Gewerkschaft der Polizei NRW

31. Januar 2019

Forderungspapier der GdP NRW

zur

Bekämpfung Cybercrime

Gewerkschaft der Polizei NRW

A. Situation

Die aktuell bekannt gewordenen „Hackerangriffe“ auf die Daten von Abgeordneten des nordrhein-westfälischen Landtags sowie anderer Parlamente zeigen dringenden Handlungsbedarf auch für die Polizei in Nordrhein-Westfalen auf.

Bereits seit Längerem weisen wir darauf hin, dass der Umfang des Ermittlungsbereiches „Cybercrime“ hohe Wachstumsraten aufweist. Enorme Datenmengen und die Sicherung sowie Auswertung dieser stellen die Polizei in NRW vor ständig wachsende Herausforderungen. Das erforderliche qualifizierte Personal fehlt, da es entweder nicht gewonnen werden oder nicht dauerhaft gebunden werden kann. Die dringend benötigten Sachbearbeiter für „IT-Forensik“ und „Cyberdelikte“ sind nicht oder nicht in erforderlicher Anzahl vorhanden.

B. Forderungen

Die GdP NRW hält es daher für dringend erforderlich, Sofortmaßnahmen und auch kurzfristige Maßnahmen zur Optimierung der Aufgabenwahrnehmung zu ergreifen.

1. Sofortmaßnahmen

Nutzung von 75 vorhandenen Stellen (Regierungsbeschäftigte) zur sofortigen Personalgewinnung und schnellstmögliche Schaffung von 75 zusätzlichen Planstellen (Beamte) für Sachbearbeiter „IT-Forensik“, um eine unverzügliche Verbeamtung dieses Personals im Polizeibereich zu ermöglichen.
Sofortige Konzeption und Durchführung von zusätzlichen Arbeitstagungen und Seminaren für die jeweiligen Zielgruppen in der Polizei zu den unterschiedlichen Facetten von Cybercrime unter Einbeziehung von polizeiexternem Expertenwissen. Hierfür müssen zusätzliche Lehrende in der Fortbildung sowie zusätzliche Hausmittel – insbesondere für die Vergütung von polizeiexternen Dozenten (Experten) – zur Verfügung gestellt werden.

2. Kurzfristige Maßnahmen

Überprüfung des Vergütungssystems sowohl im Besoldungs- als auch im Tarifbereich. Ermöglichung von Fachkarrieren. Optimierung der Aus- und Fortbildung in Gänze.

C. Erläuterungen

1. Die unter den Sofortmaßnahmen geforderten 75 Stellen mit Möglichkeit zur Verbeamtung im Polizeiverwaltungsbereich berechnen sich wie folgt:

- 3 je Kriminalhauptstelle gem. § 2 KHSt-VO = 48
- zusätzlich je 2 für die Kriminalhauptstellen mit Aufgaben gem. § 4 KHSt-VO = 12
- 15 beim LKA NRW

Die beamten- und laufbahnrechtlichen Voraussetzungen für diese Laufbahn besonderer Fachrichtung existieren bereits - § 8 Landesbeamtengesetz NRW (LBG NRW) i.V.m. § 16 Verordnung über die Laufbahnen der Beamtinnen und Beamten im Land Nordrhein-Westfalen (LVO NRW) -.

Es besteht ein hoher Informationsbedarf in den unterschiedlichen Bereichen der Polizei zu dem Thema „Cybercrime“. Es darf nicht sein, dass auf aktuelle Entwicklungen im Bereich Cybercrime nicht angemessen reagiert werden kann, weil erforderliche Fortbildungsmaßnahmen nicht zeitgerecht durchgeführt wurden. Der Anspruch auf Erhalt und Besuch dieser Veranstaltungen muss festgeschrieben sein. Dies gilt auch für die Fachleute im Bereich der Bekämpfung der Cybercrime, also auch für die zukünftig zu gewinnenden Fachleute. Hier muss ein verbindliches Fortbildungskonzept greifen, damit diese Fachleute dauerhaft auf dem aktuellen Stand der Technik bleiben. Das derzeitige Fortbildungsangebot ist daher deutlich auszuweiten. Auch ist es erforderlich, polizeiexternes Wissen noch stärker einzubeziehen. Die Abwicklung der administrativen Abläufe, Planung und Organisation der Fortbildungsveranstaltungen, Gewinnung von externen hochspezialisierten Referenten etc. muss zentral in einer Hand liegen.

2. Die Anforderungen und Aufgaben der Sachbearbeiterin/Sachbearbeiter „IT-Forensik“ und „Cyberdelikte“ stellen sich für uns wie folgt dar:

a) Sachbearbeiterin/Sachbearbeiter „IT-Forensik“

<u>Anforderungsprofil:</u>

Beamtinnen/Beamte besonderer Fachrichtung der Polizei

mit abgeschlossenen Studium an einer Fachhochschule in einem Fachhochschulstudiengang (Bachelor) der Fachrichtung Informatik oder einem vergleichbaren Abschluss mit fundierten Kenntnissen im Bereich der praktischen Informatik oder einem vergleichbaren Abschluss im Bereich der Datentechnik, guten Kenntnissen im Bereich Rechnerarchitekturen und Betriebssystemen, der Internet- und Verschlüsselungstechnologien und Zertifizierungsverfahren, der Analyse und Abwehr von Netzwerkangriffen sowie Kenntnissen im Bereich internetspezifischer Programmiersprachen, von Datenbanksystemen und Kommunikationstechnologien.

Aufgaben:

Forensische Ermittlung und Auswertung digitaler Spuren,
Aufklären von Hackerangriffen in Zusammenarbeit mit dem SB,
Beweissicherung bei Computersabotage,
Analyse und Abwehr von Netzwerkangriffen,
Computer-Forensik, bei der es um die Analyse von Computer- oder Mobilgeräten und der darin enthaltenen Daten geht,
Forensische Datenanalyse, bei der es um die gezielte und strukturierte Analyse von (meist großen) Datenbeständen aus Anwendungen und den zugrunde liegenden Datenbanken geht

Der Analyseprozess der IT-Forensik dürfte aus folgenden vier Schritten bestehen:

· Identifizierung
· Datensicherung
· Analyse
· Aufbereitung

Live-Forensik (auch bekannt als Online-Forensik) zur Beweismittelsicherung
Sachverständiger Zeugin/Zeuge vor Gericht (lückenlose Dokumentation der Sicherung und Auswertung)

Die nachfolgenden Aufgaben sind darüber hinaus auch von allen IUK-Ermittlungsunterstützern in allen KPB wahrzunehmen:

- Schulung von Mitarbeitern der KK
- Beratung der Ermittlungsstellen bei der Ausgestaltung von Informationserhebungen

b) Sachbearbeiterin/Sachbearbeiter „Cyberdelikte“

Anforderungsprofil:

Kriminalpolizeiliche Sachbearbeiterin/Sachbearbeiter

Aufgaben:

- Sachbearbeitung von Betrugsdelikten im Internet (hier benötigen wir keinen speziell ausgebildeten Sachbearbeiter für Computer- und Internetkriminalität). Betrugsdelikte im Internet sind in der Regel Delikte des Waren- und Warenkreditbetrugs, die von kriminalpolizeilichen Sachbearbeitern in Betrugskommissariaten bearbeitet werden. Wichtig ist, dass zukünftig auch dezentral in solchen Ermittlungskommissariaten IUK-Ermittlungs-unterstützer eingesetzt werden, die die Sachbearbeiter bei der Auswertung, der zuvor von der zentralen IUK-Ermittlungsunterstützung gesicherten und aufbereiteten Daten verfahrensbezogen unterstützen.

- Delikte der Computerkriminalität im engeren Sinne (z.B. Phishing)

- Aufklären von Hackerangriffen nach Bereitstellung der Daten durch den IT-Ermittlungs-unterstützer. (Hier sollte unterschieden! Was verstehen wir unter Hackerangriffen. Ein Hackerangriff auf einen Privat-PC kommt in der Regel nicht zur Anzeige, es sei denn, der Geschädigte sieht sich erpresserischen Forderungen ausgesetzt. Relevanter sind hier die Angriffe auf kritische Infrastrukturen, wie IT-Systeme von Krankenhäusern, Versorgern etc. Auch hier besteht eine Zuständigkeit des Landeskriminalamts bzw. der Behörden mit Aufgaben nach § 4 KHSt.)

- Durchsuchungen, Sicherstellung und Auswertung von Beweismitteln, die vom IUK-Ermittlungsunterstützer aufbereitet wurden

- Daten und Analyseschritte für die Beweismittelanforderung von Gerichten durch eine lückenlose und umfassende Dokumentation gewährleisten (mit IUK-Ermittlungsunterstützer)