlicher Bestandteil der Strafverfolgung. Die digitalen Spuren haben ergänzend zu den klas-

Digitale Spuren nehmen an Bedeutung zu

sischen Spurenarten, wie Finger-, Schuhlaufflächen-, Werkzeug- oder DNA-Spuren, in den zurückliegenden Jahren stark an Bedeutung gewonnen.
In einer immer enger vernetzteren Welt, in der nicht nur Menschen sondern zunehmend Maschinen und Systeme miteinander kommunizieren, fallen diese Spuren fortlaufend an, auch ohne menschliches Zutun. Insbesondere diese kaum manipulierbaren Spuren sind auch in der Digitalen Forensik von besonderem Interesse und können in nahezu jedem Deliktsfeld auftreten. Digitale Spuren spielen daher nicht nur oder gar ausschließlich bei der Bekämpfung der Cyberkriminalität eine Rolle. Gerade in Wirtschaftsdelikten, Rauschgiftverfahren und in Staatsschutzangelegenheiten nimmt ihre Bedeutung stetig zu.

STRUKTURIERTE UND UNSTRUKTURIERTE MASSENDATEN

Die Polizei Baden-Württemberg unterscheidet bei der Untersuchung von großen Datenmengen zwischen strukturierten und unstrukturierten Massendaten.
Daten, die im Vorfeld bereits in definierte Strukturen mit festgelegter Bedeutung überführt wurden, werden als strukturierte Massendaten bezeichnet. So handelt es sich beispielsweise bei Funkzellendaten, die in tabellarischer Form vorliegen, um strukturierte Massendaten. 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 im allgemeinen von unstrukturierten Massendaten.

Die wesentlichen Bearbeitungsschritte sind bei beiden Datenarten sehr ähnlich. Zuerst erfolgt die Sicherung, im Anschluss die Untersuchung und Aufbereitung der Daten und abschließend die (inhaltliche) Bewertung der dann verfügbaren und lesbaren digitalen Spurenlagen. Die ersten beiden Arbeitsschritte fallen für unstrukturierte Datenquellen in den Zuständigkeitsbereich der spezialisierten Sachbearbeiter digitaler Spuren. Sie bearbeiten damit eine Querschnittsaufgabe als Serviceeinheit innerhalb der Polizei für alle anderen Polizeieinheiten.

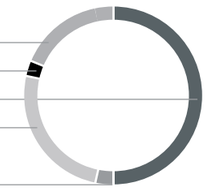
IT-BEWEISSICHERUNG

Die Untersuchung und Aufbereitung der unstrukturierten Daten unter forensischen Gesichtspunkten erfordert ein hohes Maß an Fachwissen, Zeit und Rechenleistung. Jede einzelne Datei ist (unter Umständen auch nach deren Löschung) zu lokalisieren, lesbar zu machen, gegebenenfalls zu entschlüsseln, zu klassifizieren und für die weitere Verwendung und Bewertung durch den polizeilichen Ermittler aufzubereiten. Hierbei ist insbesondere darauf zu achten, dass keine Veränderungen an den Originalasservaten oder am Originaldatenbestand durchgeführt werden.
Nur durch stetige Weiterentwicklung der Untersuchungsmethoden und Investitionen in die eingesetzte Technik kann eine Aufrechterhaltung der aktuellen Leistungsfähigkeit in der IT-Beweissicherung gewährleistet werden. Bei einer generellen Tendenz nach oben unterliegt das tatsächlich bearbeitete Datenvolumen von Jahr zu Jahr starken Schwankungen. Dies ist unter anderem in Unterschieden bei den bearbeiteten Ermittlungsverfahren begründet. Wird beispielsweise gegen eine illegale Raubkopierplattform vorgegangen, so können hierbei in einem einzigen Verfahren Datenmengen im dreistelligen Terabyte-Bereich anfallen. Bei Verfahren, in denen lediglich E-Mails für den Tatnachweis sichergestellt werden, nimmt zwar die inhaltliche Auswertung ebenfalls viel Zeit in Anspruch, die tatsächliche Datenmenge ist im Vergleich zu hochauflösenden Kinofilmen jedoch wesentlich geringer.

07

ASSERVATENMIX 2015

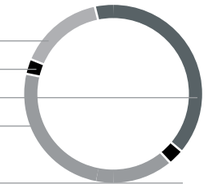
PC	3.990	14 %
Sonstige	883	3 %
Mobiltelefone und SIM-Karten	**15.087**	**54 %**
Datenträger	7.193	26 %
Tablets	958	3 %



08

ASSERVATENMIX 2014

PC	4.494	12 %
Sonstige	1.232	3 %
Mobiltelefone und SIM-Karten	14.663	37 %
Datenträger	**18.114**	**46 %**
Tablets	738	2 %



BOMBENDROHUNG BEI GERMANY'S NEXT TOPMODEL

Am 15. Mai 2015 wurde die Live-Übertragung der Fernsehshow Germany's Next Topmodel in der SAP-Arena in Mannheim aufgrund einer anonymen Bombendrohung abgebrochen. Durch Mitarbeiter des LKA BW wurden Maßnahmen der IT-Beweissicherung direkt vor Ort in der SAP-Arena in Mannheim durchgeführt. Dies geschah in Abstimmung mit der sachbearbeitenden Dienststelle des Polizeipräsidiums Mannheim. In Zusammenarbeit mit dem technischen Betreiber der Arena wurden Daten der Telefonanlage gesichert und das Telefon, auf welchem der Drohanruf angenommen worden war, für weitere Untersuchungen sichergestellt. Nach Kontaktaufnahme mit dem Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (Bitkom) im Rahmen der Sicherheitskooperation Cybercrime erhielt das LKA technische Informationen, die für die Aufklärung des Sachverhalts hilfreich waren. Des Weiteren waren Daten von einem Webserver in München, auf dem die Internetseite der SAP-Arena betrieben wird, für die nachfolgenden Ermittlungen zu sichern. In Kooperation mit dem Webhoster konnten potenziell beweiserhebliche Daten gesichert und an die sachbearbeitende Dienststelle zur weiteren inhaltlichen Auswertung übergeben werden.

SONSTIGE AKTIVITÄTEN

Im Berichtsjahr wurden umfangreiche Vorbereitungen für den Aufgabenbereich Multimediaforensik getroffen.

MULTIMEDIAFORENSIK

Zu den Kernaufgaben dieses neuen Aufgabenbereichs zählt die Aufbereitung und forensische Untersuchung von digitalen Bild-, Video- und Audioaufnahmen (beispielsweise Bildmaterial von Überwachungskameras). Hierzu zählt auch die Untersuchung von verdächtigen Multimediadateien, zum Beispiel auf Veränderungen oder Manipulationen. Durch einen solchen neuen Aufgabenbereich besteht die Möglichkeit, die zuständigen Mitarbeiter bestmöglich zu spezialisieren und fortzubilden. Ziel ist es, den Dienststellen des Landes Untersuchungen und Dienstleistungen mit hoher Qualität anbieten zu können.
Im Bereich der IT kommt es zu einer stetigen und äußerst dynamischen Entwicklung. Umso wichtiger ist ein ständiger Informations- und Erfahrungsaustausch, sowohl zwischen den in der IT-Forensik tätigen Mitarbeitern der Polizei Baden-Württemberg als auch mit Vertretern von ermittlungsführenden Dienststellen und der Justiz.

INFORMATIONS- UND ERFAHRUNGSAUSTAUSCH

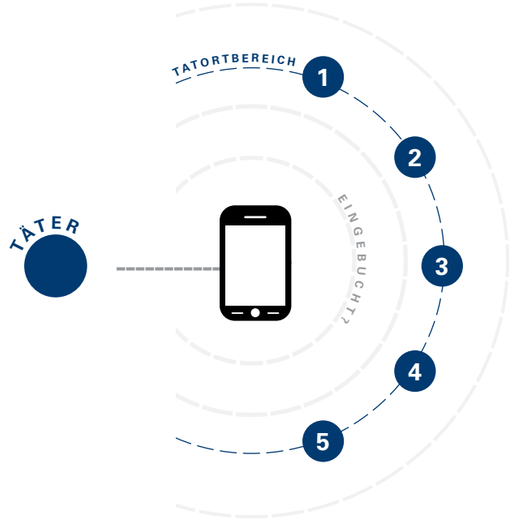
Auch im Jahr 2015 wurden Workshops und Kontakttreffen zu verschiedenen Spezialthemen der IT-Forensik durchgeführt, um eine rasche Weitergabe von Informationen, Fachwissen und Erfahrungen zu gewähleisten. Darüber hinaus dienen Workshops dieser Art der Pflege professioneller Netzwerke, durch welche zum Beispiel aufkommende Fragen schneller gelöst und neue Entwicklungen früher erkannt werden können. Im November 2015 wurde ein Workshop zur forensischen Untersuchung von Rechnern mit Apple Mac OS X-Betriebssystemen durchgeführt, welcher durch das LKA BW und die HfPol BW organisiert wurde. Ein wesentliches Ziel war der Austausch über die neuesten Entwicklungen. Neben Teilnehmern der IT-Beweissicherungsdienststellen waren Angehörige der Steuerfahndung als Referenten und Kursbesucher anwesend. Weitere Workshop- beziehungsweise Vortragsthemen waren „Möglichkeiten und Grenzen bei der Sicherung volatiler digitaler Spuren“ oder die „Sicherung und Untersuchung digitaler Spuren auf mobilen Endgeräten“. Neben den Fortbildungsangeboten der HfPol BW sind nationale aber auch internationale Schulungen und Konferenzen von großer Bedeutung. Hier werden beispielsweise Zertifizierungen für die Bedienung spezieller forensischer Hard- und Softwareprodukte sowie für Untersuchungsmethoden erlangt.

DATENANALYSE AN EINEM BEISPIEL

Und wieder kam es zu einem Wohnungseinbruch in den frühen Abendstunden. Der Wert des Diebesgutes ist beträchtlich. Es verdichten sich die Hinweise, dass es sich um eine Tatserie handelt. Zeugen wollen beobachtet haben, wie eine unbekannte verdächtige Person das Gebäude über ein Fenster an der Gebäuderückseite telefonierend verließ.

09

EIN FALL FÜR DIE DATENANALYSE



Die Ermittler der örtlichen Kriminalpolizei übernehmen zu diesem Wohnungseinbruch die Sachbearbeitung. Im weiteren Umkreis ist es bereits der fünfte Fall mit ähnlicher Vorgehensweise. Der Hinweis auf eine verdächtige Person, die am Tatort telefoniert haben soll, eröffnet den Ermittlern neue Aufklärungsansätze.

LÄSST SICH DAS TELEFON FESTSTELLEN, DAS DIE VERDÄCHTIGE PERSON NUTZTE?

Mit dieser zentralen Fragestellung entwickeln die polizeilichen Ermittler gemeinsam mit den Sachbearbeitern Datenanalyse von der örtlich zuständigen Analysestelle eine Strategie. Es sollen die Telekommunikationsverkehrsdaten (TK-Daten) zu den relevanten Tatortbereichen erhoben und miteinander verglichen werden.

Damit die Sachbearbeiter Datenanalyse ihre Arbeit aufnehmen können, bedarf es zunächst vorbereitender Maßnahmen.

DIE ERHEBUNG DER TK-DATEN ALS BASISARBEIT

Die Erhebung derartiger Daten zum Zwecke von Vergleichsuntersuchungen stellt einen Grundrechtseingriff dar und bedarf grundsätzlich einer richterlichen Anordnung. Daher regen die Ermittler in Abstimmung mit den Sachbearbeitern Datenanalyse gemäß § 100g Strafprozessordnung (StPO) bei der örtlich zuständigen Staatsanwaltschaft die Erhebung der TK-Daten an. Die Staatsanwaltschaft stellt nach Prüfung einen Antrag auf Erhebung von TK-Daten beim zuständigen Amtsgericht, welches den Beschluss, dass die Betreiber der Mobilfunknetze (Netzbetreiber) die beantragten Auskünfte gegenüber der Polizei zu erteilen haben, erlässt.

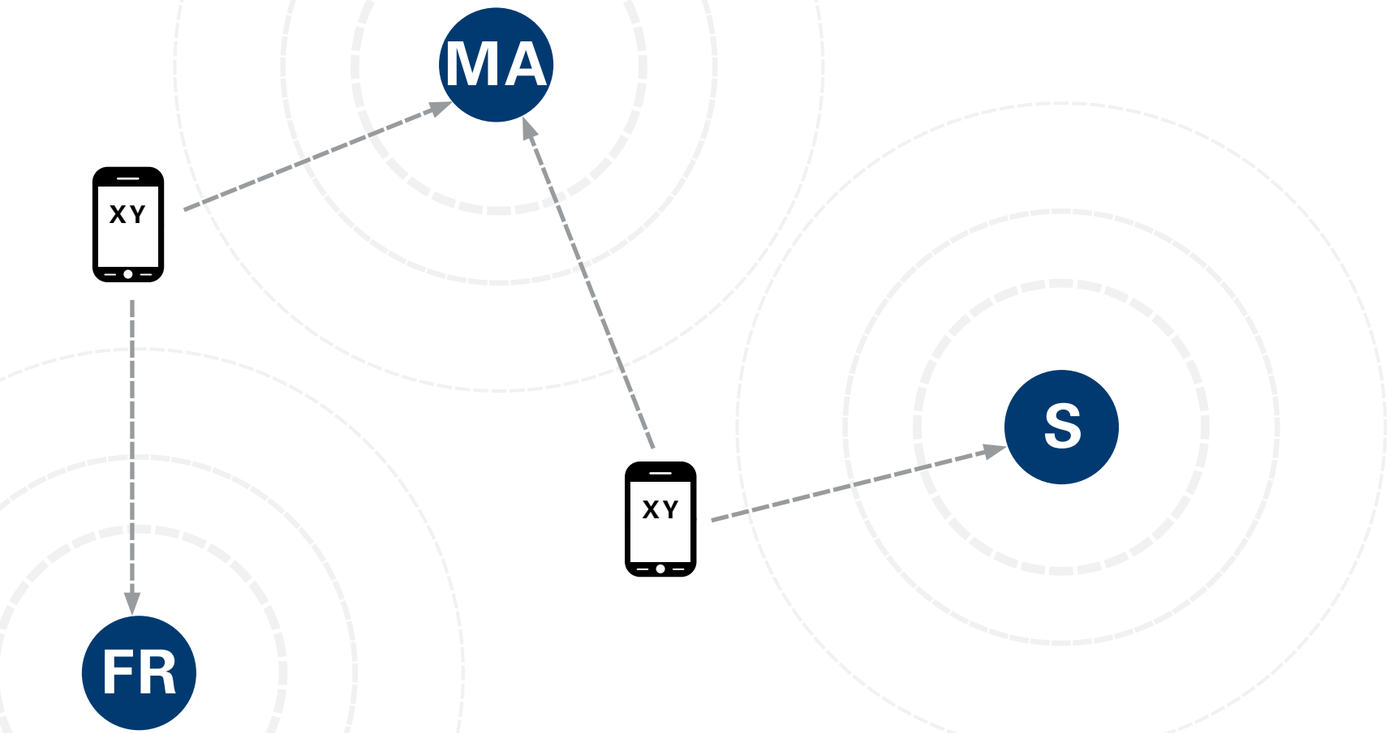
DIE NETZBETREIBER WERDEN VERPFLICHTET, DIE TK-DATEN DER POLIZEI MITZUTEILEN

Der richterliche Beschluss wird an die Netzbetreiber übermittelt. Die Ermittler erhalten daraufhin die TK-Daten für die beantragten fünf Tatortbereiche, bezogen auf die jeweils relevanten Tatzeiträume.

BEGINN DER EIGENTLICHEN ANALYSEARBEIT

Der Sachbearbeiter Datenanalyse beginnt, die Antwortdaten der Netzbetreiber strukturiert zu archivieren und aufzubereiten. Eine fehlerfreie Datenbasis ist für eine sachgerechte Analyse zwingend erforderlich. Jeder Datensatz steht für eine Telekommunikationsverbindung innerhalb der erhobenen Tatortbereiche. Eine zentrale Frage des Ermittlers ist:

GIBT ES EINE MOBILFUNKNUMMER, DIE AN MEHREREN TATÖRTLICHKEITEN EINGEBUCHT WAR?



Mit Nachdruck untersuchen die Sachbearbeiter Datenanalyse den Datenbestand. Es ist höchste Eile geboten, da in Anbetracht der mutmaßlich vorliegenden Tatserie mit einem weiteren Auftreten der Einbrecher in allernächster Zeit zu rechnen ist. Es gelingt den Sachbearbeitern Datenanalyse, aus der Vielzahl der Datensätze vier Mobilfunkrufnummern zu filtern, die jeweils in zumindest zwei Tatortbereichen zu den tatrelevanten Zeiten eingebucht waren. Es können zu diesen eingebuchten Rufnummern mehrere Kommunikationsvorgänge nachvollzogen werden und damit der sachbearbeitenden Dienststelle wichtige Ermittlungsansätze an die Hand gegeben werden.

DIE ANALYSEERGEBNISSE GEHEN UNVERZÜGLICH AN DIE ERMITTLUNGSDIENSTSTELLE

Der Sachbearbeiter Datenanalyse fertigt einen Analysebericht, in dem er die wesentlichen Arbeitsschritte dokumentiert und die erzielten Ergebnisse darlegt. Dieser Bericht wird umgehend der sachbearbeitenden Dienststelle übermittelt, damit diese weitere Ermittlungsmaßnahmen einleiten kann. Vielleicht sind eine oder mehrere der erkannten Mobilfunkrufnummern tatsächlich von der mutmaßlichen Einbrecherbande verwendet worden. Das werden die weiteren Ermittlungen zeigen.

FALLZAHLEN DER ANALYSESTELLEN

Der dargestellte fiktive Fall entspricht grundsätzlich den Realbedingungen und gibt nur einen thematischen Teilbereich der Arbeit des Sachbearbeiters Datenanalyse wieder. Die Aufgaben des Datenanalysten beziehen sich neben der Verarbeitung von TK-Daten zudem auf weitere analysefähige Datenfelder, wie zum Beispiel Personendaten, Kraftfahrzeugdaten oder georeferenzierte Informationen, die im Rahmen von Ermittlungsverfahren zu untersuchen sind. Die unten aufgeführten Kerndaten beziehen sich insofern auf alle betroffenen Daten. Für das Jahr 2015 sollen erstmals landesweite Kerndaten ausgewiesen werden, die einen Eindruck über das erfolgte Arbeitsaufkommen vermitteln. Diese Daten dürfen insofern als Basisinformationen für die Werte der kommenden Jahre gesehen werden.

Vorgänge	**2.090**	Anzahl der Ermittlungsverfahren, die von den Analysestellen bearbeitet wurden.
Fälle	**4.579**	Anzahl der Einzelfälle, die innerhalb der Ermittlungsverfahren bearbeitet wurden. Einzelfälle sind die eigentlichen „Datenpools“ die aufbereitet und untersucht werden. Das können zum Beispiel TK-Verbindungsdatenbestände, Personendatenbestände, Kraftfahrzeugdatenbestände, georeferenzierte Datenbestände sein.

Grundsätzlich unterstützen die Analysestellen Sonderkommissionen, die wegen diverser Kapitaldelikte und anderer schwerer Straftaten eingerichtet werden. Die Analysestelle des LKA BW leistete in vier Sonderkommissionen entsprechende Unterstützungarbeit bei der Aufklärung von Tötungs- und Brandstiftungsdelikten.

TELEKOMMUNIKATIONSÜBERWACHUNG

4

LKA BW

TELEKOMMUNIKATIONSÜBERWACHUNG

Telekommunikationsüberwachung liefert auch unter zunehmend schwierigeren Rahmenbedingungen weiterhin unverzichtbare Ermittlungsansätze. Übertragungsgeschwindigkeiten, Bandbreiten und Datenmengen der Telekommunikation nehmen stark zu. Darüber hinaus zeichnet sich dieser Markt durch eine zunehmende Verschlüsselung der Kommunikationsinhalte, technisch bedingte oder absichtlich erzeugte Anonymisierung von Teilnehmeranschlüssen, Internationalisierung und die Einführung neuer technischer Standards aus. Herkömmliche Kommunikations- und Telemediendienste verschmelzen miteinander und führen zu einer steigenden Anzahl an Kommunikations- und 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. Früher wurde fernmündlich „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 vor allem 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. Durch das Kompetenzzentrum für informationstechnische Überwachung beim Bundeskriminalamt, kurz CC-ITÜ, wurden in einem engen rechtlichen Rahmen technische Alternativen erarbeitet. Diese ermöglicht es den berechtigten Stellen, die Telekommunikationsinhalte „an der Quelle" zu erheben.

KOMPETENZZENTRUM TELEKOMMUNIKATIONSÜBERWACHUNG

Die landesweite TKÜ-Zentrale setzt Beschlüsse nach den §§ 100 a StPO (Telekommunikationsüberwachung) i.V. m. 100 b StPO (Verfahren bei der Telekommunikationsüberwachung) und Verkehrsdatenanfragen nach § 100 g StPO beziehungsweise § 23 a Polizeigesetz Baden-Württemberg (PolG BW) um. Verkehrsdaten sind beispielsweise Datum, Uhrzeit und Kennung eines beteiligten Telefonanschlusses oder bei mobilen Anschlüssen die Standortdaten der genutzten Funkzelle. Lediglich die technische Umsetzung wird hierbei im LKA BW realisiert. Die Inhalte werden im Folgenden landesweit an den Arbeitsplatz des jeweiligen Sachbearbeiters ausgeleitet. Kernstück der technischen Plattform für die Telekommunikationsüberwachung ist die leistungsfähige TKÜ-Anlage. Statistische Daten zu Maßnahmen nach den §§ 100 a und 100 g StPO sind über das Bundesamt für Justiz im Internet abrufbar:
https://www.bundesjustizamt.de/de/themen/buergerdienste/justizstatistik/telekommunikation/telekommunikationsueberwachung_node.html

Neben den oben genannten technischen Unterstützungen beraten die Mitarbeiter Polizeibeamte des Landes 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 hier ebenfalls durchgeführt. Beispielsweise kann bei einer suizidgefährdeten Person die Funkzelle festgestellt werden, in welcher ein Mobiltelefon eingebucht ist. Zur Sicherstellung einer 24/7-Erreichbarkeit ist außerhalb der Kernarbeitszeit ein Bereitschaftsdienst verfügbar.

AUS- UND FORTBILDUNGSANGEBOTE

Das Feld der Telekommunikation und damit verbundene Möglichkeiten der Überwachung unterliegen einem ständigen Wandel, der auch Auswirkungen auf die Hard- und Software der TKÜ-Anlage und damit auf die Anforderungen an die Ermittler im gesamten Land hat. Die Mitarbeiterinnen und Mitarbeiter des TKÜ-Zentrums bieten daher unter dem Motto „aus der Praxis für die Praxis" Aus- und Fortbildungsveranstaltungen für Ermittler, die Justiz und andere Bedarfsträger an. Im Jahr 2015 wurden 35 derartige Veranstaltungen durchgeführt.

OPERATIVE IT / NETZWERKFORENSIK

Die hochqualifizierten Polizeivollzugsbeamten und IT-Spezialisten (Informatiker) des Arbeitsbereichs Operative IT/Netzwerkforensik (OIT) unterstützen Polizeibeamte landesweit im Bereich IT-bezogener Ermittlungen. Die beratenden und unterstützenden Maßnahmen der Operativen IT/Netzwerkforensik müssen für jedes Verfahren individuell angepasst und abgestimmt werden.

Im Jahr 2015 wurde die OIT in 151 Verfahren einsatzunterstützend tätig. Beispielsweise wurde bei Erpressungslagen unterstützt, um die Täter im Internet zu lokalisieren. In einem anderen Fall konnte in Zusammenarbeit mit dem LKA Berlin der Beschuldigte in einem Fall des sexuellen Missbrauchs an einem Kind geortet und so letztlich festgenommen werden. Der Täter hatte versucht, seinen E-Mail-Verkehr durch ständiges Wechseln von Internet-Cafes zu verschleiern.

MOBILFUNKAUFKLÄRUNG (MFA)

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

MOBILFUNKAUFKLÄRUNG AN EINEM BEISPIEL

Im Mai 2015 wurde ein 15-jähriges Mädchen als vermisst gemeldet. Laut Auskunft der Eltern war sie in psychiatrischer Behandlung und suizidgefährdet. Nach dem Verschwinden kündigte sie ihren Suizid gegenüber der Mutter an. Der Messenger-Status wurde auf „Au revoir“ gesetzt. Das Telefon wurde danach ausgeschaltet. Überprüfungsmaßnahmen an bekannten Hinwendungsorten sowie eine Suche mittels Hubschrauber verliefen negativ. Mitten in der Nacht wurde das Mobiltelefon des Mädchens wieder eingeschaltet. Der Funkmast, über welchen das Handy eingebucht wurde, konnte so in Erfahrung gebracht werden. Um den Standort weiter einzugrenzen erfolgte die Anforderung der Mobilfunkaufklärung. Die Mitarbeiter konnten bereits wenig später den Standort des Mobiltelefons lokalisieren. Die Überprüfung durch eine Polizeistreife ergab, dass die 15-Jährige bei einem Bekannten übernachtet hatte.

Im Zusammenhang mit suizidgefährdeten oder vermissten Personen wurden die Fachkräfte des Arbeitsbereichs Mobilfunkaufklärung im Jahr 2015 in 34 Fällen angefordert.

Seit April 2015 leisten die Mitarbeiter der Mobilfunkaufklärung einen 24/7 Bereitschaftsdienst. Hierdurch ist die Erreichbarkeit auch außerhalb der regulären Dienstzeiten gewährleistet. Wegen einer Zunahme an Aufträgen wurde der Arbeitsbereich personell aufgestockt.

TKÜ-Zentrale des LKA BW

ZENTRALE ANSPRECHSTELLE CYBERCRIME

5

LKA BW, L. Köhnlein

Infomaterial der ZAC, gerichtet an Wirtschafts-unternehmen und Behörden

SINGLE POINT OF CONTACT

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 2015 nahmen die Kontaktaufnahmen der primären Zielgruppe im Vergleich zum Vorjahr deutlich zu. Insgesamt gingen 481 Hinweise und Anfragen bei der ZAC ein. Die Mitarbeiterinnen und Mitarbeiter der Ansprechstelle können zwischenzeitlich auf ein bundesweites Netzwerk von ZAC-Dienststellen, die beim BKA und den Landeskriminalämtern eingerichtet sind, zurückgreifen. Insbesondere für die Unternehmen des Landes rücken die Zentralen Ansprechstellen zunehmend in den Mittelpunkt der Information und Kommunikation rund um das Thema Cybercrime. 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 2015 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. Bei herausragenden Kriminalitätsphänomenen veröffentlichte die ZAC anlassbezogen Warnmeldungen, welche sowohl über die Industrie- und Handelskammern sowie andere Kooperationspartner, als auch über die Internetseite der ZAC zur Verfügung gestellt wurden.

www.lka-bw.de/zac

Vor einer besonders perfiden Masche wurde im Oktober 2015 gewarnt. Hier wurden an zahlreiche Firmen vermeintliche Bewerbungen per E-Mail übersandt.

Schadsoftware in vermeintlichen „Bewerbungsmappen“

Beim Öffnen der „Bewerbungsmappe“ wurde jedoch kein Lebenslauf oder Ähnliches dargestellt, stattdessen wurden Dateien, auf welche der Benutzer aktuell Zugriff hatte (auch Netzlaufwerke) verschlüsselt. Zur Entschlüsselung wurde eine Zahlung in Form von Bitcoins erpresserisch gefordert.
Bitcoin ist eine digitale Währung. Der Wert eines Bitcoin lag im Dezember 2015 bei circa 400 Euro. Wer mit Bitcoins eine Zahlung vornehmen möchte, muss eine sogenannte Bitcoin-Wallet (Geldbörse) installieren. Mit dieser kann eine Bitcoin-Adresse generiert werden. Ähnlich wie bei Paypal kann man seine Bitcoin-Adresse

einfach weitergeben, damit andere Nutzer darauf einzahlen können. Alle bestätigten Buchungen werden in der sogenannten Blockchain (Blockkette) eingetragen. Die Blockchain ist ein gemeinsames öffentliches Buchungssystem, auf dem das gesamte Bitcoin-Netzwerk basiert. Auf diese Art kann der Kontostand der Bitcoin Wallets berechnet und neue Transaktionen ausgeführt werden.
Um das Bitcoin-Wallet aufzuladen kann man bei bestimmten Online-Marktplätzen Bitcoins (gegen Euro) erwerben.
Um die Wahrscheinlichkeit zu erhöhen, dass durch den Angeschriebenen die Schadsoftware ausgeführt wird, wurde der Bewerbungstext häufig tatsächlich ausgeschriebenen Stellen angepasst. Die E-Mails waren meist orthografisch sowie grammatikalisch fehlerfrei formuliert. Teilweise wurde zudem die Schadsoftware nicht direkt der E-Mail beigefügt, sondern in einer Cloud als „Bewerbungsmappe" verlinkt. Dadurch konnte der Täter auch nach Versand der E-Mails die Schadsoftware in der Cloud aktualisieren, so dass diese in der Regel von aktuellen Antivirenprodukten nicht erkannt wurde.

FAKE PRESIDENT

Ein weiteres Phänomen, zu welchem die ZAC Baden-Württemberg im Berichtszeitraum eine Warnmeldung veröffentlichte, ist bekannt unter dem Begriff CEO-Fraud oder Fake President. Hierbei werden Mitarbeiter einer Firma vom vermeintlichen Geschäftsführer (CEO) angeschrieben und angewiesen, eine Zahlung einer beträchtlichen Summe in die Wege zu leiten. Häufig wird als Hintergrund der Transaktion eine angebliche Firmenübernahme genannt. Der Betrag liegt meist im sechs- bis siebenstelligen Bereich. Um Authentizität des Absenders vorzugaukeln, tragen die Täter die originale E-Mailadresse des Geschäftsführers als Alias ein. Für den Versand der E-Mails werden kostenlose E-Mail Provider genutzt. Da der Angeschriebene erkennen kann, dass die Nachricht nicht vom firmeneigenen E-Mail Dienst verschickt wurde, wird meist am Ende der Nachricht der Zusatz „sent from my iPhone" eingefügt. Somit wird dem Angeschriebenen suggeriert, dass der Geschäftsführer über seinen privaten E-Mail Account kommuniziert. Bei einer direkten Antwort auf die Nachricht wird jedoch der Täter und nicht der tatsächliche Geschäftsführer angeschrieben. Nach Veröffentlichung der Warnmeldung des LKA BW meldeten sich weitere Firmen bei der ZAC und teilten mit, dass auch ihr Unternehmen von der Betrugsmasche betroffen sei. In einigen Fällen konnten durch die Hinweise Schäden in Millionenhöhe verhindert werden. Für die kleinen und mittelständischen Unternehmen aus der Region sind die beiden oben genannten Kriminalitätsphänomene nicht selten existenzgefährdend.

Von: Gustav.Geschäftsführer@firma.de <Gustav.Geschäftsführer@presidency.com>
An: Otto Opfer

KOOPERATIONEN

Die rasante Entwicklung der Informationstechnologie 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

Public Private Partnerships:
Mit der Sicherheitskooperation Cybercrime ist ein leistungsstarkes Bündnis zwischen Unternehmen der IT-Branche und Strafverfolgungsbehörden entstanden. (Michael Bartsch)

Michael Bartsch, Vorsitzender Arbeitskreis Öffentliche Sicherheit und Mitbegründer der Sicherheitskooperation Cybercrime, Quelle M. Bartsch

Hervorzuheben ist die Sicherheitskooperation Cybercrime, welcher das LKA BW im Jahr 2013 beigetreten ist. Zusammen mit dem Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) und den Landeskriminalämtern Niedersachsen, Nordrhein-Westfalen, 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 2015 auf der CeBIT in Hannover, der weltweit größten Messe für Informationstechnik, als Aussteller vertreten. 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, Forschung und Wissenschaft zur Verfügung. Ein weiterer wesentlicher Bestandteil der Arbeit der Initiative ist die Förderung des Erfahrungsaustausches unter den Teilnehmern. Derzeit beteiligen sich 1553 teilnehmende Institutionen, über 95 aktive Partner und mehr als 43 Multiplikatoren an der Allianz (Stand: Februar 2016). Das Landeskriminalamt Baden-Württemberg fungiert als Multiplikator und erhält so ausführliche Informationen zu aktuellen Cyber-Bedrohungen, die an die jeweiligen Bedarfsträger weitergegeben werden.

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

HOCHSCHULE ALBSTADT-SIGMARINGEN

„Die Zusammenarbeit von LKA BW und den Partner-Hochschulen ergibt ein akademisch fundiertes und gleichzeitig praxistaugliches Weiterbildungsangebot.“ (Prof. Dr. Rieger)

Prof. Dr. Rieger ist Studiendekan der Fachrichtung Digitale Forensik und Leiter des Open C³S Zertifikats-Programmes

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 Polizeibeamte haben das Studienangebot im Nebenamt in Anspruch genommen und sich, ohne dass hierfür von Seiten des Landes eine Kostenerstattung erfolgen konnte, weitergebildet. Neben dem konsekutiven 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.

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 acht Wochen pro Modul

Jahresbericht 2015
Cybercrime/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
Internet www.lka-bw.de

Ansprechpartner für Fachfragen
Zentrale Ansprechstelle Cybercrime,
Führungsgruppe 500
Name Jürgen Fauth
Telefon 0711 5401-2444
E-Mail stuttgart.lka.abt5.fuegr@polizei.bwl.de

Ermittlungen/Auswertung Cybercrime
Inspektion 510
Name Frank Winterhalter
Telefon 0711 5401-2510
E-Mail stuttgart.lka.abt5.i510@polizei.bwl.de

IT-Beweissicherung/Analyse Strukturierter
Massendaten, Inspektion 520
Name Martin Lühning
Telefon 0711 5401-2520
E-Mail stuttgart.lka.abt5.i520@polizei.bwl.de

TKÜ-Zentrum, Inspektion 530
Name Claus-Dieter Schiemann
Telefon 0711 5401-2530
E-Mail stuttgart.lka.abt5.i530@polizei.bwl.de

Projektleitung
Klaus Ziwey, Vizepräsident

Projektkoordination
Axel Mögelin, Natalie Meidl,
Stabsbereich Grundsatz, Gremien,
Geheimschutz

Inhalt
Reinhard Tencz, Jürgen Fauth, Stefan Reinhard,
Cybercrime/Digitale Spuren, Abteilung 5

Konzept und Gestaltung
Liane Köhnlein
Stabsstelle Öffentlichkeitsarbeit

Druck
e.kurz + co Druck und Medientechnik GmbH,
Stuttgart

350.000 NEUE SCHADSOFTWARE-VARIANTEN PRO TAG

Baden-Württemberg

LANDESKRIMINALAMT