Positionspapier – Cybercrime

Präambel:
Bei der Bayerischen Polizei hat sich die Bekämpfung der Cyberkriminalität seit dem Jahr 2010 grundlegend gewandelt. So wurden seit dem Jahr 2011 mehrere Kontingente von IT-Kriminalisten eingestellt und zu polizeilichen Sachbearbeitern ausgebildet. Im Jahr 2017 wurden bayernweit bei allen Kriminalpolizeidienststellen neue Kommissariate 11 bzw. Cybercrime eingerichtet.

Der BDK LV Bayern hat sich federführend sowohl für die Einführung der neuen Laufbahnen als auch der neuen Kommissariate 11 eingesetzt.
Um nun die aktuelle Situation bei der Bekämpfung von Cyberkriminalität kennen zu lernen und weitere Optimierungsvorschläge machen zu können, wurde durch den BDK LV Bayern eine Arbeitsgruppe Cybercrime eingerichtet. Diese sollte neben einer Bestandsaufnahme auch Vorschläge für Verbesserungen zu unterschiedlichsten Gesichtspunkten erarbeiten.
Im Zuge der Tätigkeit der Arbeitsgruppe wurde auch eine Mitgliederbefragung durchführt, in welcher die Mitglieder, die im Bereich Cybercrime tätig sind, nicht nur vorgegebene Fragen beantworten, sondern auch eigene Anregungen einbringen konnten.

Aktuelle Situation:
Während es beim LKA, PP Mittelfranken und dem PP München eigene Cybercrime-Dezernate gibt, erfolgt die Bekämpfung der Cyberkriminalität bei den Flächen-Präsidien durch die erst kürzlich eingeführten Kommissariate 11 bei den Kriminalpolizeiinspektionen. Dort sind neben den IT-Kriminalisten auch Polizeibeamte mit klassischer Polizeiausbildung tätig.
Abhängig vom konkreten Präsidium unterscheiden sich Stärke und Aufgaben dieser Kommissariate. Teilweise wurden entsprechend der Konsensentscheidung der Verbände bereits die RBA-s in die K11 integriert.

- IT-Kriminalisten -
Eine durchgeführte Befragung bei den BDK-Mitgliedern im Cybercrime-Bereich ergab, dass einerseits zwar die Arbeit auf den Cybercrime-Dienststellen durch den Einsatz der IT-Kriminalisten effektiver gestaltet wird, jedoch die IT-Kriminalisten nur selten ihr Fachwissen in die Sachbearbeitung einfließen lassen können [1].

Im Zuge der Befragung sollten die Teilnehmer auch ihre Tätigkeiten in Kategorien (z.B. Fortbildung, Unterstützung und Sachbearbeitung von einfach gelagerten Fällen bzw. von qualifizierten Fällen) einteilen und die dazu verwendeten Arbeitsstunden pro Woche angegeben. Bei der Auswertung der Angaben der IT-Kriminalisten fällt Folgendes auf [2]:

Für die Unterstützung von anderen Kollegen wenden diese im Durchschnitt bereits ca. 13 Stunden pro Woche auf. Weitere 13 Stunden pro Woche erfordert die Bearbeitung von einfach gelagerten Fällen. Dazu kommen 6 Stunden für die Bearbeitung von fachfremden Fällen und lediglich 5 Stunden für die Bearbeitung von qualifizierten Fällen.

Für die im schnelllebigen Bereich der Informationstechnologie notwendig Fortbildung im Selbststudium verbleiben nur ca. 3 Stunden pro Woche.

Bund Deutscher Kriminalbeamter Landesverband Bayern
Gebhardtstr. 7 | D-90762 Fürth/Bay
Tel.: +49 (0) 911.4229909 (0) 911.429290
E-Mail: lv.bayern@bdk.de | Internet: www.bdk.de

- Auf Basis der Rückmeldungen lässt sich sagen, dass die IT-Kriminalisten derzeit ca. 50% ihrer Arbeitszeit mit der Bearbeitung einfach gelagerter Fälle beschäftigt sind, wofür deren Fachwissen in den seltensten Fällen notwendig wäre. Die fehlende Zeit bei der Sachbearbeitung von qualifizierten Fällen führt entweder zur Verzögerung der Ermittlungen, einer unnötig langen Bearbeitungsdauer oder zu einem Verzicht von bestimmten Ermittlungsschritten.

Aus Sicht des BDK müssen die IT-Kriminalisten effektiver genutzt werden. Derzeit wird weder das Fachwissen, noch das technische Potential der Beamten auch nur annähernd ausgenutzt.

- ***Der BDK fordert daher, die IT-Kriminalisten nur noch im Bereich der qualifizierten[1] Sachbearbeitung und der fachlichen Unterstützung der Kollegen aus anderen Kommissariaten bzw. im Bereich der IT-Forensik zu verwenden.***

Dieser Punkt muss eigentlich selbstverständlich sein, immerhin wird mit dieser Aufgabenbeschreibung in der Werbeoffensive „Mit Sicherheit anders – IT Kriminalist" geworben.

- Organisation -
Aus Sicht des BDK ist eine Zusammenlegung von IT-Forensik (RBA) und den Cybercrimedienststellen zwingend erforderlich. Die bestehende Konsensentscheidung ist endlich mit Vorrang bayernweit praktisch umzusetzen.

Unterstützt wird diese Forderung durch die Erkenntnisse aus der Erhebung:
Im Zuge der Befragung zeigte sich, dass die Kriminalbeamten mit der derzeitigen Verfahrensweise bei der Auswertung von digitalen Spuren nicht zufrieden sind. Das liegt unter anderem daran, dass die RBA zwar die Daten der sichergestellten EDV-Geräte sichert und diese mit „Viewer"-Software zur Verfügung stellt.
Die Bewertung bzw. Sichtung dieser Daten muss jedoch nach wie vor durch die Sachbearbeiter erfolgen. Diese haben dabei Probleme wie z.B. fehlendes Equipment (z.B. Blu-ray Laufwerk in den Auswertelaptops) oder fehlende Erfahrung bei der Handhabung der sich ständig weiterentwickelnden „Viewer"-Programme.

Da die K11 bereits unterstützend im IT-Bereich den anderen Kommissariaten zur Seite stehen scheint es sinnvoll, die Bewertung der digitalen Spuren durch die IT-Kriminalisten in den K11 auftragsbasiert für die anderen Kollegen der KPI durchführen zu lassen. Dazu ist jedoch ausreichend Personal und geeignetes Equipment notwendig. Dies könnte zudem zur Entlastung der Kollegen der gesamten Kriminalpolizeiinspektion und zur Einsparung an Auswertungsequipment führen.
Die Landespolizei Baden-Württemberg setzt schon seit einigen Jahren auf studierte Informatiker im Bereich der Datenanalyse, welche zwischen den Forensiker der RBA und den kriminalpolizeilichen Sachbearbeitern angesiedelt sind.

[1] Unter qualifizierten Fälle der Cyberkriminalität werden z.B. Serien von Ransomware und „Fake-Shop"-Fällen, Fälle des Computerbetrugs im Zusammenhang mit dem Onlinebanking, DDOS-Attacken und „Einbrüche" in Firmennetzwerke bzw. Servern verstanden.

Um die neugegründeten Kommissariate 11 für die Zukunft effizient aufstellen zu können, stellt der BDK aus fachlicher Sicht die folgenden Forderungen:

- Die **Hauptaufgabe** der K11 muss in der **Unterstützung** der anderen Kommissariate im Bereich der Informationstechnologien liegen. Das könnte z.B. Aufbereitung und Auswertung von Massendaten, Durchführung von OSINT-Recherchen und Ermittlungen im Zusammenhang mit Kryptowährungen sein.

- Im Bereich der Sachbearbeitung werden nur noch **qualifizierte** Fälle von **Cybercrime** durch die K11 bearbeitet. In Fällen klassischer Kriminalität, die aufgrund der Begehungsweise umfangreiche technische Kenntnisse voraussetzen, stehen die K11 unterstützend zur Verfügung.

- Diese beiden Punkte sind **bayernweit einheitlich** und **verbindlich** zu regeln.

- Die Finanzierung der K11 muss nachhaltig erfolgen und nicht durch einmalige Sondermittel. Gerade beim verwendeten EDV-Equipment zeigt sich, die rasche Fortentwicklung im Bereich der IT. Durch eine nachhaltige Finanzierung kann gewährleistet werden, dass sich das vorhandene Equipment auf einem Stand befindet, welcher notwendig ist um auf die aktuellen Anforderungen von Programmen oder fallbezogene Situationen agieren zu können.

Um eine effektive Datenanalyse zu ermöglichen muss es möglich sein, studierte Informatiker als Datenanalysten einstellen zu können. Eine Notwendigkeit für solche Stellen wurde bei den befragten Kriminalbeamten gesehen und diese konnten sich auch den Einsatz der IT-Kriminalisten in diesem Bereich vorstellen. Daher wird die Schaffung von weiteren Dienstposten für ausgewiesene Datenanalysten-Stellen bei den Dienststellen gefordert.

Die wenigsten eingestellten IT-Kriminalisten haben bei ihrer Einstellung Kenntnisse im Bereich der Computerforensik. Jedoch hat nahezu jeder studierte Informatiker „Erfahrungen" in den Bereichen Datenbanken und Programmierung. Speziell aufgrund der zunehmenden Datenmengen aus z.B. sichergestellten Asservaten ist heutzutage eine Bearbeitung, Visualisierung und ein Korrelieren von sog. Massendaten notwendig. Da „eingekaufte" Software meist nicht bezahlbar bzw. nicht einsetzbar ist, sind fallbezogene Individuallösungen notwendig. „Gehypte Universallösungen", die seitens der Industrie angeboten werden, müssen kritisch getestet werden.

- Fortbildung -
Damit die IT-Kriminalisten und die Kriminalbeamten in den Cybercrime-Dienststellen in dem sich rasant ändernden Feld der IT auf dem Laufenden bleiben können, ist eine ständige und nachhaltige Fortbildung notwendig.
Da Fortbildungen mit externen Referenten sehr teuer sind, kann dieser Ansatz aus Sicht des BDK bayernweit nicht als zielführend für die Fortbildung im Bereich Cybercrime angesehen werden.
Hierbei ist es aus Sicht des BDK sinnvoller, den bereits mehrmals geforderten Ausbau des BPFI anzugehen und eine Finanzierung von weiteren Dienstposten für den Bereich Cybercrime zu ermöglichen. Durch die Befreiung der K11 von der Bearbeitung von einfach gelagerten bzw. fachfremden Fällen steht den Beamten mehr Zeit zum Selbststudium zur

Verfügung. Im Zuge diesem Selbststudium könnte an Webinare von internen (BPFI) als auch externen Stellen (z.B. Europol) zu Themen der Cyberkriminalität teilgenommen werden.
Um eine weitere effektive Fortbildung durch das BPFI leisten zu können, müssen die „Cybercrime"-Kurse vom Fortbildungskontingent der Kriminalpolizeidienststellen losgelöst sein, wie es im Falle der RBA-Kurse schon lange Zeit üblich ist.

Um eine nachhaltige und zukunftsfähige Fortbildung zu ermöglichen muss daher:

- ein weiterer Ausbau (inkl. neuer und hochwertiger Stellen) des BPFI im Bereich der Cyberkriminalität erfolgen. Diese seit dem ersten Cybercrime-Konzept bestehende Forderung ist endlich umzusetzen.

- eine Erstellung von interaktiven Lehrmaterialien durch das BPFI zum Thema Cyberkriminalität möglich sein und diese muss für die Kollegen im Selbststudium über das E-Learning-Portal abrufbar sein.

- Die Teilnahme an Fortbildungen am BPFI im Bereich Cyberkriminalität unabhängige vom Dienststellenkontingent möglich sein.

Fazit:
Damit die Bayerische Polizei weiterhin der "Garant für die Sicherheit" bleibt, ist nicht nur eine Weiterentwicklung der derzeitigen Bekämpfungsstrategien im Bereich Cybercrime notwendig, sondern auch eine Anpassung der bestehenden Organisationsstrukturen und Fortbildungsmöglichkeiten unabdingbar.
Die in diesem Papier vorgestellten Vorschläge und Forderungen stellen aus Sicht des BDK wichtige Punkte dar, welche in Angriff genommen werden müssen, um dies zu gewährleisten.

Literatur:
1. Arbeitspapier „Auswertung Fragebogen AG Cybercrime" von Dominik Dommer
2. Arbeitspapier „Einsatz Cybercops" von Christian Hainzinger