Landtag Mecklenburg-Vorpommern
8. Wahlperiode
**- Ausschuss für Inneres,
Bau und Digitalisierung -**

Ausschussdrucksache 8/61

Schwerin, den 30. März 2022

Schriftliche Stellungnahmen

zum Antrag der Fraktion der FDP
Cyberkriminalität verhindern - Mecklenburg-Vorpommerns kritische Infrastruktur vor Angriffen aus dem Netz schützen
- Drucksache 8/249 -

1. Landeskriminalamt Mecklenburg-Vorpommern
2. Fachhochschule für öffentliche Verwaltung, Polizei und Rechtspflege M-V

Landeskriminalamt
Mecklenburg-Vorpommern
Der Direktor

POLIZEI
Mecklenburg-
Vorpommern

Landeskriminalamt Mecklenburg-Vorpommern, Retgendorfer Straße 9, 19067 Rampe

Landtag Mecklenburg-Vorpommern
Ausschuss für Inneres, Bau und Digitalisierung

nachrichtlich:

Referat II 440

bearbeitet von: Rico Freitag
Jens Pfahl
Telefon: +49 3866 64- 8205
Telefax: +49 3866 64- 8102
E-Mail: rico.freitag@polmv.de

- per elektronischer Post -

Rampe, 28.03.2022

Antrag der Fraktion der FDP-Cyberkriminalität verhindern - Mecklenburg-Vorpommerns kritische Infrastruktur vor Angriffen aus dem Netz schützen

Bezug: Einladung zur Anhörung am 31.03.2022
Hier: Stellungnahme des Landeskriminalamtes Mecklenburg-Vorpommern

Lage

Durch die frei von staatlichen Grenzen mögliche Nutzung des Internets zielen Straftäter und kriminelle Gruppierungen aus der gesamten Welt u.a. auch auf Opfer innerhalb Deutschlands ab. So sind ständig Angriffe wie z.B.

- Betrugsversuche und vollendete Betrugsstraften u.a. aus Westafrika,
- Angriffe mittels Schadsoftware aus Osteuropa und Asien,
- Hackerangriffe aus Südostasien usw.

zu verzeichnen. Durch die Cybercrime-Dienststellen der Landeskriminalämter (LKÄ) der Bundesrepublik werden intensiv neue Methoden der Bearbeitung von Cybercrimedelikten erprobt und genutzt. So werden verstärkt zentrale Ermittlungen für Angriffskomplexe durchgeführt. Dabei erfolgen unabhängig vom Tatort die Ermittlungen zu einem Komplex (z.B. für eine Schadsoftware) in nur einem Landeskriminalamt, ohne dass ein staatsanwaltschaftliches Sammelverfahren erforderlich ist.

Eine derartige zentrale Ermittlung führt z.B. seit November 2021 die Ermittlungsgruppe (EG) „Indigo“ im Landeskriminalamt Mecklenburg-Vorpommern (LKA MV) zur Hackergruppe „DeepBlueMagic“. Diese Gruppe ist unter anderem mutmaßlich für den Angriff auf den kommunalen IT-Dienstleister SIS Schwerin verantwortlich.

Die Aufklärungsquote im Bereich Computerkriminaliät/Cybercrime lag im Jahr 2019 bei 38.2% und insgesamt 605 aufgeklärten Fällen. Die Quote fiel im Jahr 2020 auf 30,7% bei 532 aufgeklärten Fällen. Für das Jahr 2021 ist bei etwa gleichbleibender Gesamtfallzahl ein weiterer geringer Abfall der Aufklärungsquote im Bereich Cybercrime erkennbar.

Zu beachten ist, dass es eine Vielzahl von Auslandstaten gibt, welche auch bei erfolgter Anzeigenerstattung nicht in der Polizeilichen Kriminalstatistik (PKS) berücksichtigt werden. So sind nur Straftaten mit deutschem Tatort PKS-relevant, wenn der Erfüllungsort innerhalb der Bundesrepublik liegt. Die zur Verfügung stehenden Daten spiegeln somit nur den Teil der Kriminalität wieder, der polizeilich bekannt geworden und bei der eine Tathandlung innerhalb Deutschlands gegeben ist.

Erstmals im Jahr 2020 wurden Auslandsstraftaten gesondert statistisch erfasst, flossen aber noch nicht in die PKS ein, da sich diese Daten noch in der Evaluation befinden. Hier zeichnet sich jedoch ein deutlich steigender Trend ab.

Hier wird zusätzlich auf das durch die erste Dunkelfeldstudie in MV belegte Dunkelfeld von 99,2 % im Deliktsbereich Cybercrime (Straftaten gegen Privatpersonen) verwiesen. Somit ist eine valide Darstellung der Kriminalitätsbelastung und so auch der Aufklärungsquote im Phänomenbereich Cybercrime nur bedingt möglich.

<u>Herausragende Fälle von Cyber-Angriffen auf Verwaltung und Wirtschaft in MV in den letzten zwei Jahren (beispielhaft)</u>

- Ransomware-Angriff auf die AIDA Cruises (Tatzeit Dezember 2020)
- Verschlüsselungsangriff auf Rostocker Unternehmen (Tatzeit März 2021)
- DDoS Attacke auf Stadtwerke Rostock (Tatzeit Juni 2021)
- Ransonware-Angriff auf Stadtwerke Wismar (Tatzeit 2021)
- Ransomeware-Angriff auf Wismarer Unternehmen (Tatzeit 2021)
- Angriff auf E-Mail-System einer Stadt in Westmecklenburg (Tatzeit 2021)
- Verschlüsselungsangriff auf kommunale Firma SIS Schwerin (Tatzeit 2021)

Die hier vorangestellte Einführung macht deutlich welche Herausforderungen sich für die Landespolizei Mecklenburg-Vorpommern (Landespolizei MV) bei der Bekämpfung der Cyberkriminalität ergeben. Um diesem Deliktsbereich wirksam begegnen zu können, sind weitreichende technische, personelle und strukturelle Entwicklungen notwendig.

Aufgaben/Aufgabenabgrenzung im Bereich Cybercrime

Zur Strafverfolgung sind die Dienststellen der Landespolizei gemäß der Verwaltungsvorschrift des Ministeriums für Inneres und Sport vom 11. Dezember 2015 - II 440c - II-203-30430-2011/029-033 – mit unterschiedlichen Aufgaben in die Cybercrime-Bekämpfung mit einbezogen.

Die Bearbeitung von Cybercrime erfolgt grundsätzlich entsprechend dem Grunddelikt durch die Kriminalpolizeiinspektionen, die Kriminalkommissariate bzw. durch das Landeskriminalamt.

Darüber hinaus werden vom LKA MV alle eingehenden Hinweise über die seit Juni 2010 bestehende Onlinemeldestelle www.netztverweis.de bearbeitet. Über diese Internetplattform können Hinweise (zumeist anonym) zu Inhalten und Handlungen mit Bezug auf Kinder- und Jugendpornografie, Extremismus und Cybercrime an das LKA MV gemeldet werden.

Von 2010 bis 2021 sind über die Onlinemeldestelle www.netztverweis.de insgesamt über 14.000 Hinweise eingegangen, wovon das Dezernat Cybercrime alleine 5.726 Hinweise zu Kinder- und Jugendpornografie und 5.661 Hinweise zu Cybercrime bzw. Sonstiges zu prüfen hatte, Anzeigen gefertigt hat und weitere Ermittlungen durchführte. Für das Jahr 2022 gab es bereits insgesamt 241 neue Hinweise (160 Kinder- und Jugendpornografie, 40 Cybercrime und 41 Extremismus).

Wichtige polizeiliche Partner der Cybercrime-Dienststelle des LKA MV sind die Abteilung Cybercrime des Bundeskriminalamtes, das Bundesamt für die Sicherheit der Informationstechnik (BSI), das Cyberabwehrzentrum, die Cybercrime-Dienststellen der anderen LKÄ und der Bundespolizei. Zur bundesweiten Koordination und zum Erfahrungsaustausch finden zweimal jährlich die Leitertagung Cybercrime, Sachbearbeitertagungen und andere Veranstaltungen statt.

Rolle und Grenzen der Polizei bei einem IT-Vorfall

Das Feld der IT-Sicherheit betrifft viele verschiedene private und öffentliche Akteure. In erster Linie ist für die IT-Sicherheit in Unternehmen das BSI Ansprechpartner, insbesondere wenn es sich um KRITIS-Unternehmen handelt. Darüber hinaus haben die LKÄ zentrale Ansprechstellen Cybercrime (ZAC) eingerichtet, so auch das LKA MV.

Die Rolle der Polizei bei einem IT-Vorfall ist die Strafverfolgung und Gefahrenabwehr sowie die Prävention/Beratung.

Die Polizei leistet keinen Wiederaufbau der befallenen IT-Infrastruktur und keine Entschlüsselung der befallenen Systeme. Gegebenenfalls liegen der Polizei Erkenntnisse vor, wie Daten entschlüsselt werden können oder es sind Ermittlungserkenntnisse aus anderen Verfahren bekannt, die im Bedarfsfall dem Geschädigten zur Verfügung gestellt werden. Die Polizei berät Unternehmen zu IT-Sicherheitsvorfällen, wie diese zu verhindern sind, wie ihnen im Schadensfall zu begegnen ist bzw. wie einem erneuten Angriff entgegengewirkt werden kann. Allerdings ist hier deutlich anzumerken, dass es keinen 100%igen Schutz vor Cyber-Angriffen gibt. Der Fokus sollte vielmehr auf die wirkungsvolle Abwehr gerichtet werden bzw. darauf auf den Schadensfall vorbereitet und weiter handlungsfähig zu sein.

Zentrale Ansprechstelle Cybercrime (ZAC)

Die ZAC sind miteinander vernetzte, polizeiliche Kontaktstellen des Bundes und der Länder, die speziell für Unternehmen sowie öffentliche und nichtöffentliche Institutionen eingerichtet worden sind und diesen als zentraler Ansprechpartner (SPoC) im Bedarfsfall zur Verfügung stehen. Von dort werden im Falle eines Schadensereignisses die ersten Maßnahmen zur polizeilichen Gefahrenabwehr und zur Strafverfolgung durchgeführt bzw. mit den Flächendienststellen koordiniert. Darüber hinaus informiert sie zum einen über Cyber-Angriffe und Sicherheitsrisiken, zum anderen gibt sie Wirtschaftsunternehmen Verhaltensempfehlungen. Neben der Strafverfolgung und der Beratung der Unternehmen im Schadensfall stellt auch die Präventionsarbeit einen wichtigen Aspekt des Aufgabenportfolios dar. Dafür führt die ZAC MV regelmäßig Informationsveranstaltungen, z.B. im Rahmen der Sicherheitspartnerschaft MV, zu „digitalen Bedrohungen“ durch.

Die ZAC MV ist im Cybercrime-Dezernat des LKA MV eingerichtet.

Im Gegensatz zu größeren LKÄ ist die ZAC MV nicht hauptamtlich besetzt. Derzeit gehören der ZAC MV vier Mitarbeiter des Dezernates an, die alle Aufgabenbereiche des ZAC MV im Nebenamt und im Rahmen einer internen Arbeitsgruppe abdecken. Dieser Bereich ist insofern bislang nicht in ausreichendem Maße personell besetzt. Der deutlich zunehmende Bedarf an Beratungsleistungen und Prävention durch das ZAC MV verlangt nach zusätzlichen hauptamtlichen Stellen, damit diese Tätigkeit sich nicht nachteilig auf den Ermittlungsbereich auswirkt.

CERT MV (Computer Emergency Response Team)

In der vom IT-Planungsrat im März 2013 beschlossenen „Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung“ wird die Zusammenarbeit bei der Abwehr von IT-Angriffen als eine der grundlegenden Säulen des Vorgehens bei der Umsetzung der gemeinsamen IT-Sicherheitsstrategie hervorgehoben. Dies bedingte den Aufbau von Landes-CERTs und deren Zusammenarbeit in einem Verwaltungs-CERT-Verbund.

Das CERT MV ist zuständig für die Planung und Umsetzung von vorbeugenden, reaktiven und nachhaltigen Maßnahmen im Rahmen des Informationssicherheitsmanagements des Landes. Es unterstützt das Informationssicherheitsmanagement u.a. durch die Bereitstellung von Sicherheitsinformationen (*Prävention*), Behandlung von Sicherheitsvorfällen (*Reaktion*) sowie die Sensibilisierung von Beschäftigten (*Nachhaltigkeit*).

Die Zuständigkeit des CERT MV erstreckt sich auf die Landesverwaltung und die Kommunen. Aktuell ist es in der Abteilung 2 des Ministeriums für Inneres, Bau und Digitalisierung angesiedelt.

Zwischen dem LKA MV und dem CERT MV erfolgt ein umfangreicher Informationsaustausch zu IT-Angriffen und bekannt gewordenen Schwachstellen in der IT-Infrastruktur.

KoST KRITIS

Die Ressorts sind im Rahmen ihrer jeweiligen fachlichen Zuständigkeit verantwortlich, geeignete Regeln zu schaffen und Maßnahmen zu ergreifen, um den Schutz der jeweiligen Infrastrukturen und damit die Verfügbarkeit der kritischen Dienstleistungen gewährleisten zu können. Darüber hinaus ist auch jede Behörde selbst als kritische Infrastruktur zu verstehen, deren Funktionsfähigkeit in jedem Fall erhalten werden muss.

Diesem Grundsatz des Ressortprinzips folgend, bedarf es dennoch einer zentralen Koordinierung um Doppelarbeiten in den Ressorts zu vermeiden und Interessen abzustimmen. Die KoSt KRITIS fungiert als Geschäftsstelle der interministerielle Arbeitsgruppe für kritische Infrastrukturen (IMAG KRITIS) und moderiert bei KRITIS Fragestellungen zwischen den Ressorts auf Landesebene. Außerdem dient sie neben der Sicherstellung einer zentralen Anlaufstelle des Landes für den Bund für KRITIS-Fragestellungen auch der Auswertung und Aufbereitung von Empfehlungen des Bundes und wissenschaftlicher Gefahrenanalysen für die betroffenen Ressorts.

Die KoSt KRITIS unterstützt bei Bedarf die Fachressorts bei Kontakten zu den Betreibern und in der Umsetzung von Maßnahmen zum Schutz kritischer Infrastrukturen.

Grundlage der Risikobetrachtung von kritischen Infrastrukturen ist der Allgefahren-Ansatz. Es wird hierbei primär der Ausfall der kritischen Dienstleistung betrachtet und nur sekundär die Ursache wie z.B. einen Cyber-Angriff.

Die KoST KRITIS ist derzeit in der Abteilung 4 des Ministeriums für Inneres, Bau und Digitalisierung angegliedert.

Präventionsarbeit

Neben der Tätigkeit der ZAC erfolgen im Rahmen der vorgelagerten Gefahrenabwehr durch die Landespolizei umfangreiche Maßnahmen zur Prävention von Cybercrime. Zum einen stehen insbesondere bei den Präventionsberatern der Polizeiinspektionen Kinder und Jugendliche mit Fragen der Medienkompetenz im Fokus. Neben dieser jungen Adressatengruppe richten sich Präventionsangebote an ältere Mitmenschen, beispielgebend ist hier der „Silver Surfer“ zu nennen. Ebenso werden insbesondere diese Zielgruppen durch die polizeiliche Prävention des LKA MV angesprochen. Über die Sicherheitspartnerschaft Mecklenburg-Vorpommern werden für die Partner bzw. für die Mitglieder der dort vertretenen Interessensgemeinschaften beispielsweise im Rahmen von Vorträgen Cybercrime-spezifische Inhalte für Klein- und mittelständische Unternehmen (KMU) zur Sensibilisierung angeboten.

Hier erfolgt eine enge Abstimmung mit der ZAC. Im Jahr 2021 nahm die ZAC an zahlreichen Präventionsveranstaltungen mit Unternehmens- und Verbandsvertretungen zum Thema Cybercrime teil. Darüber hinaus erfolgen regelmäßig Publikationen unter anderem in Verbandszeitschriften des Handwerks und der Industrie.

Die Präventionsangebote der Landespolizei MV richten sich an alle von Cybercrime betroffenen oder tendenziell gefährdeten Gruppen. Neben Unternehmen und anderen Institutionen müssen weite Teile der Gesellschaft über die Phänomene der Cybercrime aufgeklärt und für die damit einhergehenden Gefahren sensibilisiert werden. Die Präventionsarbeit erfolgt anlassbezogen und kann notwendige Impulse dafür geben, dass Unternehmen und Institutionen in eigener Verantwortung notwendige IT-Sicherheitsmaßnahmen umsetzen. Eine begleitende, kontinuierliche Prävention für die Zielgruppe der KMU etc., auch durch dezentrale Präventionsberater/-innen, könnte das Angebot hier noch erweitern, bedarf jedoch auch der zusätzlichen Ressourcenbereitstellung.

Personelle Situation in den Ermittlungsdienststellen

Zur Bekämpfung der weiterhin steigenden Anzahl von Cybercrimedelikten, der Abarbeitung der Hinweise der Onlinemeldestelle (www.netzverweis.de), der Gewährleistung der Tätigkeiten der ZAC, zur Bildung von fallbezogenen Ermittlungsgruppen und zur Gewährleistung einer qualifizierten Einsatz- und Ermittlungsunterstützung innerhalb des LKA MV und auch für die Kriminalpolizeiinspektionen, ist ein Personalaufwuchs im Bereich Cybercrime-Dienststellen notwendig. Die Fallzahlen der Cybercrime steigen insgesamt an, die Ermittlungen des Einzelfalls werden komplexer, woraus sich ein erhöhter Ermittlungsbedarf für eben diese Bereiche ergibt. Außerdem gewinnt die Auswertung, Analyse und Aufarbeitung digitaler Daten und Spuren rapide an Bedeutung auch in andersgelagerten Ermittlungsverfahren, wodurch sich zusätzliche Unterstützungsbedarfe für die Cybercrime-Ermittler/-innen ableiten lassen. Deshalb werden wir sowohl personell als auch technisch auf diese Anforderungen reagieren müssen.

Ebenso ist eine personelle Verstärkung im Bereich der digitalen Forensik erforderlich. Bei vielen Straftaten und insbesondere bei fast allen Cyberermittlungen wird erst durch die Auswertung von Datenträgern und der Bereitstellung von Daten der Grundstein für weitere Ermittlungen gelegt. Die Auswertung und Aufbereitung von Datenträgern spielt auch in deliktsübergreifenden Verfahren eine entscheidende Rolle. Das Ziel muss es daher sein, entsprechende Arbeitsbereiche so zu stärken, dass durchweg angemessene Bearbeitungszeiten bestehen und somit negative Auswirkungen auf den Ermittlungserfolg unterbleiben.

Aus- und Fortbildung

Die spezifische Aus- und Fortbildung im Bereich Cybercrime bildet eine entscheidende Grundlage für die zukunftsfähige Cybercrimebekämpfung. Aufgrund der zunehmenden deliktsübergreifenden Bedeutung von Cybercrime und digitalen Spuren ist es notwendig allen Ermittler/-innen der Landespolizei MV eine entsprechende Ausbildung zu ermöglichen. Das Aus- und Fortbildungskonzept Cybercrime muss daher noch intensiver zur Umsetzung gebracht werden, um die Schaffung weitreichender Kompetenzen bei der Cybercrimebekämpfung zu einem Schwerpunkt der Aus- und Fortbildungsmaßnahmen zu machen. Dazu soll die Zusammenarbeit an der Fachhochschule für öffentliche Verwaltung, Polizei und Rechtspflege weiter ausgebaut werden.

Es ist ausdrücklich darauf hinzuweisen, dass die Kosten für die notwendige Spezial-Aus- und Fortbildung in diesem Bereich erheblich sind. Die Fortbildung der Fachkräfte zur Aufrechterhaltung und Erweiterung der Befähigungen muss derzeit überwiegend extern erfolgen.

Für spezielle Wochenlehrgänge sind zu erwartende Kosten von 3.000 bis 6.000 € pro Teilnehmer/-in nicht unüblich. Grundlehrgänge, wie derzeit in Schleswig-Holstein angeboten, werden mit Kosten von 10.000 € pro Teilnehmer/-in kalkuliert. Zukünftig wird es aber unverzichtbar sein, den Cybercrime-Ermittler/-innen des LKA MV und der Flächendienststellen solche Aus- und Fortbildungsangebote zu ermöglichen.

Technische Ausstattung der Cybercrime-Dienststellen

In der Cybercrime-Strategie der Landespolizei wurden die Anforderungen an die technische Ausstattung der Cybercrime-Dienststellen des LKA MV und der Kriminalpolizeiinspektionen entwickelt. Diese Beschreibung wurde seitdem entsprechend der technischen Entwicklung fortgeführt. Eine Fortschreibung muss auch zukünftig regelmäßig erfolgen, um die Ausstattung der Cybercrime-Dienststellen auf dem aktuellen technischen Stand zu halten. Zur Vereinheitlichung der technischen Ausstattung erfolgt eine zentrale Beschaffung.

Ermittlungsdienststellen sehen sich außerdem in allen Deliktsbereichen zunehmend mit der Bearbeitung und Auswertung von Massendaten konfrontiert. Dazu muss eine Massendateninfrastruktur (MDI) für eine effektive vernetzte und behördenübergreifende Bearbeitung entsprechender Daten ausgebaut werden. Andernfalls entstehen Transfer- und Speichergrenzen und weder die Aufbewahrung, noch die Auswertung größerer Datenmengen kann gewährleistet werden.

Die technische Ausstattung in den Ermittlungsdienststellen wurde in jüngster Vergangenheit zwar verbessert, nunmehr gilt es jedoch diese schnellstmöglich zu vervollständigen. Hier ist insbesondere zu beachten, dass die Ausstattung der rasanten Entwicklung technischer und digitaler Standards angepasst wird und flexibel auf notwendige Bedarfe reagiert werden kann. Da gerade bei Delikten der Cybercrime der endgültige technische Bedarf für die Ermittlungen nicht abschließend eingeschätzt werden kann, muss auch kurzfristig auf weitere Beschaffungsbedarfe reagiert werden können. Herausforderung hier ist das Vergaberecht, um in besonderen Lagen auch schnell reagieren zu können.

Die technische Ausstattung der Dienststellen zur Bekämpfung der Cybercrime bestimmt maßgeblich die Möglichkeiten und Grenzen der Ermittlungen. Außerdem wird der Cybercrime als Massenkriminalität zukünftig nur mit einer entsprechenden Massendateninfrastruktur zu begegnen sein. Ebenso müssen ausreichend Speicherkapazitäten auf allen Ebenen der Ermittlungsdienststellen bereitgestellt werden.

Kooperation mit Hochschulen des Landes Mecklenburg-Vorpommern

Das Konzept zur Neueinstellungen von IT-Spezialistinnen und -Spezialen nach § 16 PolLaufbVO MV hat sich in der zurückliegenden Zeit bewährt und sollte fortgesetzt werden. Es wird allerdings immer schwieriger genügend entsprechende Fachkräfte für die Landespolizei MV zu gewinnen, was sich auch in den sinkenden Bewerberzahlen für die ausgeschriebenen Dienstposten in diesem Bereich widerspiegelt. Hier gilt es auch zusätzliche Wege der Personalgewinnung zu beschreiten. Beispielgebend ist das praxisintegrierende duale Studium im Bereich der Informatik. Im Jahr 2019 begannen 18 Studentinnen und Studenten ein duales Studium in der Landespolizei an verschiedenen Hochschulen des Landes. 2022 werden die Ersten dieses Studium abschließen und anschließend in unterschiedlichen Bereichen der Landespolizei ihre berufliche Tätigkeit aufnehmen. Dabei steht einigen der Weg in die Cybercrime-Bekämpfung bzw. die Forensische IT offen.

Darüber hinaus werden auf Grund des anhaltend hohen Bedarfs an speziellen Fachwissen in verschiedenen Bereichen, insbesondere Cybercrime, Forensik und Wirtschaftskriminalität, sogenannte Quereinsteiger mit abgeschlossenen Hochschulstudium benötigt. Es finden bereits heute zielführende Kooperationen mit den Hochschulen statt. Sowohl das LKA MV als auch die Hochschulen sehen zusätzliche Möglichkeiten für eine weiterführende und intensivere Zusammenarbeit. Die Gewinnung von extern ausgebildeten Fachpersonal kann jedoch nur gelingen, wenn die Landespolizei MV in der Lage ist attraktive Arbeitsverhältnisse anzubieten, die mit Wettbewerbern der Wirtschaft konkurrieren können.

Entwicklung der Bekämpfungsstrategie

Auf Initiative des LKA MV erarbeitete eine Projektgruppe im Jahr 2011 die erste Cybercrime-Bekämpfungsstrategie für Mecklenburg-Vorpommern. Aus dieser Strategie resultierte eine erste Verwaltungsvorschrift des Innenministerium zur Bekämpfung der Cybercrime. Diese führte zur Einrichtung des Dezernates 45 „Cybercrime“ in der Abteilung 4 „Schwere Kriminalität“ im LKA MV sowie die Aufgabenzuweisung für die Delikte der Cybercrime im engeren Sinne an die übrigen Ermittlungsdienststellen des Landes. Von den vorgeschlagenen Maßnahmen zur Gewinnung von Fachpersonal wurde die Einstellung von IT-Spezialisten als Polizeibeamte (§16 PolLaufbVO MV) umgesetzt. Nach erfolgten Auswahlverfahren konnten zum 01.02.2012 die ersten drei Mitarbeiter mit einem abgeschlossene IT-Studium als Polizeikommissar bzw. Polizeioberkommissar für das Dezernat 45 sowie einer für das Dezernat 55 (Forensische IT) eingestellt werden.

Im Rahmen der Umsetzung des auf Grundlage der Evaluation der Polizeistrukturreform 2010 erarbeiteten Maßnahmenplanes wurden im November 2014 Vorschläge für eine neue Cybercrime-Bekämpfungsstrategie der Landespolizei MV durch eine behördenübergreifende Projektgruppe unter Federführung des LKA MV entwickelt und dem Innenministerium Mecklenburg-Vorpommern (IM MV) zur Entscheidung vorgelegt. In der Strategie wurden die Aufgabenfelder und Rahmenbedingungen für eine erfolgreiche Cybercrime-Bekämpfung seitens der Landespolizei MV betrachtet und eine Vielzahl von Maßnahmen zur quantitativen sowie qualitativen Verbesserung insbesondere auf den Gebieten Zuständigkeiten, Personal, Beschaffung und technische Ausstattung sowie Aus- und Fortbildung angeregt. Seitens des IM MV erfolgte im September 2015 Zustimmung. Die Realisierung der vorgeschlagenen Maßnahmen sollte ohne explizite Zuweisung von Haushaltsmitteln auf Ebene der beteiligten Behörden und Dienststellen erfolgen. Im Ergebnis wurde durch das IM MV im Dezember 2015 eine neue Verwaltungsvorschrift zur Bekämpfung der Cybercrime erlassen. Hervorzuheben sind dabei die für die Kriminalpolizeiinspektionen sowie das LKA MV nach § 16 PolLaufbVO MV erfolgten Neueinstellungen von weiteren IT-Spezialisten als Cybercrime-Ermittler. Ebenso konnten auf dieser Grundlage für das LKA MV Fachkräfte für die forensische Informations- und Kommunikationstechnik (IuK) sowie die Telekommunikationsüberwachung gewonnen werden.

Im Jahr 2020 erfolgte eine Evaluation der Cybercrime-Strategie. Darin wurden weitere Maßnahmen benannt, um eine zuverlässige Bekämpfung von Cybercrime gewährleisten zu können. Dazu zählen u. a.

- die Verbesserung der spezifischen Aus- und Fortbildung,
- die weitere Gewinnung und Einstellung von Spezialistinnen und Spezialisten,
- die personelle und technische Stärkung im Bereich Digitale Forensik,
- und die Weiterentwicklung der technischen Ausstattung der mit Cybercrime befassten Dienststellen sowie die Schaffung der notwendigen IT-Infrastruktur (auch für Massendaten und „Schmutzdaten“).

gez. Rogan Liebmann

Fachhochschule für öffentliche Verwaltung, Polizei und Rechtspflege
des Landes Mecklenburg-Vorpommern
Goldberger Straße 12-13, 18273 Güstrow

Fachhochschule für
öffentliche Verwaltung,
Polizei und Rechtspflege
des Landes
Mecklenburg-Vorpommern

Fachbereich Polizei

FHöVPR MV

Fachbereich Polizei

bearbeitet von	☎	E-Mail	Az	Ort, Datum
Peter Balschmiter	300	p.balschmiter@fh-guestrow.de		Güstrow, 23.03.2022

Sehr geehrte Damen und Herren,

zu den von Ihnen aufgeworfenen Forderungen kann ich aus der Sicht der FHöVPR M-V und des Fachbereiches Polizei nur zu den Aussagen 1 und 2 Stellung beziehen, die weiteren Punkte liegen thematisch außerhalb des Zuständigkeitsbereiches und damit auch der hier vorhandenen fachlichen Expertise.

Zu 1.
„mehr gut ausgebildetes Personal für den Bereich IT-Sicherheit und Infrastruktur bereitzustellen.“

Dafür gilt es, in Ausbildung, Studium und besonders auch der Fortbildung den Mitarbeiter*innen der Landespolizei die erforderlichen Kompetenzen zu vermitteln, mit denen Cybercrime erfolgreich bekämpft werden kann.
Für die Vermittlung dieser Kompetenzen gibt es ein auf Bundesebene abgestimmtes Bildungskonzept (Anlage: Konzeption Aus- und Fortbildung Cybercrime der Landespolizei M-V). Diese Konzeption wurde bisher in der Ausbildung Studium mit den folgenden Inhalten umgesetzt:
Ausbildung:

- Internetkriminalität - Phänomenologie
- Betrugsdelikte im Internet
- Sicherstellung von elektronischen Beweismitteln,

Studium:

- Phänomenologie und Ätiologie von Internetkriminalität
- Kriminalistische Bearbeitung und Prävention Internetkriminalität (u.a. Computerbetrug, Phishing, Handel mit Zugangsdaten, Fake-Shops, Datenveränderung, Computersabotage, Kinderpornografie im Internet,
- Eingriffsrecht bei Ermittlungen im Internet
- Strafrecht Themenfeld Cybercrime
- Grundsätze des Ersten Angriffs
- Durchsuchungen von Räumen zum Auffinden von elektronischen Beweismitteln, Sicherung elektronsicher Beweismittel
- Informationsgewinnung aus öffentlichen Datenspeichern (Internet)
- Polizeiliche Ermittlungen in Sozialen Netzwerken
- Fragestellungen und Auswertemöglichkeiten elektronischer Datenspeicher
- IT-Forensik, Möglichkeiten der technischen Auswertung von elektronischen Datenträgern
- Fälschung beweiserheblicher Daten.

In der Fortbildung gab es bisher folgende Angebote:

- Ersteinschreiter/in Cybercrime
- Internetermittlungen
- Cellebritereader (Auswertung Smartphones)
- Cybercrime spezial (Toolbox des BKA).
-

Mit diesen Angeboten wurden bereits wichtige fachliche Kompetenzen vermittelt.

Im Rahmen einer Evaluation der Cybercrimebekämpfungsstrategie der Landespolizei M-V (Anlage) aus dem Jahr 2020 wurde allerdings festgestellt, dass das Aus- und Fortbildungskonzept nicht im erforderlichen Maß umgesetzt wird. „Die geringe Zahl an Mitarbeitern der Landespolizei MV, welche in den vergangenen Jahren einen Lehrgang zur Erlangung essentieller Fähigkeiten für Ermittlungen im digitalen Raum absolviert haben, zeigt, dass die Angebote der FHöVPR in diesem Bereich … nur unzureichend ... bereitgestellt werden“ (Evaluation, S. 13).
Die Angebote des Fachbereiches Polizei sollten in Hinsicht auf Quantität aber auch mit Blick auf die inhaltliche Ausgestaltung verbessert werden.
Als Forderung formuliert der Bericht zur Evaluation, dass die materiellen und personellen Ressourcen aufzustocken wären.

Insbesondere vor dem Hintergrund aktueller Herausforderungen, wie den erfolgten IT-Angriffen auf Verwaltungen des Landes und der Kreise sind weitere Anstrengungen auch im Bereich der Aus- und Fortbildung erforderlich.
Unterstrichen wird diese Tatsache auch mit der „Brüsseler Erklärung der IMK 2022“, in der die Innenminister der deutschen Bundesländer auf die aktuellen Herausforderungen verweisen. Danach hat die digitale Kriminalität einen besonders hohen Stellenwert für die öffentliche Sicherheit. Die Cybersicherheit von Staat, Wirtschaft, Wissenschaft und Gesellschaft ist weiter zu stärken. Unter

anderem sind im Deliktsbereich der sexuellen Gewalt gegen Kinder die Ermittlungsprozesse zielführender auszugestalten und Ermittlungen zur Aufdeckung und Verfolgung von Straftaten, die unter Nutzung kryptierter Kommunikation erfolgen, sind zu fördern.

Um diesen neuen und zusätzlichen Aufgaben im Bildungsbereich gerecht werden zu können bedarf es:

1. Sachliche Ausstattung am Fachbereich Polizei
   Dazu ist festzustellen, dass die gegenwärtig vorhandenen PC Kabinette nicht ausreichend sind. Es fehlt ein PC Labor zur Durchführung spezieller Fortbildungen und von Aufbaukursen, indem die Möglichkeit besteht, unabhängig von Netz der Landespolizei bzw. dem Hochschulnetz zu arbeiten. Im Rahmen der geplanten Baumaßnahmen an der FHöVPR M-V soll dieses PC Labor planmäßig bis zum 01.01.2024 (Gebäude 9) errichtet werden.
   Nach Realisierung der Baumaßnahme dürften die entsprechenden sachlichen Voraussetzungen gegeben sein.
2. Zur qualitativen Verbesserung der Fortbildung hat der Fachbereich ein Konzept „Cybercrime, digitale Spuren und digitale Ermittlungen“ (Anlage) entwickelt.
3. Für den Bereich der externen Fortbildung reichen die Ansätze im Titel 0406.525.08 regelmäßig nicht aus, so dass jährlich angemeldete Fortbildungen gestrichen werden müssen. Hier wäre eine angemessene Erhöhung des Titels notwendig.
4. Eine angemessene personelle Ausstattung im Bereich der Lehrenden. Die gegenwärtige Personalressource reicht nicht aus, um alle erforderlichen Bildungsmaßnahmen durchführen zu können. Da auch in den anderen Bildungsbereichen (z.B. Recht, Kriminalistik usw. keine volle Personaldeckung gegeben ist, kann keine Personalumsteuerung erfolgen).
   Um den Ansprüchen der vorliegenden Konzepte im vollen Umfang gerecht werden zu können, sind zwei zusätzliche feste Stellen (einmal PVB, einmal Verwaltung (abgeschlossenen IT Studiengang)) erforderlich.

2. gemeinsam mit den Hochschulen des Landes ein Konzept zu entwickeln, die Weiterentwicklung der IT-Studiengänge voranzutreiben sowie entsprechende Stipendienprogramme aufzulegen.

Zu diesem Thema hat die FHöVPR M-V im Frühjahr 2021 ein Konzept „Zukunftsfähigkeit der Verwaltung – Digitalisierungskompetenzen in Studium und Ausbildung fördern“ entwickelt und vorgelegt.
Vorgesehen sind laut Konzept entsprechende Module zur Digitalisierung der Verwaltung und Vermittlung von Kenntnissen zu elektronischen Aktenmanagementsystemen, zum Datenschutzrecht und zum Informations-sicherheitsrecht in die Ausbildung zu integrieren; des Weiteren soll die Entwicklung von analytischen Fähigkeiten zur Digitalisierung von Verwaltungsvorgängen und zur Optimierung von Geschäftsprozessen vermittelt werden. Im Bereich Fortbildung sind ergänzende fachbereichsübergreifende Qualifizierungsprogramme zur digitalen Kompetenzentwicklung und

Durchführung von Ringvorlesungen geplant. Darüber hinaus bestehen Überlegungen einen Studiengang „Verwaltungsinformatik“ in Kooperation mit anderen Hochschulen zu etablieren und/oder ein Vertiefungsstudium „Verwaltungsinformatik im Fachbereich allgemeine Verwaltung anzubieten.
Das Konzept wird nach Auswertung der Ressortanhörung demnächst dem Kabinett zur Beschlussfassung übersandt.

Zur Umsetzung dieses Konzeptes ist die Einrichtung eines Institutes für Digitalisierung vorgesehen. Für das Institut sind vier bis befristete Stellen (1x A 15, 2x A13, 1xA11) im Haushaltsplan vorgesehen. Da es sich hier um eine künftig dauerhafte Aufgabe handeln wird, ist die Entfristung dieser Stellen erforderlich. Nur so können die im Konzept vorgesehenen Varianten verstetigt werden.

Peter Balschmiter
Leiter Fachbereich Polizei