Magazinreihe

Moderne POLIZEI

3/2019

► Die Cyber-Polizei: Innovationen – Sharing – Tools

ISSN 2626-3823

Behörden Spiegel-Gruppe

bechtle.com

Bei Sicherheit geht es immer ums Ganze.

Mit einem eigenen Geschäftsbereich richtet Bechtle seit Jahren den Blick gezielt auf den Public Sector. Wir suchen aktiv den Dialog, um den Wandel der Aufgaben und Anforderungen umfassendzu verstehen und unser Angebot entsprechend anzupassen. Ein permanenter Prozess, mit dem wir als Technologiepartner ganz nah an unseren Kunden dran sind. Dass wir die besonderen Spielregeln des Public Sector Business verstehen, ist für Bechtle ebenso ein Vorteil wie unsere flexible und flächendeckende Präsenz vor Ort – optimal kombiniert mit der zentralen Stärke eines internationalen IT-Konzerns. Impulse setzen außerdem unsere Business-Architekten, die sich speziell auf die Anforderungen der öffentlichen Verwaltung konzentrieren und den Blick fürs große Ganze haben: Von der Analyse der bestehenden IT-Landschaft bis zur langfristigen Strategieplanung ebnen sie mithilfe einer modernen und zukunftsorientierten IT den Weg. Sie setzen heute um, was auch morgen noch Bestand hat. Denn: Als IT-Partner des öffentlichen Sektors.

Wer die besonderen Anforderungen öffentlicher Auftraggeber erfüllen will, muss sie verstehen. Dazu gehört, über den eigenen Horizont hinauszuschauen. Vernetzt, mit klarem Fokus auf die Zielgruppe, die Zukunft immer im Blick. Auch deshalb ist Bechtle anerkannter Partner öffentlicher Auftraggeber.

Denn Technologie verändert sich und mit ihr die Ansprüche der Polizeibehörden. Um hohe Ziele zu erreichen, brauchen die Polizeibehörden einen Partner, der IT als Erfolgsfaktor versteht. Einen Dienstleister, der herstellerunabhängig moderne, sichere und effiziente Lösungen anbietet. Der für traditionelle Werte wie Bodenhaftung, Beharrlichkeit, Zuverlässigkeit und Begeisterungsfähigkeit ebenso steht wie für zukunftsstarke IT. Und dabei nie den Blick fürs Ganze verliert.

Unsere mehr als 300 Consultants und Experten unterstützen die Polizeibehörden in allen Themen der Cybersecurity und Compliance.

- Application Security
- Cloud Security
- Cyber Crime & Defence
- Datacenter Security
- Datenschutz & Informationssicherheit
- Infrastruktur & Perimeter Security
- Workplace Security

Als einer der weltweit führenden Anbieter von IT-Sicherheit verfolgt Trend Micro mit Leidenschaft das Ziel, eine sichere Welt für den digitalen Datenaustausch zu schaffen – heute und in Zukunft. Unsere innovativen Lösungen für Privatanwender, Unternehmen und Behörden bieten dank der XGen™ Sicherheitsstrategie vernetzten Schutz für Rechenzentren, Cloud-Workloads, Netzwerke und Endpunkte. Unsere Connected Threat Defense ermöglicht das nahtlose Teilen von Bedrohungsinformationen und bietet zentrale Transparenz und Kontrolle, um Organisationen bestmöglich zu schützen.

Mit über 6.500 Mitarbeitern in 50 Ländern und der weltweit fortschrittlichsten Erforschung und Auswertung globaler Cyberbedrohungen bietet Trend Micro Schutz für eine vernetzte Welt.





Inhalt

CYBER-POLIZEI – INNOVATIONEN

CYBER-POLIZEI – SHARING

CYBER-POLIZEI – TOOLS

Impressum

Dieses Magazin wird von der Behörden Spiegel-Gruppe, ProPress Verlagsgesellschaft mbH Bonn/Berlin, verlegt.
Herausgeber: Uwe Proll
Redaktionelle Leitung: Marco Feldmann, Benjamin Stiebel
Autoren: Peter Beuth, Dr. Julia Bussweiler, Markus Eisenbraun, Mario Foth, Dr. Julia Fricke, Thilo Gottschalk, Alexander Hahn, Helge Hinrichs, Mario Huber, Dr. Christian Hummert, Rainer Kasecker, Dirk Kunze, Prof. Dr. Dirk Labudde, Franziska Ludewig, Thomas-Gabriel Rüdiger, Alexander Seger, Manuela Siegemund, Steven Wilson
Verlagshaus Bonn: Friedrich-Ebert-Allee 57, D-53113 Bonn, Telefon: +49/228/970970, Fax: +49/228/97097-75
Hauptstadtbüro Berlin: Kaskelstr. 41, D-10317 Berlin, Telefon: +49/30/557412-0, Fax: +49/30/557412-57
E-Mail: verlag@behoerdenspiegel.de
Layout und Herstellung: Spree Service- und Beratungsgesellschaft m.b.H., Susan Wedemeyer
Druck: Heider Druck GmbH, Bergisch Gladbach
Fotos: stock.adobe.com
Titelfoto: © jijomathai, stock.adobe.com
Schutzgebühr: 5 €

Sehr geehrte Leserinnen und Leser,

► Uwe Proll, Chefredakteur und Herausgeber des Behörden Spiegel

Foto: Nicole Schnittfincke

auf die Polizeibehörden und die einzelnen Beamten und Beamtinnen kommen vielfältige neue Herausforderungen zu. Die "Moderne Polizei" muss über zahlreiche Fähigkeiten und Kenntnisse verfügen, um Sicherheit und Ordnung zu gewährleisten sowie Straftaten effizient zu verfolgen. Schon längst verlagern sich Teile der Kriminalität einerseits, aber auch der polizeilichen Arbeit andererseits in den digitalen Raum. Technisches Know-how wird daher eine immer größere Rolle im Kompetenzprofil spielen. Ein geschätzter jährlicher Schaden von über 50 Milliarden Euro allein in der deutschen Wirtschaft macht es deutlich: Datendiebstahl, -sabotage und -spionage gehören zu den größten Gefahren für die öffentliche Sicherheit. Auch einzelne Bürger und Bürgerinnen sind immer wieder von Schadsoftware, Identitätsdiebstahl oder Betrugsmaschen im Netz betroffen. Neben der Cyber-Kriminalität im engeren Sinn erleichtert das Internet als Tatmittel auch den Handel mit illegalen Gütern wie Drogen und die Verbreitung von Kinderpornografie.

Die Bekämpfung von Internet-Kriminalität muss daher hohe Priorität haben. Ermittlungen bei Straftaten, die im Wesentlichen im digitalen Raum stattfinden, stellen den Cyber-Polizisten vor große Schwierigkeiten. Anders als Zuständigkeiten und Kompetenzen von Polizeibehörden machen Cyber-Kriminelle nicht an Landesgrenzen Halt. Mittel zur Anonymisierung und Verschlüsselung schaffen zusätzliche Hürden bei der Verfolgung. In Teilen hinken die Übertragung etablierter Befugnisse in die digitale Welt und die Schaffung neuer erforderlicher Rechtsmittel dem technischen Wandel hinterher.

Auch in Bezug auf die konkreten technischen Kompetenzen muss die "Moderne Polizei" mit schnellen Innovationszyklen und ständig angepassten Tools und Methoden aufseiten der Angreifer mithalten können. Die Ausbildung, vor allem aber die Fort- und Weiterbildung von Cyber-Polizisten muss ausgebaut werden. Ohne die Rekrutierung von IT-Spezialisten mit nicht-polizeilichem Hintergrund wird der Bedarf aber nicht zu decken sein. Um den Öffentlichen Dienst für die begehrten Fachkräfte attraktiver zu gestalten, muss noch stärker als bisher über flexiblere Laufbahnen und Zulagen nachgedacht werden.

Dafür und für eine zeitgemäße technische Ausstattung der Polizei muss der Staat die nötigen Ressourcen aufbringen. Nicht nur bei der Bekämpfung von Cyber-Kriminalität, sondern bei der Verfolgung von praktisch allen Straftaten spielen digitale Spuren eine immer größere Rolle. Der Zugriff auf womöglich verschlüsselte Kommunikation und Daten sowie die effiziente Auswertung unstrukturierter Daten erfordern eine moderne Ausstattung auf dem Stand der Technik. Nur so wird die Polizei ihre Aufgaben in einer zunehmend digitalen Welt effizient erfüllen können.

Klar ist aber: Nicht jede Polizeidienststelle wird das gesamte Spektrum der digitalen Polizeiarbeit abdecken können. An zentralen Kompetenzzentren, wie sie in einigen Ländern bereits eingerichtet sind, und an Kooperationen zwischen den Polizeibehörden, aber auch mit Wissenschaft und Wirtschaft führt kein Weg vorbei. Die vorliegende Ausgabe unserer Magazinreihe "Moderne Polizei" beinhaltet Beiträge von Experten aus Polizeibehörden, Politik und Wissenschaft. Beleuchtet werden aktuelle und zukünftige Herausforderungen für die Cyber-Polizei sowie Lösungsansätze zu Kompetenzaufbau, Personalgewinnung, Ausstattung und Zusammenarbeit. Eine interessante Lektüre wünscht Ihnen

Ihr
Uwe Proll

Neue Impulse gegen Cyber-Kriminelle

► Peter Beuth, Innenminister Hessens

Die Anforderungen an die Sicherheitsbehörden haben im Zuge der fortschreitenden Globalisierung und Digitalisierung in den letzten Jahren stetig zugenommen. Cyber-Kriminelle, Extremisten und Gefährder haben längst die Möglichkeiten der Digitalisierung für sich entdeckt. Neue, zuvor nicht dagewesene Kriminalitätsphänomene wie Doxxing, Cyber-Grooming und Ransomware, aber auch die Vorbereitung von staatsgefährdenden Straftaten, digitale Spionage und Sabotage kamen hinzu und stellen die Ermittler vor immer neue Herausforderungen.

Seitens der Sicherheitsbehörden sind neue Strategien erforderlich, um angemessen reagieren zu können und zukunftsorientiert aufgestellt zu sein. Hessen hat frühzeitig auf diese neuen Herausforderungen reagiert. Bereits 2007 wurden landesweit bei allen Polizeipräsidien und dem Hessischen Landeskriminalamt Internetkommissariate eingerichtet. Neben Stellen für Ermittlungsbeamte wurden auch Stellen für Informatiker geschaffen, die seitdem zusammen mit den Ermittlern Cyber-Kriminalität effektiv bekämpfen. Begleitend wurde der Bereich der polizeilichen Prävention gestärkt. In den Beratungsstellen wurden Cyber-Berater als Ansprechpartner für den Bürger installiert.

Im Zuge der sich verschärfenden Sicherheitslage durch die Anschläge in Madrid, Paris oder Berlin sowie durch die allgemein zunehmende Terrorgefahr extremistischer Organisationen wurde darüber hinaus eine Weiterentwicklung der Cyber-Strategie des Landes notwendig. Aus diesem Grund haben wir jetzt ein eigenes "Cyber Competence Center" (Hessen3C) eröffnet. Eine Denkfabrik, die als zentrale Kompetenzstelle die Anstrengungen aller hessischen Behörden, der Verwaltung und Wissenschaft im Kampf gegen Cyber-Kriminelle bündelt. Ziel von Hessen3C ist es, Bedrohungen aus dem Netz durch Ausnutzung von Synergieeffekten effizienter und wesentlich schneller zu begegnen.

Weiterer Aufwuchs bis 2021

Bei Hessen3C arbeiten bereits derzeit 20 IT-Experten aus der Verwaltung, der Polizei sowie dem Verfassungsschutz. Die Spezialisten unterstützen auch hessische Städte und Gemeinden, sind zentrale Ansprechpartner für Unternehmen der Kritischen Infrastrukturen (KRITIS) und bieten darüber hinaus auch kleinen und mittleren Betrieben ihr Know-how an. Noch bis Ende dieses Jahres soll der Personalbestand auf etwa 50, bis Ende 2021 auf bis zu 100 Beschäftigte anwachsen.


Foto: HMdIS

Das Alleinstellungsmerkmal des Hessen3C ist die Bündelung in den Bereichen Cyber Security, Cyber Intelligence und Cyber Crime. Der durch die Einrichtung neu geschaffene regelmäßige Lageaustausch ermöglicht es, Schwachstellen, Angriffe und aktuelle Kriminalitätsphänomene im Cyber-Bereich umfassend zu bewerten sowie zielgerichtete und abgestimmte Maßnahmen einzuleiten. Mit der Einrichtung eines Organisationsbereiches Cyber Crime reagiert das Hessen3C auf die vielschichtigen Herausforderungen durch neue Kriminalitätsphänomene und gibt frühzeitig Impulse zur Unterstützung bei der Bekämpfung von Cyber-Kriminalität.

Ohne Verzahnung geht es nicht

Eine enge Verzahnung mit dem Landespolizeipräsidium sowie eine stetige Abstimmung mit dem Landeskriminalamt, dem Bundeskriminalamt (BKA), der Generalstaatsanwaltschaft Frankfurt am Main und anderen Sicherheitsbehörden sind dabei unerlässlich. Die gemeinsame, regelmäßige Lagebesprechung trägt zu einem deutlichen Qualitätsgewinn des Lagebildanteils Cyber Crime bei. Bereits heute erfolgt eine Unterstützung der Polizeibehörden durch fachliche Beratungen und Informationssammlung. Durch die Weiterentwicklung des Bereichs Cyber Crime wird zeitnah die fachliche Beratung um die technische Unterstützung in komplexen Ermittlungsverfahren erweitert. Darüber hinaus werden zukünftig effektive Werkzeuge zur Bekämpfung von Cyber Crime, insbesondere im Umfeld der digitalen Forensik und der Auswertung von Massendaten bereitgestellt.

Bei Aus- und Fortbildung von Polizeianwärtern und -anwärterinnen sowie Bediensteten im polizeilichen Einzeldienst nimmt die Unterstützung der Polizeibehörden bei der Vermittlung von Fachwissen einen künftigen Schwerpunkt ein. Mit der Errichtung von Hessen3C sind unsere Behörden gut aufgestellt, um bei der Bewältigung der Cyber-Herausforderungen von morgen bestehen zu können.

"ZIEL VON HESSEN3C IST ES, BEDROHUNGEN AUS DEM NETZ DURCH AUSNUTZUNG VON SYNERGIEEFFEKTEN EFFIZIENTER UND WESENTLICH SCHNELLER ZU BEGEGNEN."

Voraussetzungen früh geschaffen

► Mario Huber, Leiter des Dezernats 54 – Cyber Crime – im Bayerischen Landeskriminalamt

Beim Bayerischen Landeskriminalamt wurde – wie bereits zuvor bei mehreren anderen Landeskriminalämtern – im Jahr 2014 ein eigenes Fachdezernat zur Bekämpfung von Cyber Crime gegründet. In der Informationstechnologie markiert ein Zeitraum von fünf Jahren eine ganze Generation von Geräten und Anwendungen. Zeit für eine Rückschau und Bestandsaufnahme.

Durch die Einführung einer beamtenrechtlichen Laufbahn mit der Bezeichnung "Technischer Computer- und Internetkriminaldienst" waren bei der Bayerischen Polizei bereits im Jahr 2011 die Voraussetzungen für den Quereinstieg von Hochschulabsolventen der Fachrichtung Informatik in den polizeilichen Vollzugsdienst geschaffen worden.

Von dieser Möglichkeit wurde beim Aufbau der neuen Organisationseinheit umfangreich Gebrauch gemacht, sodass aktuell knapp die Hälfte der circa 50 beim Dezernat Cyber Crime tätigen Kolleginnen und Kollegen dieser Laufbahn angehören.

Viel Präventionsarbeit

Der mittlerweile am deutlichsten spürbare Unterschied zur kriminalpolizeilichen Arbeit in anderen Deliktsbereichen zeigt sich beim Dezernat Cyber Crime in dem hohen Zeit- und Personalanteil, der für deliktsspezifische Präventionsberatungen aufgewendet wird. Hierfür gibt es verschiedene Gründe: Zum einen ist im Deliktsbereich Cyber Crime die Zielgruppe in besonderem Maße für Präventionsberatungen empfänglich. Es rückt immer mehr ins öffentliche Bewusstsein, dass im heutigen Internetzeitalter nahezu jeder Mensch zu praktisch jeder Zeit Opfer einer Cyber-Attacke werden kann.

Darüber hinaus können Cyber-Angriffe, die sich gegen Behörden, Institutionen und Unternehmen richten, ernste Bedrohungen zum Beispiel für die öffentliche Gesundheits- oder Energieversorgung und somit für die öffentliche Sicherheit darstellen. Hieraus erwächst ein besonderes staatliches Interesse an einer intensiven und breit angelegten Vermittlung von Präventionswissen.

ZAC in enger Abstimmung

Mit dem Ziel einer möglichst professionellen und effektiven Aufklärung über einschlägige Vorbeugungs- und Interventionsmaßnahmen wurde deshalb beim Bayerischen Landeskriminalamt eine "Zentrale Ansprechstelle Cybercrime" (ZAC) eingerichtet, die Unternehmen, Behörden und sonstigen Institutionen als polizeilicher Single Point of Contact für phänomenspezifische Beratungen und als Vermittlungsstelle zu anderen Sicherheitsbehörden zur Verfügung steht.


Foto: Bayerisches Landeskriminalamt

Diese Aktivitäten der ZAC werden regelmäßig mit benachbarten Behörden, so etwa mit dem Landesamt für Sicherheit in der Informationstechnik (LSI) oder mit dem Cyber-Allianz-Zentrum (CAZ) des Bayerischen Landesamtes für Verfassungsschutz abgestimmt. Das CAZ bietet im Rahmen seiner Zuständigkeit für Wirtschaftsschutz ebenfalls Präventionsberatungen für Unternehmen an.

Keine Dopplung, sondern Synergiegewinn

Diese Zuständigkeitsregelung, die bei oberflächlicher Betrachtung als Aufgabendopplung wahrgenommen werden könnte, stellt sich in der Praxis als wertvoller Synergiegewinn dar. Durch möglichst genau auf die Zielgruppe abgestimmte Beratungsinhalte können nämlich die jeweiligen aufgabenspezifischen Vorteile der beiden Behörden, insbesondere die nicht von einer Strafverfolgungspflicht eingeschränkte Möglichkeit einer umfassenden Vertraulichkeitszusage durch den Verfassungsschutz und die ausschließlich der Polizei zur Verfügung stehenden präventiven und strafprozessualen Eingriffsbefugnisse, zu einem effektiven und schlagkräftigen Maßnahmenbündel kombiniert werden. Selbstredend werden dabei das verfassungsrechtliche Trennungsgebot sowie Aspekte des Daten- und Geheimschutzes beachtet, indem Sachverhalte bei Bedarf entsprechend abstrahiert beziehungsweise anonymisiert werden.

"DER MITTLERWEILE AM DEUTLICHSTEN SPÜRBARE UNTERSCHIED ZUR KRIMINALPOLIZEILICHEN ARBEIT IN ANDEREN DELIKTSBEREICHEN ZEIGT SICH BEIM DEZERNAT CYBER CRIME IN DEM HOHEN ZEIT- UND PERSONALANTEIL, DER FÜR DELIKTSSPEZIFISCHE PRÄVENTIONSBERATUNGEN AUFGEWENDET WIRD."

Diese intensiven Präventionsmaßnahmen stellen in Kombination mit der regelmäßigen Durchführung von ausgewählten Cyber Crime-Ermittlungsverfahren die Grundstrategie dar, mit der das Bayerische Landeskriminalamt aktuell und in Zukunft im Zusammenwirken mit anderen Sicherheitsbehörden der zunehmenden Bedrohung durch Cyber Crime entgegentritt.

Große Hilfe für Ermittler

Mobilgeräte-Forensik bei Ermittlungen in Kindesmissbrauchsfällen

► Gerhard Gunst, Regional Area Sales Manager DACH, MSAB

Millionen von Kindern werden jedes Jahr sexuell ausgebeutet und die Zahl der Opfer nimmt stetig zu. Strafverfolgungsbehörden weltweit arbeiten intensiv daran, das Ausmaß des Kindesmissbrauchs zu verringern. Sie können einige Fortschritte vorweisen, aber die Herausforderungen – wie die immensen zu analysierenden Datenmengen, einschließlich Bildern und Videos – sind gewaltig.

Für erfolgreiche Aufklärungsarbeit bei Verbrechen gegen Kinder ist es von entscheidender Bedeutung, schnelle, effektive und bezahlbare Funktionen der Mobilgeräte-Forensik nutzen zu können. Die in solchen Ermittlungen verwendeten Beweise finden sich heute mehr und mehr auf Mobiltelefonen und Online-Apps statt wie zuvor auf PCs und Laptops. Mithilfe beliebter Apps können Benutzer MMS-artige Nachrichten mit Fotos, Videos und Zeichnungen als Anhang versenden. Die Kommunikation erfolgt über den Datenpfad, sodass Nachrichteninhalte nicht in den Datensätzen der Gesprächsdetails des Anbieters aufgezeichnet werden, was Ermittler vor große Probleme stellt.

Bei Ermittlungen in Kindesmissbrauchsfällen kann Mobilfunkgeräte-Forensik Ermittlern stark helfen.

Foto: ©bluetint, shutterstock.com

Zeitersparnis möglich

Software von MSAB, wie XRY und XAMN, hilft Ermittlern dabei, Zeit zu sparen und kann im Zusammenspiel mit der Project-VIC-Funktion dazu beitragen, indirekte Traumatisierungen der Ermittler zu vermeiden, die diese erleiden können, wenn sie sich die schrecklichen Bilder ansehen müssen. Wie tragen XRY und XAMN dazu bei, diese Herausforderungen zu meistern?

Die Inhaltserkennungsfunktion filtert automatisch sämtliche Fotos heraus, auf denen Menschen abgebildet sind, was eine enorme Zeitersparnis bedeutet.

Hash-Filter und Hash-Merklisten können genutzt werden, um Bilder herauszufiltern, die bereits als kinderpornografische Daten bekannt sind. Solche Bilder können entsprechend markiert und ausgeschlossen werden. Es ist dann nur noch erforderlich, die verbleibenden Bilder anzusehen und zu analysieren.

Wenn “neue” Bilder gefunden werden, können diese markiert, gehasht und im Project-VIC-Format exportiert werden. So können sie dann an andere Strafverfolgungsbehörden weitergegeben werden.

XRY ermöglicht Ermittlern eine superschnelle Verarbeitung von Bildern – bis zu 15 Mal schneller mit Computern mit CUDA-fähigen NVIDIA-Grafikprozessoren.

XAMN bietet Ermittlern die Möglichkeit, Daten aus unterschiedlichen Fällen in einer Ansicht zu betrachten – um Zusammenhänge zwischen Verdächtigen und Opfern zu finden.

Wenn ein Fall vor Gericht landet, können Ermittler, die XRY verwenden, auf ihr Beweismaterial vertrauen, weil dieses forensisch sicher ist und über ein verifiziertes Protokoll verfügt, über das sich die Rechtsgültigkeit digitaler Beweise nachweisen lässt.

Ein weiterer Grund dafür, dass sich die Produkte von MSAB so gut dazu eignen, um Delikte gegen Kinder zu untersuchen: Unter den Angestellten von MSAB finden sich viele ehemalige Mitarbeiter der Strafverfolgungsbehörden, die über langjährige Ermittlungserfahrungen im Bereich Kindesmissbrauch verfügen. Sie haben uns geholfen, die richtigen technischen Lösungen zu entwerfen, um die damit verbundenen Probleme anzugehen.

MSAB

Auf welcher Seite sitzen die Profis?

► Markus Eisenbraun, Leiter Abteilung 5, “Cybercrime und Digitale Spuren”, im Landeskriminalamt Baden-Württemberg


Foto: privat

Auf welcher Seite sitzen die Profis? Sind es die Hacker mit ihren dunklen Hoodies, die tage- und nächtelang vor ihren grünen Zahlenkolonnen sitzen? Sind die IT-Systeme von Unternehmen so unüberwindbar wie früher die chinesische Mauer? Oder bringen die Cyber Cops Licht in das Darknet?

Es ist Anfang April 2018 und der dritte Arbeitstag des neuen Leiters der Abteilung “Cybercrime und Digitale Spuren” im Landeskriminalamt Baden-Württemberg. Er ist gerade vom landesinternen IT-Dienstleister zurück in die Polizei gewechselt und schon sind seine Erfahrungen als IT-Dienstleister und die Sicht der Ermittlungsbehörden gefragt. Ein Landesamt des Ministeriums für Ländlichen Raum und Verbraucherschutz meldet auf seinen Systemen bei einer routinemäßigen und automatisierten Prüfung einen nicht bekannten Dienst. Parallel dazu erhält das Landesamt Post: Ein Erpresser droht, die Schwachstelle publik zu machen und fordert für seine Diskretion Bitcoins. Umgehend tritt der landeseigene IT-Dienstleister auf den Plan, dieser prüft sämtliche Systeme und beauftragt zudem ein spezialisiertes IT-Systemhaus mit der Untersuchung und Wiederherstellung.

Exekutive als Teil des IT-Krisenmanagements

Die “Zentrale Ansprechstelle Cybercrime” (ZAC) beim Landeskriminalamt ruft sofort eine Task Force ins Leben. Die Spezialistinnen und Spezialisten der ZAC führen erste Maßnahmen in den Rechenzentren des Landesamtes und des IT-Dienstleisters durch. Sie analysieren Netzstrukturen, suchen nach Anomalien, sichern Logdateien und werten diese aus. Schnell ist das Ausmaß des Angriffs deutlich. Der Täter hat sich über Tage und Wochen Zugang ins Netz verschafft und seine Rechte immer weiter ausgeweitet. Eine Frage drängt sich auf: Besteht hier ein Zusammenhang mit den aktuellen Cyber-Angriffen eines russischen Nachrichtendienstes auf baden-württembergische Unternehmen, die Kritische Infrastruktur betreiben? Wie immer in solchen Fällen laufen die umfangreichen Ermittlungen sofort auf Hochtouren. Auch hier rufen die Expertinnen und Experten eine Task Force ins Leben. Diese schaut sich die technische Ebene, die Organisation, das Personal und die Sicherheitsmechanismen der betroffenen Unternehmen an. Relativ zügig finden sie die Schwachstelle.

Die Aufgabe einer Ermittlungsbehörde wie dem Landeskriminalamt Baden-Württemberg oder einer spezialisierten Kriminalpolizeiinspektion 5, die es in allen regionalen Präsidien flächendeckend im Land gibt, ist nicht nur die Ermittlung von Tätern. Vielmehr ist die Polizei immer auch Teil des sogenannten Incident Response, des IT-Krisenmanagements. Die Polizei schließt zwar keine Sicherheitslücken und stellt auch keine Systeme wieder her, aber die forensischen Erkenntnisse helfen den Betroffenen. Neben der Forensik sind aber auch die Eingriffsbefugnisse der Ermittlungsbehörden bei der Erforschung von Cyber-Attacken von großer Bedeutung. Denn Durchsuchungen oder Beschlagnahmen sind ein Alleinstellungsmerkmal der Exekutive. Diese und andere Instrumente wendet die Polizei nicht nur in der realen, sondern auch der digitalen Welt an. Ein echter Mehrwert, der aber auch anderen beziehungsweise potenziellen Betroffenen zugute kommt. Denn in der Regel wenden Tätergruppierungen ihren Modus Operandi nicht nur einmal an.

“DIE POLIZEI IST IMMER AUCH TEIL DES SOGENANNTEN INCIDENT RESPONSE, DES IT-KRISENMANAGEMENTS.”

Warum sollte ein erfolgreiches Geschäftsmodell nicht erneut die Kasse klingeln lassen? Dies ist einer von vielen Gründen, warum bei Cyber-Angriffen die Beteiligung der Ermittlungsbehörden beziehungsweise staatlicher Stellen so immens wichtig ist. Bislang ist es leider in der öffentlichen Diskussion oft so, dass den Betroffenen eine Mitschuld oder zumindest ein Makel anhaftet. Zur Wahrheit gehört aber auch: Einen hundertprozentigen Schutz gibt es nicht. Es kann prinzipiell jeden treffen und niemand sollte mit dem Finger auf andere zeigen. Es braucht vielmehr Transparenz und die Bereitschaft der Betroffenen, die Sachverhalte aufzuklären. Die Dinge unter den Teppich zu kehren, ist definitiv der falsche Weg. Wenn die Möglichkeit der Erforschung von Cyber-Angriffen besteht, können zukünftige verhindert werden.

Wissen und kriminelle Dienstleistungen im Netz

Im Falle des Landesamtes ging es sogar noch viel weiter: Die forensische Auswertung und die Ermittlungen führten zu einem 25-Jährigen aus der Region Stuttgart, der sich nach Feierabend als Freizeit-Hacker betätigte. Die Ermittlungen deckten auf, dass der junge Mann auch in die IT-Infrastruktur eines städtischen Energieversorgers eindringen konnte. Der 25-Jährige hatte keine

tiefgreifenden technischen Kenntnisse, sondern hat sich sein Wissen und die Werkzeuge größtenteils im Selbststudium beigebracht, überwiegend aus frei zugänglichen Quellen. Zum Glück arbeitet er nicht für einen Nachrichtendienst. Er wollte einfach mal sehen, was denn so möglich ist. Fraglich bleibt bis heute, ob ihm bewusst war, was er alles hätte anrichten können.

Es ist im Grunde unerheblich, wo die Profis sitzen. Kriminelle bieten im Darknet diverse Dienstleistungen – Stichwort "Cyber-Crime-as-a-Service" – an, somit ist es mit überschaubarem Aufwand und ohne fundierte IT-Kenntnisse möglich, eine Cyber-Attacke zu starten. Entscheidend ist, dass die Digitalisierung in allen Gesellschaftsbereichen weiter vordringt. Für die Unternehmen bedeutet dies, dass sie die entsprechenden Rahmenbedingungen schaffen müssen, damit der Wirtschaftsstandort Deutschland weiterhin seine Spitzenposition behält und so der Wohlstand gesichert bleibt. Die Digitalisierung bietet der Wirtschaft enorme Chancen, gleichzeitig schafft sie auch für Kriminelle neue Tätigkeitsfelder. Phänomene wie "Cyber-Crime-as-a-Service" und Verkaufsplattformen im sogenannten Darknet lassen dies erahnen.

Neue Ansätze gefragt

Für Ermittlungsbehörden kann das nur bedeuten, diesen Weg mitzugehen und die eigene Digitalisierung zu forcieren. Damit ist nicht nur Smart Policing gemeint. Es bedarf nicht nur einiger Cyber Cops. Die Digitalisierung aller Lebensbereiche bedarf des Ermittlers 4.0, denn Kriminalistinnen und Kriminalisten müssen die Zusammenhänge verstehen, brauchen profundes technisches Wissen, das bereits während der Ausbildung vermittelt werden muss. Die digitalen Spuren bieten nicht nur neue Möglichkeiten und Ermittlungsansätze, es gibt bereits jetzt Kriminalitätsbereiche, die ausschließlich digital sind. Wir können es uns nicht leisten, diese Kriminalität nur zaghaft zu bekämpfen beziehungsweise dieser Entwicklung hinterherzulaufen.

Grundrechtskonforme Datenverarbeitung mit TITANIUM

► Thilo Gottschalk, Legal Research Associate am Zentrum für Angewandte Rechtswissenschaft (ZAR) des Karlsruher Instituts für Technologie (KIT)


Foto: privat

Cyber-Kriminalität ist in all ihren Facetten steter Weiterentwicklung unterlegen. Diese Entwicklung ist unvermeidbar und reflektiert gleichzeitig den Wettlauf zwischen Strafverfolgung und kriminellen Aktivitäten. Dabei müssen sich Ermittler den neuen technologischen Herausforderungen und Gegebenheiten stets anpassen. Das gilt für die Effektivität der Ermittlung gleichermaßen wie für die Wahrung der Grundrechte der Betroffenen. Die Vereinbarkeit dieser beiden Ziele wirft im Zeitalter von Big Data, KI und OSINT drängende Rechtsfragen auf, welche schon bei der Entwicklung neuer Analysemethoden und Softwarelösungen zu berücksichtigen sind.

Ermittlungen im Bereich des Darknets und von Kryptowährungen sind momentan sehr zeitaufwendig oder aber mit rechtlichen Anforderungen schwer vereinbar. Ein Mangel an polizeiintern verfügbaren Lösungen führt dazu, dass Analysen häufig extern vorgenommen werden müssen. Die Kooperation mit privaten Analyseanbietern birgt jedoch nicht selten die Gefahr einer fragwürdigen Ausweitung der Ermittlungsbefugnisse, während die faktischen Kontrollmöglichkeiten der Datenverarbeitungsprozesse zudem häufig stark eingeschränkt sind.

Brücke zwischen Recht und Technik

In diesem Spannungsfeld entwickelt das EU-Projekt TITANIUM eine mögliche Alternative. 15 Partner aus ganz Europa entwickeln in einem interdisziplinären Team Software zur rechtskonformen Analyse von öffentlich verfügbaren Darknet-Inhalten sowie Kryptowährungen unter Wahrung der Grundrechte der Betroffenen. Die Tools ermöglichen unter anderem eine gezielte Suche nach relevanten Informationen im Darknet und die Verknüpfung der Ergebnisse mit der Analyse von Kryptowährungen. So können Transaktionen einzelnen Entitäten zugeordnet und damit wertvolle Ansätze zur Identifikation von Verdächtigen generiert werden. Die Datenverarbeitung ist dabei so gestaltet, dass damit einhergehende Grundrechtseingriffe möglichst gering ausfallen, um strikten rechtlichen Anforderungen zu genügen. Das Forschungsteam um Prof. Dr. Franziska Boehm am Zentrum für Angewandte Rechtswissenschaft (ZAR) des Karlsruher Instituts für Technologie (KIT) leitet dabei federführend die Erforschung der rechtlichen Rahmenbedingungen und legt so den Grundstein für eine nachhaltig rechtskonforme Softwareentwicklung.

Die Verarbeitung personenbezogener Daten – auch bei öffentlicher Verfügbarkeit – stellt grundsätzlich einen Grundrechtseingriff dar. Die Verarbeitung muss also möglichst gezielt und effektiv stattfinden. In TITANIUM werden dafür Algorithmen so trainiert, dass sie relevante Strukturen und Inhalte erkennen und irrelevante Inhalte aus der Datenverarbeitung ausschließen können. Welche Inhalte relevant sind, kann bereits vor der Datenverarbeitung definiert und so der Grundrechtseingriff minimiert werden. Die Stellschrauben der Datenverarbeitung sollen dabei aber flexibel sein, sodass sie den nationalen Vorgaben und Verfahrensumständen entsprechend angepasst werden können. Gleichzeitig müssen hinreichende Sicherheitsmaßnahmen implementiert sein, die eine Einhaltung gesetzlicher Grenzen auch auf technischer Ebene garantieren. Beispielsweise helfen umfangreiche Logs dabei, die rechtskonforme Nutzung der Tools nachweisbar zu machen, aber auch den Beweiswert der Ergebnisse durch Reproduzierbarkeit zu erhalten.

“DIE VERARBEITUNG PERSONENBEZOGENER DATEN – AUCH BEI ÖFFENTLICHER VERFÜGBARKEIT – STELLT GRUNDSÄTZLICH EINEN GRUNDRECHTSEINGRIFF DAR. DIE VERARBEITUNG MUSS ALSO MÖGLICHST GEZIELT UND EFFEKTIV STATTFINDEN.”

Kryptowährungen im Fokus

Auch der zweite Schwerpunkt, die Analyse von Kryptowährungen, sieht sich durch die Weiterentwicklungen der zugrundeliegenden Blockchain-Protokolle immer neuen Herausforderungen ausgesetzt. Längst geht es nicht mehr nur um Bitcoin, sondern

insbesondere um Kryptowährungen wie Monero oder ZCash, welche einen stärkeren Fokus auf Anonymisierung legen und somit offenkundig auch Vorteile für kriminelle Transaktionen versprechen. Sog. Cross-Chain-Transaktionen erschweren die Analyse zusätzlich. Der Wechsel zwischen Währungen muss in diesen Fällen in die Analyse mit einbezogen und die Eigenheiten der jeweiligen Blockchain berücksichtigt werden. Im Ergebnis können so beispielsweise Adressen einzelnen Entitäten zugeordnet (Clustering) oder der kürzeste Pfad bis zur Auszahlung nachvollzogen werden (Shortest-Path-Algorithm). TITANIUM hat dabei bereits jetzt aufgezeigt, dass viele Währungen längst nicht so anonym sind, wie sie es versprechen.

Neue Analyseverfahren bieten dabei allerdings keine absolute Sicherheit und müssen hinsichtlich ihres Beweiswertes stets differenziert betrachtet werden. In diesem Kontext erforscht das ZAR auch die beweisrechtlichen Anforderungen an neuartige Analysemethoden, damit diese im Strafprozess sinnvoll genutzt werden können. Erste Ergebnisse des Projekts werden seit dem 24. Januar 2019 bereits von Polizeibehörden aus Deutschland, Finnland, Spanien und Österreich getestet. Die Beteiligung des Bundeskriminalamtes und Interpol sowie weiterer Polizeibehörden zeigt sich dabei als enorm wichtig, um neben rechtlichen und technischen Anforderungen auch die nötigen Praxiserfahrungen in die Forschung und Entwicklung mit einfließen zu lassen.

Frühzeitig Kompetenzzentrum eingerichtet

► Dirk Kunze, Landeskriminalamt Nordrhein-Westfalen


Foto: privat

Die Veröffentlichung von persönlichen Daten von Personen des öffentlichen Lebens zu Beginn dieses Jahres hat die Bedeutung des Themas Sicherheit im digitalen Raum noch einmal besonders medienwirksam heraus gestellt. Cyber Crime und Cyber-Angriffe – auch auf Kritische Infrastrukturen (KRITIS) – sind spätestens seit den Warnungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) sowie des Bundesamtes für Verfassungsschutz (BfV) vor Angriffen auf deutsche Energieversorger im letzten Sommer nicht nur in der Presse, sondern auch in aller Munde.

Cyber Crime, Cyber-Terrorismus und Cyber-Spionage haben dabei eines gemeinsam: Am Anfang der Ermittlungen ist es oft schwierig, herauszufinden, welches Ziel der Angreifer verfolgt und woher er kommt – denn das Internet kennt keine geografischen Grenzen. Ebenso verhält es sich bei Straftaten, die das Internet lediglich als Tatmittel nutzen, wie dem Betrug. Viele Delikte, die im Strafgesetzbuch ursprünglich als analoge Tatbestandshandlungen (der Betrug in diesem Fall auf echtem Papier) erfasst wurden, finden heute digital statt. Das stellt die für Gefahrenabwehr und Strafverfolgung zuständigen Behörden vor neue Herausforderungen. Extrem kurze Innovationszyklen der Entwicklung neuer technischer Systeme und digitaler Hilfsmittel sind nur eine davon.

Cyber Crime ist kriminalstrategischer Schwerpunkt

Die Polizei in Nordrhein-Westfalen hat die Bekämpfung von Cyber Crime bereits 2011 als kriminalstrategischen Schwerpunkt verankert. Folgerichtig und frühzeitig hat sie beim Landeskriminalamt das Cybercrime-Kompetenzzentrum (CCCC) eingerichtet und damit eine Vorreiterrolle im Bundesgebiet eingenommen. Parallel wurde im Jahr 2012 die Zuständigkeit für die Bearbeitung von Cyber Crime-Delikten allen 47 Kreispolizeibehörden übertragen, entsprechendes Personal und Sachausstattungen zugewiesen.

Schon damals hat sich gezeigt, dass eine breite Ausbildung von Kompetenzen der kriminalpolizeilichen Sachbearbeitung notwendig ist, um das Phänomen Cyber Crime zu bewältigen. Gleichzeitig wurde ein kaskadierendes System geschaffen, in dem größere Behörden umfangreichere und komplexere Verfahren übernehmen. Die sechs großen Polizeipräsidien Bielefeld, Dortmund, Düsseldorf, Essen, Köln und Münster nehmen dabei als Kriminalhauptstellen noch einmal eine besondere Stellung ein. Ihnen obliegt die Kompetenz zur Bearbeitung herausgehobener Sachverhalte im Bereich des Cyber Crime. Gut aus- und fortgebildete Ermittler und Beratungsteams vor Ort sollen sicherstellen, dass die Cyber Crime-Delikte orts- und zeitnah bearbeitet und die Täter schneller ermittelt werden können.

Bündelung für besondere Sachverhalte

Das Landeskriminalamt Nordrhein-Westfalen hat im CCCC die Kompetenzen für herausragende Sachverhalte, die eine besondere Bedeutung entfalten oder spezielle Ermittlungsmethoden erfordern, gebündelt. Häufig können Sachverhalte nicht mit Standardlösungen bearbeitet werden. Die Täter nutzen in der Regel alle Möglichkeiten des Internets: Sie verschlüsseln oder anonymisieren Daten oder entwickeln vollständig neue Begehungsformen (Modi Operandi), um digital Straftaten zu begehen. Hier kommt das Landeskriminalamt Nordrhein-Westfalen mit seinen Innovationen zum Zug – entweder um die Kreispolizeibehörden effektiv zu beraten und zu unterstützen oder um die Ermittlungen zu übernehmen.

Die Mitarbeiter im CCCC arbeiten jeden Tag daran, neue Modi Operandi frühzeitig zu erkennen, Erkenntnisse zusammenzutragen und Hinweise an die Kreispolizeibehörden und die Präventionsdienststellen weiterzugeben. Eine besondere Herausforderung stellt dabei das hohe Dunkelfeld von circa 90 Prozent der Straf-

“DIE POLIZEI IN NORDRHEIN-WESTFALEN HAT DIE BEKÄMPFUNG VON CYBER CRIME BEREITS 2011 ALS KRIMINALSTRATEGISCHEN SCHWERPUNKT VERANKERT.”

taten dar. Denn Trends und sich abwandelnde Begehungsweisen lassen sich so teilweise nur sehr schwer oder spät erkennen. Neue Auswerteansätze und Workshops in Zusammenarbeit mit dem Bundeskriminalamt (BKA) tragen dazu bei, neue Phänomene wesentlich schneller zu erkennen und diesen mit neu angepassten Bekämpfungsstrategien wirksam zu begegnen.

Gute Kooperation mit Justiz

Darüber hinaus stellt das nordrhein-westfälische Landeskriminalamt die Zentral- und Ansprechstelle Cybercrime für alle Behörden des Landes und den 24/7 Single Point of Contact für die Wirtschaft. Experten klassifizieren eingehende Meldungen und leiten Sofortmaßnahmen ein. Anschließend wird der Fall entweder in den Ermittlungskommissionen Cyber Crime des Landeskriminalamtes oder den Kreispolizeibehörden, gegebenenfalls mit Unterstützung des Landeskriminalamtes, bearbeitet.
Besonders positiv hat sich hier die Zusammenarbeit mit der Justiz entwickelt: Das fachlich zuständige Justizressort hat mit der Zentralen Ansprechstelle Cybercrime (ZAC NRW) bei der Staatsanwaltschaft Köln eine landesweit zuständige Stelle für alle Fragen der Bekämpfung von Cyber Crime-Delikten geschaffen. Damit ist auch nachts und am Wochenende ein konsequentes, sachkundiges und koordiniertes Vorgehen aller Strafverfolgungsbehörden in Nordrhein-Westfalen gewährleistet. Diese eng verzahnte und vertrauensvolle Zusammenarbeit bewährt sich auch bei der Übernahme durch eine der derzeit drei festen Ermittlungskommissionen des Landeskriminalamtes – hier sind technischer Fachverstand und kriminalistische Expertise zu einer Einheit geformt.

Auch aktive Fahndung im Internet

Das Cyber-Recherche- und Fahndungszentrum ist ein weiterer innovativer Zweig des CCCC. Es fahndet aktiv nach Straftaten im Internet wie Drogen- und Waffenhandel, politisch motivierter Kriminalität, Cyber Grooming oder der Verbreitung von Kinderpornografie. Mehrere Ermittlungsverfahren gegen Drogen- und Waffenhändler im Darknet wurden erfolgreich geführt. Außerdem verhinderten die Beschäftigten erfolgreich aktuelle Missbrauchsfälle oder trugen durch die schnellen und aktiv geführten Ermittlungen des Cyber-Recherche- und Fahndungszentrums dazu bei.
“Das Internet ist kein rechtsfreier Raum”, betonte jüngst der Direktor des nordrhein-westfälischen Landeskriminalamtes, Frank Hoever. “Mit dem Cyber-Recherche- und Fahndungszentrum gehen wir aktiv und konsequent gegen Straftaten im Internet, auch im Darknet, vor.” Nähere Einzelheiten dazu werden aus ermittlungstaktischer Sicht allerdings nicht verraten.
Besonderen Wert legt Hoever darauf, dass das Landeskriminalamt Triebfeder bei der Entwicklung neuer kriminalfachlicher Anwendungen ist. So führte das Landeskriminalamt bereits frühzeitig Tests mit Produkten Künstlicher Intelligenz (KI) durch. “Auch wenn wir für den kriminalpolizeilichen Einsatz derzeit kein Produkt favorisieren können, haben wir doch grundlegende Erkenntnisse für den Einsatz von KI-Produkten gewinnen können”, stellt Hans-Josef Lemper, Leiter des CCCC, fest. Umfassende Lösungen seien für den kriminalfachlichen Einsatz mit ständig wechselnden Fallkonstellationen nur sehr bedingt und mit unverhältnismäßig hohem Aufwand einsetzbar.

Dienststelle extra geschaffen

Eine eigens für diese Aufgaben geschaffene Dienststelle kümmert sich jetzt um Erprobung und Entwicklung potenziell geeigneter Werkzeuge. Auch die Entwicklung geeigneter Analysemethoden und Umgebungen sei bei den ständig wachsenden Datenbergen ein wesentlicher Punkt zur Effizienzsteigerung. “Die ausschließlich manuelle Auswertung von digitalen Asservaten ist nicht mehr zeitgemäß. Wir wollen die Sachbearbeiter im Land technisch unterstützen, damit sie möglichst viel Zeit auf die Ermittlungen verwenden können”, erklärt Jörg Schalk, Leiter der Landesarbeitsgruppe IT-Asservate. Unterstützt wird er dabei von den umfangreichen Erfahrungen, die die Forensiker bei der Sicherung und Aufbereitung digitaler Spuren haben. “Digitale Spuren sind die DNA der Zukunft”, betont Direktor Hoever. “Wir bearbeiten sie mit der gleichen Akribie und Sorgfalt wie Finger- oder DNA-Spuren.”
Die erfolgreiche Bekämpfung der Verbreitung von Kinderpornografie ist nicht nur Aufgabe des Cyber-Recherche- und Fahndungszentrums. Eine eigene “Zentrale Auswertestelle Kinderpornografie” analysiert gesicherte Daten und überprüft diese auf Ermittlungsansätze und Hinweise auf aktuelle Missbrauchsfälle. “Die Kolleginnen und Kollegen, die hier arbeiten, verdienen meinen allerhöchsten Respekt. Diese täglichen Belastungen stellen hohe Anforderungen an die Persönlichkeit, aber auch die Integrität der hier Arbeitenden”, stellt der Leiter, Sven Schneider, fest. “Einen aktuellen Missbrauch zu beenden und ein Kind oder Jugendlichen aus dieser Situation zu befreien, ist für uns der größte Lohn der Arbeit.”

Ohne Kooperation geht es nicht

Diese Aufgaben können weder das Landeskriminalamt noch die nordrhein-westfälische Polizei alleine bewältigen. Der ständige Austausch mit anderen Behörden sowie dem privaten Sektor und das gemeinsame, koordinierte Vorgehen in diesem anspruchsvollen Themenbereich sind Garanten erfolgreichen Arbeitens.
Nicht nur die Mitarbeit in der “Sicherheitskooperation Cybercrime”, in der neben dem Branchenverband Bitkom nunmehr sieben Landeskriminalämter vertreten sind oder die Zusammenarbeit mit den Verbänden “eco” und “Voice e. V.” stellen effektive und erfolgsbegünstigende Kooperationen mit der Wirtschaft dar. Die vertrauensvolle Zusammenarbeit mit der Zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZITiS), dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und allen Strafverfolgungsbehörden sind weitere wesentliche Erfolgsfaktoren. Als kompetente Netzwerkpartner des nordrhein-westfälischen Landeskriminalamtes tragen sie auch dazu bei, gemeinsam mit allen Beteiligten den Kampf gegen Cyber Crime erfolgreich fortzusetzen.

Spurensuche im Cyber Space

► Dr. Christian Hummert, Leiter Geschäftsfeld Digitale Forensik bei der Zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZITiS)


Foto: ZITiS

Im September 2016 findet die Polizei in Adelaide (Australien) die 57-jährige Myrna Nilsson tot in ihrer Wäschekammer. Die Verstorbene ist an einen Stuhl gefesselt und wurde offenbar erschlagen. Der Nachbar hatte kurz zuvor die Polizei gerufen, nachdem die aufgelöste Tochter der Toten ihn zu Hilfe gerufen hatte. Sie berichtet von einer Gruppe Männer, die ihrer Mutter in einem Pick-up gefolgt waren. Am Haus gibt es Einbruchspuren. Am 8. März 2018 wird die Tochter des Opfers dann selbst verhaftet und steht inzwischen vor Gericht. Was war geschehen? Myrna Nilsson trug zur Tatzeit eine Apple Watch. Das smarte Gerät hatte den Tathergang genau protokolliert. So zeigten die Aktivitäts- und Herzfrequenzmessungen erst eine erhöhte Aktivität und große Aufregung beim Opfer, dann ist genau der Moment zu erkennen, in dem die Frau zunächst bewusstlos wurde und schließlich starb. Sogar wie die Tote dann bewegt wurde, ist genau festgehalten. Die Daten in der Uhr haben die Aussagen der Tochter widerlegt und sie schlussendlich selbst schwer belastet.

Smart Devices dokumentieren unfreiwillig Straftaten

Einen solchen Fall gab es nicht nur im fernen Australien – auch bei dem Mord an einer Freiburger Studentin vom 15. Oktober 2016 ist eine Smartwatch ein entscheidendes Beweisstück. Der mutmaßliche Täter sagte vor Gericht aus, er habe die Studentin im Affekt getötet. Bei der Tat hatte diesmal jedoch der Täter eine Smartwatch getragen. Die Daten aus der Uhr belegen, dass er sich vor der Tat mehr als 90 Minuten lang in der Nähe des Tatorts aufgehalten hatte. Zudem zeigte die Gesundheits-App genau, wie er eine Böschung hinuntersteigt und sie mit weniger Anstrengung wieder hinaufsteigt. Hier hatte das smarte Gerät festgehalten, wie die tote Studentin in der Dreisam abgelegt wurde.
In beiden Fällen wurden die unscheinbaren kleinen Fitness-Tracker zu entscheidenden Beweistücken. Auch wenn es vielleicht nicht überrascht, dass eine Gesundheits-App Daten zum Gesundheitszustand oder zu Bewegungen einer Person speichert, ist es doch ungewöhnlich, dass solche Daten zu Beweisstücken in einem Gerichtsverfahren werden. Leider ist es auch nicht ganz einfach, die Daten aus solchen Geräten zu extrahieren. Es gibt hunderte verschiedene Hersteller, viele davon sitzen in China. Die Armbänder verfügen über keine genormte Schnittstelle und die Daten sind in keinem dokumentierten Format abgelegt.

Forensik verlagert sich in den Cyber Space

Die wissenschaftlich-technische Untersuchung von solchen Spuren, die bei kriminellen Handlungen zurückbleiben, ist der Inhalt von Forensik. In heutigen Zeiten verlagert sich Kriminalität jedoch immer mehr in den Cyber Space. Es gibt Straftaten, die sich ganz dort abspielen, wie der Austausch illegaler Daten im Darknet. Doch auch bei ganz gewöhnlichen analogen Straftaten, wie den beiden oben beschriebenen Fällen, können digitale Spuren eine große Rolle spielen.
Die Anzahl der Geräte, die mögliche Spuren sein können, ist jedoch immens und steigt jedes Jahr. Smartphones sind nahezu allgegenwärtig, in jedem Haushalt gibt es mindestens einen Computer, viele Haushalte verfügen über smarte Geräte oder Sprachassistenten, Fitness-Tracker sind verbreitet. Die digitale Forensik extrahiert die Daten aus solchen elektronischen Geräten und stellt die Daten dem Ermittler zur Verfügung.
Die zentrale Herausforderung der digitalen Forensik besteht vor allem im schnellen technischen Fortschritt im Bereich der Elektronik und in der Vielzahl der elektronischen Geräte. Auch sind die Geräte, wenn sie in der Forensik ankommen, nicht immer in einem optimalen Zustand. Häufig sind wichtige Daten gelöscht, es wurde versucht die Geräte zu zerstören, Daten sind verschlüsselt oder verborgen, die Geräte wurden wohlmöglich lange versteckt und sind nass geworden oder korrodiert.
Zu den Aufgaben der digitalen Forensik gehört das Auslesen der

“DIE ANZAHL DER GERÄTE, DIE MÖGLICHE SPUREN SEIN KÖNNEN, IST IMMENS UND STEIGT JEDES JAHR.”

Daten aus den jeweiligen Geräten, gegebenenfalls das Dekodieren der Daten und später auch deren Analyse dahingehend, ob sie einen Nutzen für den Fall haben.

Technische Grundlagen für digitale Forensik legen

Um dieser und weiteren Herausforderungen in Ermittlungen und Strafverfolgung zu begegnen, hat das Bundesministerium des Innern, für Bau und Heimat 2017 die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) geschaffen. ZITiS ist Teil der Cyber-Sicherheitsstrategie für Deutschland und ist Dienstleister für das Bundeskriminalamt (BKA), die Bundespolizei (BPol) und das Bundesamt für Verfassungsschutz (BfV). In deren Auftrag erforscht und entwickelt die Behörde neue technische Lösungen und Methoden, die die Innere Sicherheit verbessern, und bietet zudem Beratung zu technischen Fragen sowie Strategien im Sicherheitsbereich an.

Die ZITiS selbst hat keine Eingriffsbefugnisse, wertet keine Daten aus und bearbeitet keine Spuren aus Verbrechen. Die junge Behörde stellt den drei Bedarfsträgern unter anderem die notwendige Technik zur Verfügung, um Daten aus allen möglichen Geräten zu extrahieren. Dazu wird untersucht, welche Daten wo gespeichert werden und wie die Sicherheitsbehörden diese Daten auslesen und interpretieren können. Das ist unser Beitrag für eine moderne Strafverfolgung in Deutschland.

Schwierige Ermittlungen im digitalen Raum

► Dr. Julia Bussweiler ist Staatsanwältin bei der hessischen Zentralstelle zur Bekämpfung der Internetkriminalität (ZIT) mit Sitz in Gießen. Diese ist eine Sondereinheit der Generalstaatsanwaltschaft Frankfurt am Main.

Neben Polizisten stehen auch Staatsanwälte bei Verfahren im Internet vor großen Herausforderungen. Das gilt ganz besonders für den Bereich des Darknet. Hier bräuchte es auch neue Straftatbestände, meint Dr. Julia Bussweiler. Die Fragen an die Staatsanwältin bei der Zentralstelle zur Bekämpfung der Internetkriminalität (ZIT) im hessischen Gießen stellten Marco Feldmann und Benjamin Stiebel.

Moderne Polizei: *Frau Dr. Bussweiler, vor welchen Problemen stehen Sie als Staatsanwältin bei Ermittlungen im digitalen Raum, insbesondere im Darknet?*

Dr. Bussweiler: Bei Ermittlungen im digitalen Raum tun sich für uns als Staatsanwälte mannigfaltige Probleme auf. Sehr problematisch ist zum Beispiel die Verschlüsselung im Darknet, denn dadurch erhalten wir bei Ermittlungsverfahren in diesem Bereich keine realen IP-Adressen. Da fehlt uns dann oft ein Ermittlungsansatz. Außerdem agieren Täter im Darknet oft sehr konspirativ und vorsichtig. Wenn jemand hingegen im "normalen" Internet eine Straftat begeht, können wir IP-Adressen abfragen und dann ermitteln, zu wem sie gehören.

Moderne Polizei: *Welche weiteren Probleme gibt es?*

Bussweiler: Auf Darknet-Plattformen, auf denen kinderpornografisches Material angeboten wird, werden oft sogenannte "Keuschheitsproben" verlangt. Dabei müssen Nutzer selbst kinderpornografisches Material hochladen, um Mitglied in diesen geschlossenen Kreisen zu werden. Aber weder wir als Staatsanwälte noch Polizeibeamte dürfen das tun, denn ansonsten würden wir uns strafbar machen.
Außerdem sind Ermittlungen im digitalen Raum technisch oftmals sehr schwierig. Ansatzpunkte für uns sind in aller Regel Schnittstellen zwischen der digitalen und der realen Welt, etwa wenn im Darknet erworbene Waffen oder Drogen per Post versendet werden. Da können wir teilweise Sendungen abfangen und dann Spuren sichern. Schwieriger wird es für uns, wenn es solche Schnittstellen nicht gibt. Das ist zum Beispiel bei Kinderpornografie der Fall, weil entsprechende Dateien einfach heruntergeladen werden können.

Moderne Polizei: *Braucht es einen neuen, eigenständigen Straftatbestand, der das Betreiben illegaler Plattformen im Darknet sanktioniert?*


Foto: privat

Bussweiler: Ja, den bräuchten wir. Bisher ist es so, dass wir nur Betreiber von Kinderpornografie-Plattformen als Täter belangen können, weil es dafür eine explizite Vorschrift gibt. Bei Plattformen, auf denen etwa Betäubungsmittel oder Waffen verkauft werden, können wir gegen die Betreiber bisher in der Regel nur wegen Beihilfe zu einer Straftat vorgehen. Und da muss der Strafrahmen zwingend gemildert werden. Das wird der Sache nicht gerecht.

Moderne Polizei: *Wie gestaltet sich in den von Ihnen geführten Ermittlungsverfahren die Zusammenarbeit mit der Polizei? Unterscheidet sich diese von Verfahren im analogen Bereich oder durch eine landgerichtliche Staatsanwaltschaft?*

Bussweiler: Ja, da gibt es schon Unterschiede. Wir bei der Zentralstelle zur Bekämpfung der Internetkriminalität haben Ermittlungsmaßnahmen, die wir im Vergleich zu landgerichtlichen Staatsanwaltschaften viel häufiger einsetzen. Das gilt unter anderem für Maßnahmen zur Telekommunikationsüberwachung, weil vor allem Verkehrsdaten für Ermittlungen in unseren Fällen äußerst wichtig sind. Zudem arbeiten wir weit überwiegend mit dem Bundeskriminalamt zusammen, weil es da zahlreiche spezialisierte Sachgebiete und ein über Jahre aufgebautes Know-how gibt. Die Kollegen verfügen über viel Erfahrung, sodass wir aus den gewonnen Daten dann auch zahlreiche Erkenntnisse ableiten können. Da unterscheidet sich unsere Arbeit doch schon relativ stark von der in einer landgerichtlichen Staatsanwaltschaft. Gleiches gilt für unsere Arbeit mit verdeckten Ermittlern im Internet. Deren Arbeit unterscheidet sich schon erheblich von der ihrer Kollegen in der analogen Welt.

Moderne Polizei: *Welche strafprozessualen Instrumente haben Sie bereits und welche wünschen Sie sich noch?*

Bussweiler: Wir haben die gleichen strafprozessualen Maßnahmen wie alle anderen Staatsanwaltschaften auch, nutzen sie nur manchmal etwas anders und ausgiebiger. Bei unseren Verfahren

werden häufig E-Mails beschlagnahmt. Allerdings ist die Strafprozessordnung schon älter, weshalb sich dort keine ausdrückliche Einzelbestimmung für eine derartige Beschlagnahme findet. Wir ziehen dann immer den entsprechenden Paragraphen zur Beschlagnahme von Postsendungen heran.
Es wäre jedoch wünschenswert, wenn in die Strafprozessordnung eine explizite Bestimmung zur Beschlagnahme von E-Mails aufgenommen werden würde. Außerdem würden wir es begrüßen, wenn Ermittlern bei Kinderpornografie-Verfahren "Keuschheitsproben" erlaubt würden. Da könnte man dann mit computergenerierten Dateien und fiktiven Bildern arbeiten. Wünschenswert wäre es zudem, wenn die Vorratsdatenspeicherung auch tatsächlich umgesetzt werden würde. Und: wir hätten gern eine konkrete, gesetzgeberische Norm zur Herausgabe von Kunden- und Sendungsdaten gegenüber Postdienstleistern, da dazu divergierende Auffassungen innerhalb der höchstrichterlichen Rechtsprechung existieren. Das würde uns bei Ermittlungen sehr helfen.

Moderne Polizei: *Wie gestaltet sich die Zusammenarbeit mit anderen Staatsanwaltschaften?*

Bussweiler: Die Zusammenarbeit mit anderen Staatsanwaltschaften funktioniert sehr gut. Das gilt besonders dann, wenn es im jeweiligen Bundesland auch eine Zentralstelle wie unsere gibt. Dies ist etwa in Bayern und Nordrhein-Westfalen der Fall. Und da unsere Aktenführung vollständig elektronisch erfolgt, können wir bei Verfahrensabgaben an andere Staatsanwaltschaften die Daten sehr schnell übermitteln. Das hilft ungemein, wenn zum Beispiel ein Verdächtiger schnell in Untersuchungshaft genommen werden soll und es keinen Zeitverzug geben darf.

Moderne Polizei: *Und wie sieht es mit der grenzüberschreitenden Kooperation aus?*

Bussweiler: Auch da sieht es in der Regel gut aus, in den letzten Jahren hat sich da sehr viel getan. Internationale Zusammenarbeit ist bei der Strafverfolgung im Internet äußerst wichtig. Da hilft uns auch die Kooperation mit dem Bundeskriminalamt sehr. Sehr gut zusammengearbeitet haben wir zuletzt unter anderem mit den baltischen Staaten sowie mit Bosnien-Herzegowina.
Zur Wahrheit gehört aber auch, dass das Ausmaß der Zusammenarbeit oft vom Einzelfall, dem jeweiligen Land sowie von den involvierten Kolleginnen und Kollegen im Ausland abhängt. Schwieriger wird es, wenn die Verdächtigen weiter entfernt sitzen, zum Beispiel in Südostasien. Innerhalb der Europäischen Union, etwa mit den Niederlanden oder Frankreich, ist die Kooperation in aller Regel sehr gut. Gleiches gilt meiner Erfahrung nach für den grenzüberschreitenden Austausch polizeilicher Daten.

Auf ewig ein Traum?

Schnelle und transparente Zusammenarbeit

► Gerhard Brunner, Account Manager Government & Church D/A, Corel GmbH

Die Anforderungen an die tägliche Polizeiarbeit hinsichtlich Transparenz und Visualisierung sind extrem hoch. Aktuell begegnet dem Anwender bei der täglichen Vorgangsbearbeitung eine Vielzahl an Tools, welche die Wünsche und Anforderungen an Daten und Informationen nicht zufriedenstellend abbilden.

Einerseits besteht der Wunsch nach Qualität, Wirtschaftlichkeit, Benutzerfreundlichkeit und danach, relevante Daten zur richtigen Zeit am richtigen Ort zu finden. Andererseits sind unzählige Systeme zur Datenerfassung mit unterschiedlichen Formaten im Einsatz, die die Arbeit sehr zeitaufwendig und intransparent gestalten.

Auf dem Europäischen Polizeikongress in Berlin haben die verschiedenen Vorträge zu Big Data, Vorgangsbearbeitung, Cyber-Kriminalität, Analysen, digitaler Polizeiarbeit und Vernetzung wiederholt gezeigt, wie komplex die Themen sind und dass Schnelligkeit sowie Transparenz in der Bearbeitung heute noch nicht ausreichend gegeben sind. Der Bereich des Cyber Crime umfasst unter anderem die Themen Big Data, digitale Forensik, Telekommunikationsüberwachung und Kryptoanalyse. Dabei fehlen dem Mitarbeiter immer öfter die passenden Mittel, um diese Bereiche transparent zu verknüpfen.

Übergreifende Vereinigung möglich

Die Visualisierungsmöglichkeiten von MindManager ermöglichen, individuelle Datenquellen länder- und systemübergreifend zu vereinen und eröffnen den komfortablen Wissenstransfer. Dabei können verschiedene Systeme Input liefern, sodass MindManager als visuelles Front-End dient. Aufgaben, Prozesse und Projekte können strukturiert, aktuell, transparent und dynamisch bearbeitet werden. Wird ein Merkmal erst in der Kombination aus mehreren Quellen auffällig, kann dies per Regelwerk signifikant visualisiert werden. Das alles gelingt so benutzerfreundlich und pragmatisch, dass Teamarbeit und Wissensaustausch einen neuen Charakter erhalten.

Mehr dazu unter:
https://www.mindjet.com/de/blog/polizeiarbeit
govda@mindjet.com, Tel: 06023-9645-317

Visualisierung mit MindManager: länder- und systemübergreifender Wissenstransfer

Abbildung: Corel GmbH

Ermittlungen in einer smarten Welt

► Alexander Hahn, Leiter Dezernat “Cybercrime und Digitale Spuren”, Landeskriminalamt Schleswig-Holstein


Foto: privat

In einer zunehmend digitalisierten Welt spielt die Auswertung digitaler Spuren bei der polizeilichen Ermittlungsarbeit eine immer größere Rolle. Ob WLAN-Router, smarter Kühlschrank oder “mithörender” Sprachassistent: Der Tatort ist heute zunehmend auch ein “Smart-Ort” – ein Ort, an dem neben den herkömmlichen Spuren wie Fingerabdrücken oder DNA-Spuren auch digitale Spuren entscheidende Hinweise liefern können. Dabei geht es nicht nur um digitale Kriminalität oder Cyber Crime, sondern um das gesamte Spektrum polizeilicher Ermittlungen vom Autounfall über Einbruch bis zum Tötungsdelikt. Mit einem neuen “Kompetenzzentrum Digitale Spuren” geht das Landeskriminalamt Schleswig-Holstein neue Wege und stellt sich für die Herausforderungen der Zukunft optimal auf.

Der “Smart-Ort” als Tatort

Digitale Spuren hinterlässt ein Täter immer, ob er will oder nicht. Es ist heutzutage nahezu unmöglich, keine digitalen Spuren im engeren oder weiteren Tatortbereich beziehungsweise vor, während oder nach der Tat zu hinterlassen. Ähnlich wie bei der DNA verhält es sich dann aber auch mit dem Auffinden dieser neuen Spuren: Sie sind nicht immer auf den ersten Blick zu erkennen. Die Polizei muss daher in Abhängigkeit von der Bedeutung des Falles schon bei der Tatortarbeit hinreichend viel Zeit und Energie investieren, um digitale Spuren zu identifizieren. Der “Smart-Ort” als Tatort wird die Polizei zukünftig fordern.

Das neue Sachgebiet LKA 234, kurz KodiS genannt, ist ein Baustein des Digitalisierungsprogramms der schleswig-holsteinischen Landesregierung. Ziel ist es, digitale Spuren künftig noch besser für die Ermittlungsarbeit nutzen zu können. Dafür stellt die Landespolizei externe Spezialisten wie Informatiker und/oder Ingenieure ein, die im Team mit spezialisierten Polizeibeamten arbeiten. Außerdem sollen ähnlich kompetente Ansprechpartner in den Flächenbehörden eingesetzt werden und damit die Schnittstelle zwischen den Spezialisten im LKA und den Ermittlern und Ausbildern vor Ort abbilden. Geplant sind insgesamt 20 neue Stellen: Zwölf für das “Kompetenzzentrum Digitale Spuren”, das im LKA 23, “Cybercrime und Digitale Spuren”, angebunden sein wird. Acht weitere Stellen werden in den sieben Flächendirektionen des Landes sowie in der Polizeidirektion für Aus- und Fortbildung geschaffen.

Technisches Wissen und polizeiliches Denken vernetzen

Künftig kann die Polizei also noch mehr Zeit, Energie und Technik investieren, um digitale Spuren zu sichern und für eine Auswertung aufzubereiten. So soll zum Beispiel ein “digitales Tatort-Team” einen Tatort aus dem “digitalen Blickwinkel” betrachten und parallel zur klassischen Spurensicherung in Erscheinung treten. Die Vernetzung von Spezialwissen und polizeilichem Denken ist dabei ebenso eine Herausforderung wie die Fähigkeit, technisch mit dem hohen Innovationstempo im digitalen Bereich Schritt zu halten. Eine weitere Herausforderung bleibt die Auswertung der so gewonnenen Spuren: Insbesondere die Komplexität und Masse der Daten sowie die Komplexität der Auswerte-Tools erfordert ein hohes Maß an Zeit und Wissen.

Vor diesem Hintergrund investiert die Landespolizei natürlich auch verstärkt in die Aus- und Fortbildung: Neben neuen Ausbildungsinhalten zur digitalen Spurensicherung sichert die Polizei mit dem Angebot eines dualen Studiengangs “Informationstechnologie” in Zusammenarbeit mit der Fachhochschule Kiel erstmals ihren Nachwuchs an Fachkräften selbst. Die ersten fünf Studenten haben ihre Ausbildung im vergangenen Jahr begonnen und werden dem LKA nach dem Studium als ermittlungsunterstützende Spezialisten zur Verfügung stehen – auch für das “Kompetenzzentrum Digitale Spuren”.

In Deutschland ist das KodiS-Team in dieser Form bislang zwar einmalig, doch in vielen Bundesländern wird überlegt, einen ähnlichen Weg einzuschlagen. Fest steht: In diesem Bereich wird sich auch weiterhin vieles rasant entwickeln.

“ES IST HEUTZUTAGE NAHEZU UNMÖGLICH, KEINE DIGITALEN SPUREN IM ENGEREN ODER WEITEREN TATORTBEREICH BEZIEHUNGSWEISE VOR, WÄHREND ODER NACH DER TAT ZU HINTERLASSEN.”

Open Source Intelligence und Echtzeitanalysen in Leitstellen der Polizei

► Franziska Ludewig, Wissenschaftliche Mitarbeiterin im Projekt SENTINEL – "Sicherheit im Einsatz durch Open-Source-Intelligence (OSINT) in Einsatzleitstellen" an der Deutschen Hochschule der Polizei

In unserem Privatleben haben wir uns an den schnellen Zugang zu digitalen Informationen gewöhnt. Die Digitalisierung ermöglicht es uns, Echtzeitinformationen zu jeder Tageszeit, überall auf der Welt abzurufen. Wir nutzen den Regenradar, bevor wir das Haus verlassen, prüfen kurzfristig nochmal die Pünktlichkeit des öffentlichen Nahverkehrs oder rufen mittels Navigationssystem Informationen zum aktuellen Verkehrsaufkommen ab. Wir sehen das neue Auto, die Sportroutinen und das Lieblingscafé in Insta-Stories von Bekannten, manchmal auch völlig Fremden, und geben auf Facebook an, ein Konzert zu besuchen und posten ein aktuelles Selfie.

Das Internet – und besonders Social Media – bieten dadurch eine Vielzahl personenbezogener Informationen, von Nutzern freiwillig und häufig offen geteilt, um das eigene Profil auszugestalten und sich selbst zu inszenieren. Zahlen zur Social-Media-Nutzung zeigen, dass alleine auf Facebook jeden Tag 350 Millionen Fotos hochgeladen werden. Instagram verzeichnet 95 Millionen Posts täglich (Stand Juni 2016, die Zahl ist wahrscheinlich heute noch höher). Diese Zahlen verdeutlichen die ständig wachsende Menge von Informationen im Internet.

Die systematische und gezielte Erkenntnisgewinnung aus frei verfügbaren, offenen Quellen wird Open Source Intelligence (kurz OSINT) genannt. Derartige Informationen haben vielfach den großen Vorteil der Aktualität und können auch im Rahmen täglicher Polizeieinsätze relevant sein, beispielsweise bei vermissten Personen, Suizidandrohungen oder in Fällen häuslicher Gewalt. Schließlich können aktuelle Fotos oder Anlaufadressen die professionelle Aufgabenbewältigung unterstützen und Informationen zu Haustieren, speziellen Hobbies oder Mitgliedschaften in bestimmten Gruppen eintreffenden Einsatzkräften wichtige Eigensicherungsrückschlüsse ermöglichen. Entscheidend ist es, in dem großen Datenbestand des Internets die tatsächlich relevanten Daten zu finden und Irrelevantes auszuschließen.

Noch keine systematische Verwendung in Leitstellen

Besonders im Bereich der Ermittlungen hat sich OSINT in der Polizei bereits als Instrument und wichtige Erkenntnisquelle etabliert. In Leitstellen, die das ständige Führungsorgan der Polizeibehörden sind und von wo aus in Notlagen Maßnahmen bis zum Einsatzabschluss oder bis zur Übernahme durch ein anderes Führungsorgan koordiniert werden, wird OSINT derzeit noch nicht systematisch genutzt. Dabei lösen die dort eingehenden Einsätze ein sehr hohes Informationsbedürfnis aus. Diesem wird mit der proaktiven Bereitstellung von Informationen an die anfahrenden Einsatzkräfte aus der Leitstelle begegnet. Die Informationsbasis beruht dabei bisher standardmäßig auf den Angaben des Notrufenden und den behördlichen Datenbeständen. OSINT-Daten können das Informationsniveau jedoch weiter steigern, vorhandene Informationen sinnvoll ergänzen und den Einsatzkräften dadurch ein aktuelles und umfassenderes Bild von einer Situation geben.


Foto: privat

Pilotprojekt in drei Leitstellen

Das Forschungsprojekt SENTINEL ("Sicherheit im Einsatz durch Open-Source-Intelligence in Einsatzleitstellen") der Deutschen Hochschule der Polizei (DHPol) widmet sich dieser Echtzeitanalyse. Im Rahmen einer Pilotphase wurde in drei Leitstellen (im Polizeipräsidium Dortmund, Polizeipräsidium München und der Polizeidirektion Osnabrück) OSINT implementiert. Dafür wurden Beamte zu sogenannten Intel-Officern hinsichtlich OSINT und aktuellen Analysemethoden ausgebildet, die in Echtzeit Social Media und andere offene Quellen einsatzunterstützend analysieren, bewerten und diese an ihre Kollegen auf der Straße steuern. Die Implementierung wurde wissenschaftlich evaluiert und alle bearbeiteten Einsätze systematisch erhoben. Der Forschungsbericht wird in Kürze vorliegen.

Die niedersächsische Polizei hat bereits im März 2019 dreizehn Intel-Officer eingestellt und möchte diesen Weg konsequent weiterverfolgen.

"IN LEITSTELLEN, DIE DAS STÄNDIGE FÜHRUNGSORGAN DER POLIZEIBEHÖRDEN SIND, WIRD OSINT DERZEIT NOCH NICHT SYSTEMATISCH GENUTZT."

Gerichtsverwertbare Gutachten

DVZ M-V GmbH bietet Expertise auf dem Gebiet der IT-Forensik

► **Sebastian Schriever, IT-Sachverständiger, DVZ M-V GmbH**

Die im Rahmen einer forensischen Untersuchung gewonnenen Erkenntnisse und sichergestellten Beweise dienen als Grundlage zur Erstellung von Gutachten, die bei Bedarf in ein gerichtliches Verfahren eingebracht werden. Durch die langjährige Erfahrung und Zusammenarbeit mit Ermittlungsbehörden hat die DVZ M-V GmbH ihre Kompetenzen erweitert und unterstützt diese nun auch auf dem Gebiet der IT-Forensik.

Um gerichtsverwertbare Gutachten erstellen zu können, müssen diese durch einen IT-Sachverständigen objektiv, unparteiisch und weisungsfrei erstellt werden. Dazu ist der Inhalt korrekt, nachprüfbar, nachvollziehbar und für Laien verständlich zu verfassen. Alle im Gutachten getroffenen Festlegungen erfolgen aufgrund der vorliegenden Asservate. Weiter berät der Sachverständige den Auftraggeber in jeder Phase der Untersuchung.

Die DVZ M-V GmbH ist spezialisiert auf die Untersuchung von Computern, Mobilgeräten und GPS-Systemen, Smart-Technologien (zum Beispiel Smart-TVs oder Alexa) und Cloud-Umgebungen (zum Beispiel Dropbox oder Microsoft One Drive). Die stete Einhaltung der “chain of custody” (der lückenlosen Beweisführung) und die Erstellung präziser forensischer Protokolle dokumentieren jeden Schritt der Untersuchung und sichern die Beweisfähigkeit bei einer Anhörung vor Gericht. Dabei befolgt der Experte strikt die strengen Richtlinien zum Datenumgang.

In der forensischen Untersuchung kommen ausschließlich modernste Programme und Techniken zum Einsatz. Trotzdem sind stets IT-Know-how, Geduld und Experimentierfreude gefragt.

Mehr Informationen unter: www.dvz-mv.de

Behörden müssen nicht tatenlos zusehen

► Manuela Siegemund, Preisträgerin des “Zukunftspreises Polizeiarbeit” 2019


Foto: privat

“WERDEN DIE GEWASCHENEN BITCOIN DURCH DEN TÄTER NUN BEISPIELSWEISE IN EURO UMGETAUSCHT, BESTEHT TROTZ VERWENDUNG EINES MIXING-DIENSTES EINE GUTE CHANCE, DEN ERPRESSER AUSFINDIG ZU MACHEN.”

Und wieder wird die Kryptowährung Bitcoin in der öffentlichen Wahrnehmung als das Zahlungsmittel krimineller Machenschaften wahrgenommen. Diesmal durch Medienberichte über Erpressungsmails, die zu einer Zahlung von Bitcoin auffordern. Andernfalls würden pornografische Chats des Betroffenen veröffentlicht.

Obwohl der Bitcoin mit der dahinterstehenden Blockchain-Technologie als dezentrales Zahlungsmittel ohne staatliche Kontrolle und Einflussnahme gedacht war, zieht die Währung immer wieder Kriminelle an, die Zahlungsverkehre zwischen Täter und Opfer oder Tätern untereinander verschleiern wollen. Ein Grund dafür ist die vermeintliche Anonymität der Währung.

In der Erpressungsmail wird dem Opfer ausschließlich die Bitcoin-Adresse, eine wirre Zeichenfolge bestehend aus 32 Buchstaben und Zahlen, des Täters mitgeteilt, auf die der geforderte Betrag transferiert werden soll. Diese Transaktion ist zwar zu 100 Prozent transparent, also für jeden in der Blockchain, dem öffentlichen Transaktionsregister der Kryptowährung, einsehbar, gibt aber keinen Aufschluss darüber, wer sich hinter der genannten Adresse tatsächlich verbirgt. Das macht es Strafverfolgungsbehörden nicht einfach, dem Täter basierend auf der Nachverfolgung der Zahlungsströme auf die Spur zu kommen. Ansatzpunkte können jedoch durchaus gefunden werden, nämlich wenn die Bitcoin in konventionelle Währungen umgetauscht oder Konsumgüter damit online bezahlt werden.

Schwierigkeiten für Strafverfolger

Diese Möglichkeit der Aufklärung von Straftaten durch Behörden ist den Kriminellen nicht unbekannt. Daher blüht das Geschäft sogenannter Mixing-Dienste, welche das Prinzip der Geldwäsche für Bitcoin umsetzen. Der zu verschleiernde Betrag wird auf eine Adresse des Mixing-Dienstes transferiert, kann dort je nach Wunsch des Kunden mehrere Tage verweilen und wird nach Abzug einer variablen Gebühr zurücküberwiesen.

Dazu nennt der Nutzer dem Dienst eine neue, unbelastete Bitcoin-Adresse. Im Normalfall kann diese Auszahlung zusätzlich gesplittet werden, weshalb auch mehrere Adressen genannt werden können. Außerdem verwendet der Mixing-Dienst für die Rücküberweisung Bitcoin eines anderen Kunden. Letzteres, zusammen mit der zeitlichen Verzögerung, den variablen Gebühren und der flexiblen Anzahl an Auszahlungsadressen, macht es den Strafverfolgungsbehörden fast unmöglich, die Ein- und Auszahlungen in Zusammenhang zu bringen und somit die erpressten Bitcoin weiterzuverfolgen.

Nicht unmöglich

Jedoch gibt es durchaus Chancen, dies zu bewerkstelligen. Für gewöhnlich ist nicht bekannt, wie das Mixen der Bitcoin innerhalb eines Dienstes umgesetzt wurde. Durch testweises Verwenden des Services und Beobachten der “eigenen” ein- und ausgezahlten Bitcoin können Verhaltensmuster in dieser vermeintlichen Blackbox “Mixing-Dienst” erkannt werden, die es ermöglichen, unterschiedliche Bitcoin-Adressen einer Entität, also dem verwendeten Mixer, zuzuordnen. Dadurch entsteht ein Adressen-Cluster für den analysierten Mixing-Dienst. Das heißt, es wird davon ausgegangen, dass jede Bitcoin-Adresse dieses Clusters dem Mixing-Dienst gehört.

Aufgrund der somit definierten Größe des Clusters kann jede Transaktion in den Cluster beziehungsweise aus dem Cluster heraus als eine Interaktion des Mixing-Dienstes mit einem Kunden deklariert werden, weshalb die Ein- beziehungsweise Auszahlungen aller Kunden erfasst werden. Wird auf diese Weise nun eine Einzahlung des Erpressers in den analysierten Mixing-Dienst beobachtet, können alle potenziellen Auszahlungen aus dem generierten Cluster in Hinblick auf eine mögliche Auszahlung an den Erpresser betrachtet werden.

Weiterverfolgung leistbar

Unter Berücksichtigung der genannten Eigenschaften eines jeden Mixing-Dienstes, wie die zeitliche Verzögerung und die anfallende Gebühr, wird die Anzahl der möglichen Auszahlungen im Optimalfall derart reduziert, dass eine Weiterverfolgung der übrigbleibenden Bitcoin-Adressen für Strafverfolgungsbehörden leistbar ist. Werden die gewaschenen Bitcoin durch den Täter nun beispielsweise in Euro umgetauscht, besteht trotz Verwendung eines Mixing-Dienstes eine gute Chance, den Erpresser ausfindig zu machen.

Schwerpunkt Prävention

► Helge Hinrichs, Leiter FK Cyber Crime im Hamburger Landeskriminalamt


Foto: Polizei Hamburg

"Cyber-Sicherheit ist kein statischer Zustand, sondern ein ständiger Prozess." Einen Satz dieser Art benutzen die Mitarbeiter der "Zentralen Ansprechstelle Cybercrime" (ZAC) des Fachkommissariats Cyber Crime im Landeskriminalamt Hamburg häufig bei Beratungen der Wirtschaft. Der Fokus liegt dabei hauptsächlich auf kleinen und mittleren Unternehmen, die oftmals über keine eigene IT-Abteilung verfügen oder deren IT-Struktur über die Jahre, vielleicht sogar Jahrzehnte, gewachsen ist, ohne dass in der Zwischenzeit eine detaillierte Betrachtung stattgefunden hat.

Warum ist das Angebot einer Prävention für die Wirtschaft so wichtig? Weil die Aufklärungsquote im Bereich Cyber Crime durchaus als schlecht bezeichnet werden kann. Es geht darum, Straftaten zu verhindern, für neue Modi Operandi zu sensibilisieren und eine Basis des Vertrauens zwischen Wirtschaft und Polizei herzustellen. Denn auch das Dunkelfeld in diesem Bereich ist sehr hoch. Ziel ist es, dass die Polizei als vertrauensvoller, kompetenter Partner angenommen wird, sodass bei einer Cyber-Attacke die Hemmschwelle für eine Hinzuziehung so niedrig wie möglich ist.

Großes Interesse

Das Interesse der Wirtschaft an Beratung ist hoch, sodass die ZAC neben individuellen Beratungen vornehmlich auch Großveranstaltungen nutzt, um eine Vielzahl von Unternehmensverantwortlichen zu erreichen. Hierfür haben sich Banken oder die Handelskammer als starke Partner etabliert. Gerade bei Start-up-Unternehmen profitieren sowohl die Bank als auch das Start-up selbst, wenn die Risiken eines Schadens durch einen Cyber-Angriff minimiert oder im besten Fall eliminiert werden, denn der vollständige Datenverlust eines E-Commerce ist nicht zu kompensieren und führt fast zwangsweise zur Geschäftsaufgabe.

Bei den Beratungen sind in der Regel die Geschäftsführer oder IT-Verantwortlichen anwesend.

Für eine erfolgreiche Awareness-Kampagne ist es aus unserer Sicht jedoch notwendig, dass alle Risikofaktoren mit einbezogen werden – und die größte Gefahr geht nach wie vor von den Mitarbeitern aus. Seien es maliziöse Mail-Anhänge, die unbedarft geöffnet werden, das Ausführen von Zahlungen für einen erfolgreichen CEO-Fraud oder das Einbringen von Schadsoftware durch private Hardware (BYOD).

Um es den Unternehmen zu ermöglichen, sämtliche Mitarbeiter zu beschulen und zu sensibilisieren, hat das Landeskriminalamt Hamburg einen sogenannten Awareness-Stick entwickelt: Eine webbasierte Schulung auf einem USB-Stick, der durch die ZAC kostenfrei an Firmen bei Beratungsveranstaltungen verteilt wird, und dessen Inhalt auf den internen Netzwerken aufgespielt werden kann, sodass sich jeder Mitarbeiter mit aktuellen Risiken vertraut machen kann und Handlungsempfehlungen an die Hand bekommt. Der Stick verfügt über eine Update-Funktion, sodass neue Tatbegehungsweisen eingepflegt und neue Inhalte hinzugefügt werden können. Die Schulung kann natürlich auch ohne den USB-Stick heruntergeladen und genutzt werden.

Spezialisierung ist notwendig

Um die Akzeptanz in der Wirtschaft zu gewährleisten, sind die Mitarbeiter, die Vorträge zu Cyber-Sicherheit halten oder individuelle Beratungen vornehmen, selber Spezialisten und ausschließlich Kriminalbeamte, teilweise mit Masterabschluss in "IT Security". Dies ist aus unserer Perspektive notwendig, um zum einen mit den CIOs oder CISOs der Unternehmen auf Augenhöhe zu agieren, zum anderen aber auch eine Beratung unter kriminaltaktischen Gesichtspunkten führen zu können, denn, zum Beispiel bei einer Erpressung mittels Ransomware, ist nicht nur die technische Komponente zu betrachten. Vielmehr geht es den Firmen oftmals darum, wie sie sich verhalten sollen und immer wieder ist auch zu beobachten, dass ein großes Interesse darin besteht, die Polizei bei den Ermittlungen zu unterstützen. Dies wäre ohne die Vorarbeit der ZAC und das dadurch erworbene Vertrauen mit Sicherheit nicht so ausgeprägt. Und dieser Prozess wird auch in Zukunft weiter ausgebaut.

"FÜR EINE ERFOLGREICHE AWARENESS-KAMPAGNE IST ES AUS UNSERER SICHT JEDOCH NOTWENDIG, DASS ALLE RISIKOFAKTOREN MIT EINBEZOGEN WERDEN – UND DIE GRÖSSTE GEFAHR GEHT NACH WIE VOR VON DEN MITARBEITERN AUS."

Kampf auf mehreren Ebenen

► Mario Foth, Leiter Cyber-Competence-Center (CCC) der Polizei Brandenburg


Foto: Fotoatelier Kathrin Schmiedel, Ludwigsfelde

Auch das Land Brandenburg wappnet sich für den Kampf gegen Cyber Crime und darüber hinaus für den Umgang mit digitalen Spuren. Denn die Digitalisierung durchdringt so gut wie jedes Deliktsfeld. So bekämpft die Brandenburger Polizei Delikte gegen Datennetze, informationstechnische Systeme oder deren Daten (Cyber Crime im engeren Sinne) auf drei verschiedenen Ebenen: dem Landeskriminalamt, den vier nach den Himmelsrichtungen benannten Polizeidirektionen und den Kriminalkommissariaten in den Inspektionen.
Delikte, deren Modus Operandi Informationstechnik umfasst (Cyber Crime im weiteren Sinne), bekämpfen die meisten Organisationseinheiten der Brandenburger Polizei.

CCC von großer Bedeutung

Im Brandenburger Landeskriminalamt trägt das Cyber-Competence-Center (CCC) maßgeblich zum Kampf gegen Cyber Crime bei. Das CCC leistet auch einen Beitrag zur Hochkompetenz der Brandenburger Polizei beim Suchen, Sichern und Auswerten digitaler Spuren bei regelmäßig schwerwiegenden Delikten. Das CCC als Dezernat in einer der vier Abteilungen des Landeskriminalamtes ist in ein Kriminalkommissariat (KK) und drei Sachgebiete (SG) strukturiert.
Die Ermittler des KK verfügen über ein weit überdurchschnittliches kriminalistisches und technisches Know-how beim Umgang mit digitalen Spuren – bedingt einerseits durch spezifische Vor- und Ausbildungen (Informatik- oder vergleichbare Studiengänge, berufspraktische Erfahrungen bei IT-Dienstleistern), dienstliche Weiterbildungen sowie andererseits durch die unmittelbare und tägliche Wissensanwendung. Im Sachbereich "Zentrale Internetrecherche" wird Open Source Intelligence (OSINT) verfahrens- und projektbezogen angewendet.
Die Ansprechstelle für Kinder- und Jugendpornografie koordiniert Maßnahmen und steuert Informationen zur Bekämpfung dieses verwerflichen Deliktsfeldes. Die "Zentrale Ansprechstelle Cybercrime" (ZAC) fungiert als Single Point of Contact für die Wirtschaft und Behörden des Landes Brandenburg bei Cyber-Angriffen. Im Sinne der Spezialprävention trägt sie zu aktuellen Phänomenen und Schutzmaßnahmen vor, Versuche des CEO-Frauds oder Technical Support Scams blieben so erfolglos. Öffentlichkeitswirksam agierten die Ermittler mit der bundesweit ersten Fahndung nach einer MAC-Adresse.
Das SG Informationstechnische Überwachung (ITÜ) entwickelt die klassische Telekommunikations-Überwachung zur ITÜ weiter. Neue Ermittlungsansätze und auch neuere strafprozessuale Befugnisse wie die Quellen-TKÜ und Online-Durchsuchung fordern sowohl Personal als auch Technik.
Das SG IuK-Service hilft, digitale Spuren auf nicht flüchtigen, veränderbaren Datenträgern zu sichern und bereitet die gesicherten Daten auf. Dabei kann es sich um klassische Festplatten, Solid State Disks, USB-Speicher oder auch interne Speicher von Smartphones handeln. Um die Grenzen des Machbaren zu verschieben, kommen auch die Chip-off-Methode sowie andere mechanische Ansätze zum Einsatz. Darüber hinaus prüfen die Köpfe des Sachgebietes in einschlägigen Verfahren sichergestellte PC-Technik auf den Besitz kinder- und jugendpornografischer Schriften. Dabei greifen sie auf die Hashwerte-Datenbank des Bundeskriminalamtes zurück, wo Polizeien den Fingerabdruck (sogenannter Hash-Set) von kinder- und jugendpornografischen Dateien hinterlegen.
Die Köpfe des SG IuK-Forensik verfügen über die Sachverständigenausbildung IuK des Bundeskriminalamtes. Sie untersuchen die Datenträger forensisch und erstellen Gutachten für das Strafverfahren. In besonders kniffligen Fällen kommen sie zum Einsatz. So auch, wenn es um die Entschlüsselung passwortgeschützter Daten geht.

"IM BRANDENBURGER LANDESKRIMINALAMT TRÄGT DAS CYBER-COMPETENCE-CENTER (CCC) MASSGEBLICH ZUM KAMPF GEGEN CYBER CRIME BEI."

Arbeiten Hand in Hand

Letztlich arbeiten die Organisationseinheiten der Polizeien der Länder sowie des Bundes in Gremien, aber auch in konkreten Ermittlungsverfahren Hand in Hand zusammen, um auch die digitalen Spuren bei der Gefahrenabwehr und Strafverfolgung nutzen zu können. Dabei gilt das Prinzip der lernenden Organisation. Zukünftig werden IP-Tracking, Kryptowährungsanalyse, Honeypots etc. höchstwahrscheinlich ebenso wie die melderechtliche Auskunft zum Handwerkszeug des Polizisten gehören.

Big Data als Lösung: Auswertung unstrukturierter Datenmengen

► Dr. Julia Fricke, Preisträgerin des "Zukunftspreises Polizeiarbeit" 2019 und derzeit tätig im Polizeipräsidium Recklinghausen


Foto: privat

Wie könnte ein Sexualstraftäter anhand seines Verhaltensmusters in den Sozialen Medien, seinem Kaufverhalten bei Online-Händlern und seinen Google-Suchanfragen im Vorfeld identifiziert werden? Wie könnten Raubüberfälle auf Banken in unterschiedlichen Polizeibezirken mit dem Mieten von Pkws eines bestimmten Anbieters, der Registrierung von drei bestimmten Rufnummern in Funkzellen-Nähe des Tatorts sowie dem Kauf von Alkohol mit einer personalisierten Bonuskarte in einem bestimmten Supermarkt in Verbindung gebracht werden? Die Lösung lautet: Big Data. Dieses Phänomen beschreibt die enorm schnelle analytische Verarbeitung großer Datenmengen in hoher Geschwindigkeit. Die hierzu verwendeten Methoden der Künstlichen Intelligenz setzen dabei dort an, wo herkömmliche Werkzeuge der Datenverarbeitung an ihre Grenzen stoßen. Sie ermöglichen es, unstrukturierte Daten (Text-, Bild-, Video- und Audiodateien) in einem noch nie dagewesenen Umfang zu analysieren, Muster oder Zusammenhänge zwischen ihnen zu erkennen und letztlich Aussagen über die Vergangenheit, Gegenwart und insbesondere die Zukunft abzuleiten.

Zusätzliche Datenquellen einbeziehen

Ähnliche Anwendungen werden bereits von einigen deutschen Polizeibehörden genutzt. Predictive Policing, also die "vorausschauende Polizeiarbeit", zielt darauf ab, das Delikt des Wohnungseinbruchdiebstahls räumlich-zeitlich vorherzusagen. Bei diesen Analysen handelt es sich jedoch eher um "Small Data".
Die "intelligente Datenverarbeitung" im Kontext von Big Data würde es erlauben, neben den bisher verwendeten (polizeilichen) Daten weitere Datenquellen einzubeziehen. Durch die Verarbeitung von Daten zu Wetterbedingungen, Feier- und Ferientagen, Veranstaltungen oder zur Verkehrslage ließen sich weitaus umfassendere Analysen durchführen. Besonders interessant wäre dabei die Verknüpfung mit personenbezogenen Daten, wie die Nutzung von Open Source Intelligence (OSINT), also öffentlich zugänglichen Informationen aus den Sozialen Medien Facebook, Twitter und Instagram (etwa Lichtbilder, Kontakte, Aufenthaltsorte, persönliche Einstellungen und Meinungen). Auf diese Weise ließen sich neue polizeilich relevante Erkenntnisse gewinnen, menschliche Verhaltensmuster erkennen, neue Kriminalitätsmuster identifizieren und letztlich (personenbezogene) Prognosen über künftige Straftaten erstellen.

Fokus nicht nur auf der Gefahrenabwehr

Neben Anwendungsmöglichkeiten im Bereich der Gefahrenabwehr spielt Big Data auch im Bereich der Strafverfolgung eine wesentliche Rolle. Mit der Generierung immer größerer Datenmengen und den fortschreitenden technologischen Entwicklungen wie dem Internet der Dinge wird der Umfang zu analysierender und als Beweismittel zu sichernder Daten stetig zunehmen. Hinzu kommt, dass häufig unstrukturierte Daten (zum Beispiel Bilder, Videos, Textinhalte aus WhatsApp- und Facebook-Nachrichten oder E-Mails) zeitnah ausgewertet werden müssen, was die Ermittler oft vor große Herausforderungen stellt. In dieser Hinsicht könnten Big-Data-Analysen die kriminalpolizeiliche Ermittlungsführung entscheidend unterstützen.
Als moderne Ermittlungsmethode würden sie das schnelle Filtern enorm großer Mengen von Daten aus unterschiedlichen Quellen ermöglichen und damit personal- und zeitintensive Recherchearbeiten automatisieren. In einem mit Künstlicher Intelligenz ausgestatteten System ließen sich zum Beispiel die für das Verfahren auszuwertenden Massendaten zeitnah auf ermittlungsrelevante Inhalte reduzieren, Zusammenhänge herstellen oder Netzwerkstrukturen abbilden. Dies kann insbesondere für umfassende Ermittlungen in den Bereichen Cyber-Kriminalität, Organisierte Kriminalität (OK) und Terrorismus von großer Bedeutung sein.

Polizeiarbeit würde verbessert

Mit Blick auf ihr Anwendungspotenzial und ihre unbestreitbaren Möglichkeiten versprechen Big-Data-Analysen eine Verbesserung traditioneller Polizeiarbeit. Sie bieten der Polizei die Chance, Effektivität und Effizienz ihres Handelns zu steigern und sich insbesondere zukunftsorientiert auszurichten. Dennoch dürfen die anhaftenden Gefahren nicht außer Acht gelassen werden. Insbesondere in datenschutzrechtlicher Hinsicht bergen Big-Data-Analysen mit personenbezogenen Daten hohe Risiken für die informationelle Selbstbestimmung.

Sicherung elektronischer Beweise in der Cloud: internationale Lösungen

► **Alexander Seger, Exekutivsekretär des Komitees der Konvention zur Computerkriminalität des Europarats**
Dieser Beitrag gibt nicht notwendigerweise die Meinung des Europarats wieder.


Foto: privat

Cyber Crime – Straftaten gegen und über Computer – stellt ohne Frage eine Bedrohung fundamentaler Werte und Interessen unserer Gesellschaften und der Rechte Einzelner dar. Darüber hinaus können Beweise in Bezug auf Betrug, Korruption, Mord, Vergewaltigung, Terrorismus, sexuellen Missbrauch von Kindern und in der Tat jede Art von Straftat elektronischer Natur sein.

Bedrohungen dieser Art werden wahrscheinlich mit dem "Internet of Everything" und dem Einsatz Künstlicher Intelligenz für automatisierte und gezielte Angriffe und in einem angespannten internationalen Kontext – in dem über Cyber-Angriffe und Desinformationsoperationen politische Interessen verfolgt werden – weiter zunehmen.

Begrenzte Befugnisse der Strafverfolgungsbehörden

Die Sicherung elektronischer Beweise durch Strafverfolgungsbehörden ist notwendig, um die Rechtsstaatlichkeit zu gewährleisten und die Rechte Einzelner zu schützen. Dabei sehen sich Strafverfolgungsbehörden komplexen Herausforderungen gegenüber. Dazu gehören, neben der gewaltigen Zahl von Straftaten und den damit verbundenen Geräten, Nutzern und Opfern, die Verschlüsselung, Anonymisierungsdienste sowie die transnationale Natur von Computerkriminalität und elektronischen Beweisen. Während Daten und damit elektronische Beweise "irgendwo in der Cloud" liegen, sind die Befugnisse von Strafverfolgungsbehörden territorial begrenzt. Im Ergebnis muss man davon ausgehen, dass in den meisten Ländern weniger als ein Prozent der Computerstraften strafrechtlich verfolgt wird. Das Vertrauen in die Effizienz der Strafjustiz in diesem Bereich ist entsprechend gering.

Der Europäische Gerichtshof für Menschenrechte hat 2008 in der Entscheidung "K. U. v. Finland" festgestellt, dass Staaten dazu verpflichtet sind, aktiv die Rechte Einzelner auch gegen Computerkriminalität und auch mit den Mitteln des Strafrechts zu schützen. Es ist fraglich, ob Staaten dieser positiven Verantwortung gerecht werden.

Jedoch gehen Entscheidungen nationaler und europäischer Gerichte tendenziell dahin, die Befugnisse von Strafverfolgungsbehörden weiter zu begrenzen. Gleichzeitig werden nationalen Sicherheits- und Nachrichtendiensten von Gerichten größere Spielräume zugestanden. Ähnlich wie bei der Bekämpfung des Terrorismus werden sich auch bei der Computerkriminalität mehr Befugnisse auf diese Dienste verlagern. Ob dies im Interesse des Rechtsstaats ist, ist zu bezweifeln.

Internationale Lösungen erforderlich

Auf internationaler Ebene ist die Budapest-Konvention zur Computer-Kriminalität des Europarats das wichtigste Instrument für die Zusammenarbeit in diesem Bereich. Derzeit gehören 63 Staaten diesem Vertrag an, neben europäischen Staaten auch Australien, Japan, Kanada, USA und andere Länder in Afrika, Asien und Lateinamerika.

Seit 2017 wird ein Zusatzprotokoll verhandelt, das Polizeibehörden die Möglichkeit geben soll, elektronische Beweise effizienter und auf solider rechtlicher Grundlage zu sichern – auch in der Cloud.

Neben Maßnahmen der schnelleren Rechtshilfe wie der 24/7-Erreichbarkeit auch der für die internationale rechtliche Zusammenarbeit zuständigen Stellen gibt es zwei Bereiche, für die es bisher keine klare Grundlage gab, nämlich die Möglichkeiten,

1. Stammdaten direkt bei einem Anbieter in einer anderen Vertragspartei anzufordern;

2. die Durchsuchung auf einen Computer in einer anderen Vertragspartei auszuweiten, beispielsweise, indem die Polizei über den offenen Computer eines Verdächtigen auf dessen Webmail oder Cloudkonto zugreift.

Beides wird bereits von den Behörden vieler Länder praktiziert, ist aber kaum geregelt und die dabei erhobenen Daten sind daher oft vor Gericht nicht zulässig. Hier Regelungen in einem verbindlichen internationalen Abkommen festzuhalten, ist sehr schwierig. Es werden sowohl Fragen der Souveränität von Staaten als auch der Rechte Einzelner berührt. Derartige Lösungen sind daher nur dann möglich, wenn sie durch Grundsätze des Rechtsstaates und des Datenschutzes begrenzt werden.

Trotz der Komplexität der Thematik gibt es keine Alternative zu effektiven internationalen Lösungen, wenn die Rechte Einzelner und der Rechtsstaat auch im "Cyber Space" gelten sollen.

Digitale Polizei in einem digitalen Raum?

► Thomas-Gabriel Rüdiger, Cyber-Kriminologe am Institut für Polizeiwissenschaft der Fachhochschule der Polizei des Landes Brandenburg


Foto: privat

"Ein Teil des Hellfeldes klassischer Kriminalitätsformen ist offensichtlich in das Dunkelfeld moderner Computerkriminalitätsdelikte übergegangen." Zu dieser Schlussfolgerung kommt die Dunkelfelduntersuchung der Polizei des Landes Mecklenburg-Vorpommern im Rahmen des Forschungsberichts 2018. Dabei gehen die Autoren davon aus, dass diese Situation auch ein Grund für die sich seit Jahren positiv entwickelnden Hellfeldzahlen der polizeilichen Kriminalstatistiken sein könnte. Es ist in der Wissenschaft mittlerweile weitestgehend anerkannt, dass es bei allen digitalen Delikten eine wesentlich höhere Dunkelzifferrelation gibt als bei rein analogen Delikten. Während beispielhaft bei Ladendiebstählen angenommen wird, dass von zehn bis 15 Delikten eines zur Anzeige kommt und damit ein relativ hohes Dunkelfeld besteht, liegt diese Quote im digitalen Raum und je nach Delikt im dreistelligen Bereich. Dabei kann auch berücksichtigt werden, dass Menschen einen großen Teil ihres Lebens im digitalen Raum verbringen, je jünger, umso länger. Je weniger Zeit Menschen aber im physischen Raum verbringen, umso weniger Möglichkeiten zur physischen Kriminalität gibt es. Denn nicht selten entsteht Kriminalität auch aus einem Freizeitverhalten heraus. Ein Ergebnis ist dann tatsächlich, dass das Hellfeld dieser Delikte sinkt. Solange das Anzeige- oder Kontrollverhalten im digitalen Raum dann nicht vergleichbar steigt, bleiben diese Delikte wiederum im Dunkelfeld.

Normenkontrolle im digitalen Raum

Dies bedeutet aber auch, dass die Wahrscheinlichkeit, für ein Delikt im digitalen Raum überführt zu werden, offenbar wesentlich geringer ist als im physischen Raum. Warum sollte dann beispielsweise jemand die Risiken von Einbruchsdiebstählen auf sich nehmen, wenn auch die Möglichkeit besteht, wesentlich risikofreier digitale Vermögensdelikte zu begehen? Ein Resultat dieser Dunkelfelddiskrepanz ist es offenbar, dass das Internet nicht selten als rechtsfrei empfunden wird. Denn es kommt nicht darauf an, ob in einem System Recht gilt, es kommt darauf an, dass der Rechtsbruch mit einer gewissen Wahrscheinlichkeit auch geahndet wird.

Die Normenkontrolle scheint sich im digitalen Raum dabei in einer Art Zwischenphase zu befinden. Auf der einen Seite wird gegenwärtig der Rückgang der generellen Hellfeldzahlen in der PKS insgesamt gesellschaftlich als positiv wahrgenommen. Auf der anderen Seite werden die Ressourcen der Sicherheitsbehörden offenbar nicht in demselben Maßstab in den digitalen Raum verlagert, wie sich die Kriminalität dorthin verlagert hat. Dies zeigt sich an unterschiedlichen Aspekten. Beispielhaft gibt es in Deutschland etwa über 330 polizeiliche Social-Media-Accounts, zum Vergleich sind es in den Niederlanden etwa 2.500 solcher Accounts. Ende 2017 sollen laut Medienberichten nicht einmal ein Prozent der Polizei überhaupt für digitale Themen zuständig gewesen sein. Alleine die Bundeswehr hat in ihrem Cyber- und Informationsraum hingegen knapp sieben Prozent ihres Personals gebündelt. Eine vergleichbare Personaldichte würde bei der Polizei in etwa über 20.000 Polizisten entsprechen.

Ausweitung des Hellfeldes durch Präsenz im digitalen Raum

Der gesellschaftliche Umgang mit dem Internet ähnelt dabei gegenwärtig noch dem Konzept der "Präventivwirkung des Nichtwissens" von Popitz. Je weniger Kriminalität im Netz aufgehellt wird, umso eher geht die Politik davon aus, dass alles unter Kontrolle ist. Eine höhere Personaldichte und auch Sichtbarkeit – bspw. durch virtuelle Polizeistreifen – im digitalen Raum würde nach dem sog. Lüchow-Dannenberg-Syndrom nicht zu einem Rückgang der festgestellten Kriminalität führen. Vielmehr würde es zu einem Anstieg der digitalen Delikte im Hellfeld, aber gleichzeitig und mittelbar zu einer Reduzierung des Dunkelfeldes digitaler Delikte führen. Eine solche Situation wird zwangsläufig auch mit einer sinkenden Aufklärungsquote einhergehen. Diese Entwicklung müsste vor allem die Politik aushalten können. Es bedarf letztlich einer wirklichen Vision, wie ein digitaler Raum ohne physische Grenzen mit einer ähnlich hohen Strafverfolgungswahrscheinlichkeit versehen werden kann wie der physische Raum.

"DIE RESSOURCEN DER SICHERHEITSBEHÖRDEN WERDEN OFFENBAR NICHT IN DEMSELBEN MASSSTAB IN DEN DIGITALEN RAUM VERLAGERT, WIE SICH DIE KRIMINALITÄT DORTHIN VERLAGERT HAT."

Rekrutierung von IT-Fachkräften

► Rainer Kasecker, Projektleiter “Werbeoffensive IuK”, Bayerische Polizei


Foto: privat

Die Bayerische Polizei sorgt mit mehr als 42.000 Mitarbeiterinnen und Mitarbeitern für die Sicherheit im Freistaat. In den kommenden Jahren besteht aufgrund von Pensions- und Renteneintritten und wegen der strategischen und technischen Herausforderungen ein hoher Bedarf an IT-Fachkräften. Damit steht die Bayerische Polizei vor ähnlichen Problemen wie andere öffentliche Arbeitgeber und die freie Wirtschaft. Bereits 2016 befragte eine Marketingagentur im Auftrag des damaligen Bayerischen Staatsministeriums des Innern, für Bau und Verkehr potenzielle Bewerber zu ihrer Auffassung über die Bayerische Polizei als IT-Arbeitgeber. Sie war den Befragten als IT-Arbeitgeber nur wenig bekannt. Das galt insbesondere für die Tätigkeitsfelder des IT-Professionals, des IT-Kriminalisten und des IT-Forensikers.

Bewerbungsprozess als entscheidender Faktor

Die Wechselwilligkeit der befragten “Young und Experienced Professionals” war abhängig von der Attraktivität des “neuen” Arbeitgebers, dessen sozialen Leistungen und gerade bei der Altersgruppe ab 30 Jahren der Vereinbarkeit von Familie und Beruf. Hier zeigte sich das Streben nach langfristigen Arbeitsverträgen als Basis für die weitere Lebensplanung. Allgemein zeichnete sich ab, dass mit geeigneten Marketingmaßnahmen der Bekanntheitsgrad und die Attraktivität der Tätigkeitsfelder und der damit verbundenen IT-fachlichen Herausforderungen pointierter dargestellt werden mussten – eine Grundvoraussetzung, um mit den “Platzhirschen”, den bekannten IT-Dienstleistern, Ideenschmieden und Zukunftsgestaltern, in den Wettbewerb um die besten IT-Fachkräfte eintreten zu können.
Es zeigte sich aber auch, dass die externen Zielgruppen besondere Vorstellungen vom Bewerbungsprozess hatten. Für einen öffentlichen Arbeitgeber durchaus gewöhnungsbedürftig ist die “Sandwich”-Haltung der möglichen Bewerber. Sie stellen sich nicht nur den Anforderungen des Arbeitgebers und hoffen auf eine Anstellung. Sie prüfen ebenso kritisch, ob der öffentliche Arbeitgeber zu ihnen passt und sagen angesichts des großen Angebots an Stellen durchaus auch ab. Überraschenderweise war dabei nicht unbedingt das Gehalt die erste Priorität, sondern welchen Eindruck der künftige Arbeitgeber im Vorstellungsgespräch macht. Nach Analyse der Ergebnisse wurde in der Bayerischen Polizei das Projekt “Werbeoffensive IuK” beauftragt, entsprechende Marketingmaßnahmen zu realisieren. Im Wesentlichen wurden fünf Projektaufgaben gestellt, die stufenweise bis Ende 2020 erfüllt werden sollten.

In Bayern leben – weltweit ermitteln

Zum einen sollten eine nachhaltige Werbekampagne realisiert und hierzu eine professionelle Marketingagentur gewonnen werden. In zwei Stufen wurde 2017 und 2018 diese Werbekampagne konzipiert und umgesetzt (Mehr dazu unter www.mit-sicherheit-anders.de/IT). Da die Einstellungskompetenz für IT-Fachkräfte bei der Bayerischen Polizei verschiedenen Polizeibehörden für ihren jeweiligen Verantwortungsbereich übertragen ist, wurde das Projekt beauftragt, eine IT-Bewerberkoordinierungsstelle einzurichten, um ein zentrales Auskunfts- und Bewerbermanagement anzubieten. Gleichzeitig begann die Erhebung und Analyse der Bewerberlage, um einen soliden Überblick insbesondere zur Wettbewerbsstellung der Bayerischen Polizei und zur Wirkung der Werbemaßnahmen zu erreichen.
Ein Online-Verfahren ermöglicht den Bewerbern schnelle und zielgerichtete Bewerbungen. Eine Karriereseite informiert umfassend zum Arbeitgeber Bayerische Polizei und den IT-relevanten Tätigkeitsfeldern. Da die Zielgruppe der Studierenden an IT-relevanten Hochschulen seit Langem im operativen Fokus der Mitbewerber um IT-Fachkräfte steht, wurde eine Präsenz der Bayerischen Polizei als IT-Arbeitgeber an Hochschulen konzipiert und wird ab dem Wintersemester 2019/2020 zunächst im Rahmen eines Piloten an der Technischen Hochschule Georg Ohm in Nürnberg durchgeführt. Schwerpunkte sind hier Praktikumsangebote und die Betreuung von akademischen Abschlussarbeiten durch IT-Spezialisten in der Bayerischen Polizei. Seit Anfang August 2017 – dem Zünden der ersten Stufe der Marketingmaßnahmen – haben sich bei der Bayerischen Polizei mehr als 3.000 IT-Fachkräfte beworben.

“BEWERBER STELLEN SICH NICHT NUR DEN ANFORDERUNGEN DES ARBEITGEBERS UND HOFFEN AUF EINE ANSTELLUNG. SIE PRÜFEN EBENSO KRITISCH, OB DER ÖFFENTLICHE ARBEITGEBER ZU IHNEN PASST UND SAGEN ANGESICHTS DES GROSSEN ANGEBOTS AN STELLEN DURCHAUS AUCH AB.”

EC3 – ein erfolgreiches Konzept

► Steven Wilson, Leiter des EC3 bei Europol


Foto: Europol

Cyber-Kriminalität ist eine sehr schnell wachsende, grenzüberschreitende Verbrechensform, die substanzielle wirtschaftliche Schäden verursacht. Die Bedrohungen sind vielfältig und reichen von der Erpressung durch Verschlüsselungssoftware über Datendiebstahl, den Online-Kreditkartenbetrug, Schadsoftware-Angriffen auf Bankomaten bis hin zu kriminellen Aktivitäten im Darknet. Während cyber-kriminelle Aktionen früher oft relativ kostspielig waren und solche Aktivitäten im Regelfall auch über die technischen Kapazitäten von traditionellen Kriminellen hinausgingen, ist mittlerweile ein Markt für illegale digitale Dienste und Leistungen entstanden, der zu einer gewinnorientierten Industrialisierung der Cyber-Kriminalität geführt hat. So lassen sich beispielsweise Botnetze für diverse kriminelle Aktivitäten wie die Verbreitung von Schadsoftware oder DDoS-(Distributed Denial of Service)Attacken mieten.

Es gibt eine Reihe von Faktoren, welche die erfolgreiche Durchführung von Ermittlungsverfahren, vor allem im Bereich der Cyber-Kriminalität, zusehends erschwert. Dazu gehören, neben rechtlichen Herausforderungen wie zum Beispiel bei der grenzüberschreitenden Zusammenarbeit, der kriminelle Missbrauch der Verschlüsselung, der kriminelle Missbrauch des Darknets, Auswirkungen der Datengrundschutzverordnung auf die WHOIS-Datenbank oder eine fehlende EU-weite Regelung zur Vorratsdatenspeicherung. Diese Faktoren in Kombination mit neuen technischen Entwicklungen wie dem Internet der Dinge oder 5G erzeugen auch eine ständige Herausforderung für Ermittlungsbehörden, das notwendige Wissen, Fähigkeiten und Werkzeuge etwa für die digitale Forensik, Analyse und Ermittlung zu haben.

Kooperation ist Grundbedingung

Die grenzüberschreitende Kooperation ist die Grundvoraussetzung für eine erfolgreiche Bekämpfung der Cyber-Kriminalität, aber auch anderer schwerer und organisierter Verbrechensformen. Es braucht hier das oft zitierte Netzwerk zur Bekämpfung eines Netzwerks. Europol und sein "Europäisches Zentrum für Cybercrime" (EC3) spielen eine sehr wichtige Rolle bei der Bereitstellung eines solchen Netzwerks für die erfolgreiche Unterstützung von EU-Mitgliedsstaaten bei der Bekämpfung des schweren organisierten Verbrechens und des Terrorismus. Neben Informationen sind es auch diverse Werkzeuge, Dienste und natürlich die Zurverfügungstellung von Expertise, die bei der Unterstützung von komplexen Ermittlungsverfahren zum Tragen kommt. Der operative Fokus des EC3 liegt dabei auf der Hi-Tech-Kriminalität, dem Zahlungsmissbrauch, dem Kindesmissbrauch, dem kriminellen Missbrauch des Darknets sowie der digitalen und Dokumenten-Forensik.

Die Unterstützung über Öffentlich Private Partnerschaften ist ein weiteres wesentliches Element der erfolgreichen, aktiven und nachhaltigen Bekämpfung der Cyber-Kriminalität. Hier sind wir in der glücklichen Lage, mit unseren unterschiedlichen Beratungsgruppen erfolgreich kooperieren zu können. Außerdem besteht hier auch die Bereitschaft zur aktiven Partizipation. Ein konkretes und sehr erfolgreiches Beispiel dafür, was man damit erreichen kann, ist die No-More-Ransom-Initiative. Vor über zwei Jahren zusammen mit der niederländischen Polizei und zwei Industriepartnern ins Leben gerufen, bietet dieses Portal nicht nur relevante Informationen an, sondern stellt mehr als 60 Werkzeuge zur freien Entschlüsselung von über 100 Arten von Verschlüsselungsschadsoftware zur Verfügung.

Bei der Bekämpfung der Cyber-Kriminalität sind – wie erwähnt – auch das technische Wissen und die Expertise ausschlaggebend. Hier gilt es, sowohl in der Aus- und Weiterbildung sicherzustellen, dass wir die benötigte Top-Level-Unterstützung bei Ermittlungsverfahren zur Verfügung stellen können. Dazu zählen als Beispiel die Unterstützung hinsichtlich des kriminellen Missbrauchs von Verschlüsselung oder bei der Analyse von Kryptowährungen, inklusive Werkzeugen und Diensten, die den Mietgliedsstaaten hier zentral zur Verfügung gestellt werden können.

Es ist auch zu erwähnen, dass die operative Unterstützung ein enges Zusammenspiel mit dem strategischen und taktischen Bereich benötigt. Dazu gehört neben der Analyse krimineller Verfahrensweisen und Trends auch die Bewertung von neuen und zukünftigen Technologien. Das Ziel soll sein, einen proaktiven, umfassenden und effektiven Ansatz der Ermittlungsbehörden zu ermöglichen.

Nicht auf Erfolgen ausruhen

Europol und das EC3 und seine vielen verschiedenen Partner in den Bereichen Strafverfolgung, Industrie und Wissenschaft sind ein Paradebeispiel für die Möglichkeiten einer vernetzten Reaktion auf Cyber-Kriminalität. Das erlaubt allen Partnern, zu koordinieren, priorisieren und zusammenzuarbeiten. Wir haben hier eine Vertrauensbasis, die international operative Erfolge wie die kürzlich erfolgte Schließung zweier großer Darknet-Marktplätze ermöglicht. Wir können uns aber auf den Erfolgen nicht ausruhen, sondern müssen nach verbesserten und neuen, innovativen Ansätzen und Möglichkeiten suchen, um zusammen für die zukünftigen Bedrohungen geeignet gewappnet zu sein.

Was kann eine Hochschule für Behörden an Unterstützung leisten?

► Prof. Dr. Dirk Labudde, Professor für angewandte Computer- und Biowissenschaften an der Hochschule Mittweida


Foto: privat

Die Digitalisierung macht auch vor der alltäglichen Arbeit der Ermittlungsbehörden keinen Halt. Dabei denkt man in erster Linie an die aufwendige Auswertung von mobilen Endgeräten oder die Probleme mit digitalen Massendaten. Neben diesen Herausforderungen können die Entwicklungen im Bereich Digitalisierung jedoch auch neue Herangehensweisen und Konzepte bedingen. Gerade der Einsatz neuer Technologien, wie Drohnen, 3D-Scanner oder Modellierungssoftware, erlauben eine neue Umsetzung der hypothesengetriebenen Prozesse in der Ermittlung. Es stellt sich die Frage nach neuen und belastbaren Allianzen, z. B. zwischen staatlichen und behördenbetriebenen Hochschulen und Instituten. Eine Allianz auf den Gebieten der Aus- und Weiterbildung und der Forschung.

Strategische Verbünde zwischen Forschung und Verwaltung

Eine Hochschule oder Universität ist per Definition ein Ort, an dem Lehre und Forschung stattfinden sollen. Viele Behörden in Deutschland haben eigene Hochschulen beziehungsweise Universitäten. In der letzten Dekade ist das Zusammenwachsen in Forschung, Lehre und Aus- und Weiterbildung der verschiedenen Einrichtungen vermehrt zu beobachten und als durchweg positiv zu bewerten. Das vieldiskutierte Phänomen der Cyber-Kriminalität zieht zum einen neue Aus- und Weiterbildungsprogramme nach sich, aber zum anderen auch strategische Verbünde in Forschung und Entwicklung. Die Hochschule Mittweida kann auf mittlerweile langjährige Kooperationen mit Behörden und Institutionen der Strafverfolgung zurückblicken. Eine der wichtigsten Ebenen der Zusammenarbeit ist Vertrauen. Es bildet die Basis für den notwendigen Erfahrungs- und Informationsaustausch.
Auch wenn Behörden und Hochschulen unterschiedliche gesellschaftliche Aufgaben erfüllen, besteht die Möglichkeit einer zielführenden Zusammenarbeit. Hochschulen verfügen über ein Portfolio an theoretischem Wissen und konzeptionellen Umsetzungen. Das Wissen und der Umgang mit neuen Technologien, nicht nur in Zusammenhang mit der Digitalisierung, können in die Aus- und Weiterbildung integriert werden und speziell auf die Bedürfnisse der Ermittlungsbehörden angepasst werden. Jedoch muss dieser Prozess begleitet werden, da sonst die Gefahr von Frustration auf beiden Seiten entsteht. Oft mangelt es an einer gemeinsamen Sprache oder es bestehen unterschiedliche Zielsetzungen. Ermittlungsbehörden können oftmals nicht die Angebote von Hochschulen wahrnehmen, da alltägliche Aufgaben die erwartete Regelmäßigkeit aus der Sicht der Hochschulen nicht zulassen. Hier können berufsbegleitende Online-Angebote eine entscheidende Rolle spielen. Auch müssen sich Hochschulen von bewährten Anschlüssen in diesem Bereich trennen, kurze und inhaltlich förderliche Angebote, die mit den Weiterbildungsanerkennungen innerhalb von Behörden einhergehen, müssen die Normalität darstellen. Nur so kann das erforderliche Wissen gerade im Phänomenbereich Cyber Crime schnell bereitgestellt werden.

Hochschule leistet operative Ermittlungsunterstützung

Vor fünf Jahren war es sicher noch undenkbar, dass eine staatliche Hochschule wie Mittweida aktive operative Ermittlungsunterstützung leistet. Auch hier spielt das gegenseitige Vertrauen, neben der fachlichen Kompetenz, die entscheidende Rolle. Das Forensic Science Investigation Lab (FoSiL) der Hochschule Mittweida arbeitet seit 2015 aktiv mit Behörden in Ermittlungsverfahren zusammen und ist als Sachverständiger vor Gericht in zahlreicheichen Fällen vertreten. Der Benefit für beide Seiten kann deutlich beziffert werden. Behörden können entlastet werden und haben mit FoSiL einen fachlich unabhängigen Partner beim Einsatz neuer Methoden und Strategien. Auf der anderen Seite kann FoSIL Neuentwicklungen und wissenschaftliche Erkenntnisse realistischen Praxistests unterziehen. Auch wenn oft im Rahmen von Ermittlungen noch Anpassungen vorgenommen werden müssen, ist die Erfolgsbilanz positiv. Die Erkenntnisse und Ergebnisse aus den gemeinsam durchgeführten Verfahren bilden den Input für Weiterbildungen. Nur so ist es möglich, aktuelles Wissen und den Umgang mit neuen Technologien zeitnah in die alltägliche Fallarbeit zu integrieren.

“AUCH WENN BEHÖRDEN UND HOCHSCHULEN UNTERSCHIEDLICHE GESELLSCHAFTLICHE AUFGABEN ERFÜLLEN, BESTEHT DIE MÖGLICHKEIT EINER ZIELFÜHRENDEN ZUSAMMENARBEIT.”

Seminare der Cyber Akademie **für die Polizei**

Sicherheit durch **Know-how**

Datenschutz und Informationssicherheit
aktuell und praxisnah vermittelt

Seminar-Highlights **2019**

Ermittlungen

- **Dem Phänomen „Innentäter“ auf der Spur**
  18.09.2019, Frankfurt am Main
- **Einführung in Kryptowährungen – Funktionsweise, Nutzung, Nachverfolgung**
  24.09.2019, Bonn
- **Praxis-Kurs Darknet: Grundlagen, Einführung und Recherche**
  12.11.2019 – 13.11.2019, Berlin
- **Praktische Open-Source-Recherche für Ermittler**
  05.12.2019, Düsseldorf

Polizei und Datenschutz

- **Personalrat und Datenschutz**
  19.09.2019, Hannover
- **Datenschutz bei der Polizei - EU-DSGVO, BDSG-Neu, RI-Richtlinie & Co.**
  04.12.2019 – 05.12.2019, Berlin

Forensik

- **Smartphones - digitale Spuren, Analyse und Ermittlungen**
  04.09.2019 – 06.09.2019, Bonn
- **Netzwerkforensik IPv6**
  17.09.2019 – 18.09.2019, Frankfurt am Main
- **IT-Forensik für Einsteiger und Aufsteiger**
  05.11.2019 – 07.11.2019, Bonn

CAk Cyber Akademie

Allianz für Cyber-Sicherheit Partner

Die Cyber Akademie ist Partner der Allianz für Cyber-Sicherheit

www.cyber-akademie.de