19. Wahlperiode

Drucksache **19/3984**

HESSISCHER LANDTAG

10.11.2016

HHA

Änderungsantrag
der Fraktionen der CDU und BÜNDNIS 90/DIE GRÜNEN
zu dem Gesetzentwurf der Landesregierung für ein Gesetz über die Feststellung des Haushaltsplans des Landes Hessen für das Haushaltsjahr 2017 (Haushaltsgesetz 2017)

Drucksache 19/3674

Inhalt des Antrags: **Einrichtung eines Cyber-Kompetenzteams**

Einzelplan **03 Hessisches Ministerium des Innern und für Sport**

Der Landtag wolle beschließen:

Zu Kapitel 03 01 Ministerium
Buchungskreis: 2200

Produktnummer lt. Leistungsplan 7

Bezeichnung lt. Leistungsplan Gefahrenabwehr

Leistungsplan:

	von	Veränderung um	auf
		Beträge in 1.000 EUR	
Gesamtkosten	34.652,6	+400,0	35.052,6
Eigene Erlöse	4.235,5	0,0	4.235,5
Produktabgeltung	30.417,1	+400,0	30.817,1

Weitere Änderungen im Wirtschafts-/ Stellenplan:

Wirtschaftsplan:
Die Veränderungen in dem o.g. Leistungsplan bedingen auch entsprechende Anpassungen von Produktblättern, Erfolgsplan und Überleitungsrechnung.

Stellenplan:
Es sollen 8 Stellen neu ausgebracht werden:
1x A16, 2x A15, 3x A14, 2x A13 g.D.
Die im Stellenplan ausgewiesenen Planstellen sind entsprechend anzupassen.

Kameraler Haushaltsabschluss: **Beträge in EUR**

Hauptgruppe	**von**	**um**	**auf**
HG 4	37.785.100	+400.000	38.185.100
Kameraler Zuschuss/Überschuss	-151.307.000	-400.000	-151.707.000

Der Wirtschaftsplan und der kamerale Haushalt sind entsprechend anzupassen.

Eingegangen am 10. November 2016 · Ausgegeben am 10. November 2016
Herstellung: Kanzlei des Hessischen Landtags · Postfach 3240 · 65022 Wiesbaden · www.Hessischer-Landtag.de

Begründung des Änderungsantrags:

Fortschreibung des Hessischen Aktionsplans zur Integration von Flüchtlingen und Bewahrung des gesellschaftlichen Zusammenhalts.

Weltweit findet eine digitale Revolution statt, die alle Lebensbereiche erfasst hat. Bürgerinnen und Bürger sowie Unternehmen nutzen die Möglichkeiten des Cyberraums und erwarten, dass auch hier Recht und Gesetz, Verlässlichkeit und Sicherheit gewährleistet sind. Die enorm hohe Geschwindigkeit bei der Weiterentwicklung digitaler Technologien und die damit einhergehenden verändernden Tatbegehungsweisen der Kriminellen erfordern innovative Sicherheitsbehörden. Der Cyberraum ist Tatort, Tatmittel und bietet Tatgelegenheiten in der gesamten Bandbreite der Kriminalität von Kinderpornographie und Cybergrooming über Datenausspähung und -erlangung bis hin zu Waffen- und Rauschgifthandel oder Angriffen auf kritische Infrastrukturen. Das Ausmaß der technischen Weiterentwicklung lässt mehr und neue Tatgelegenheitsstrukturen entstehen, was zu einer weiteren Steigerung des Bedrohungs- und Gefährdungspotentials führt.

Die Ereignisse von Würzburg und Ansbach zeigen deutlich auf, dass auch terroristische Gruppierungen wie der sog. Islamische Staat den Cyberraum längst durchdrungen haben und für ihre Zwecke einsetzen. In beiden Fällen liegen Erkenntnisse vor, dass die Täter direkte Kontakte über soziale Medien zu Personen unterhielten, die dem Islamischen Staat zuzurechnen sind. Nach Angaben des Bundesamtes für Verfassungsschutz wird davon ausgegangen, dass von Seiten der Islamisten Internet und soziale Medien zunehmend als „Werkzeug hybrider Kriegsführung“ im Sinne von irregulären und asymmetrischen Mitteln wie Desinformationskampagnen und Cyberattacken in Ergänzung zum offenen Agieren durch Anschläge eingesetzt werden.

Cyberattacken, Ausspähversuche anderer Staaten, Wirtschaftsspionagehandlungen, aber auch Aktionen vor dem Hintergrund von Partikularinteressen einzelner (Privat-) Personen als Tathintergrund nehmen beständig zu.

Rechte Hasspropaganda ist ein weiteres, wichtiges Feld für die Bekämpfung der Cyberkriminalität. Fremdenfeindliche Kommentare, die unwidersprochen und somit mit umso zersetzenderer Wirkung im gesellschaftlichen Diskurs Einzug halten, gegenseitiges Anstacheln und Radikalisieren unter Nutzung netzspezifischer Verstärkungseffekte und Zugriffe auf weltweit verfügbare Inhalte der sozialen Medien, Verschlüsselungs- und Anonymisierungsmöglichkeiten über TOR-Netzwerke sowie das Darknet zum Waffen-, Rauschgift- und Datenhandel sind Stichworte, die die Bandbreite der Aufgaben der Sicherheitsbehörden skizzieren.

Europol hat in der am 27. September dieses Jahres veröffentlichten Studie "Internet Organized Crime Threat Assessment" festgestellt, dass Cyber-Crime unaufhaltsam zunimmt und in einigen europäischen Ländern die Zahl der Cyber-Crime-Anzeigen diejenigen aus traditionellen Deliktbereichen bereits übersteigt. Europol zeigt sich äußerst besorgt, dass die wachsende "cybercriminal community" in immer stärkerem Maß unsere Abhängigkeit von Internet und Technologie ausnutzt. Europol betont in diesem Zusammenhang, dass Strafverfolgungsbehörden die notwendigen Fähigkeiten und technischen Möglichkeiten ausbauen müssen, um auch im Cyberraum wirksam Informationen erheben zu können.

Daher ist die Bekämpfung der Cyberkriminalität ein hoch priorisiertes Ziel der hessischen Sicherheitsbehörden und leitet sich direkt aus der aktuellen Koalitionsvereinbarung ab. Darüber hinaus ist dem veränderten Informationsbedürfnis der Bürgerinnen und Bürger in diesem Kriminalitätsbereich Rechnung zu tragen und ein umfassendes Beratungsangebot im Hinblick auf präventive Maßnahmen erforderlich.

Viele richtige Schritte sind in der Vergangenheit bereits getan worden, um diesen Herausforderungen zu begegnen.

- So wurden in den hessischen Polizeipräsidien flächendeckend Internet-Fachkommissariate eingerichtet und die zentralen Komponenten im HLKA gestärkt. In der neu eingerichteten Abteilung 3 im Hessischen Landeskriminalamt (HLKA) – „Cybercrime und IuK-Einsatzunterstützung“ – wird erfolgreich Internet-Kompetenz gebündelt. Dies betrifft sowohl die Ermittlungen, die Einsatz- und Ermittlungsunterstützung (forensische Datenträgerauswertung, Telekommunikationsüberwachung, Netzwerkforensik), aber auch die übergreifende Analyse des Kriminalitätsgeschehens im Bereich Cyberkriminalität.

- Die im Jahr 2015 in der Abteilung 3 des HLKA eingerichtete „Zentrale Ansprechstelle Cyberkriminalität“ (ZAC) stellt für Externe und alle Polizeibehörden eine schnelle und kompetente Bewertung, Beratung und Koordinierung in Fällen von Cyberkriminalität ggf. in enger Abstimmung mit der Zentralstelle zur Bekämpfung der Internetkriminalität bei der Generalstaatsanwaltschaft Frankfurt am Main (ZIT) sicher. Die ZIT wurde ebenfalls sukzessive personell ausgebaut und setzt bundesweit Maßstäbe.

- Den aus dem IT-Sicherheitsgesetz hervorgehenden Erfüllungsaufwänden ist die Landesregierung mit personellen Verstärkungen begegnet. Für die Polizei konnten im Haushalt 2016 eine Stelle im

Landespolizeipräsidium und fünf Stellen im Polizeivollzug – zunächst zentral im HLKA – zur Verfügung gestellt werden. Für den Haushalt 2017 sind bereits 20 weitere Stellen im Polizeivollzug vorgesehen, die den Flächenpräsidien zugewiesen werden sollen.

- Internationale Ermittlungen, so auch im Darknet, mündeten in erfolgreichen Ermittlungsverfahren u. a. wegen Rauschgifthandels. Zudem konnte in einer weltweiten Operation unter Federführung des US-amerikanischen FBI, unter Mitwirkung des HLKA, in enger Abstimmung mit dem Cybercrime-Centre von EUROPOL (EC 3) ein bedeutsamer Teil des illegalen Online-Marktplatzes im Darknet stillgelegt werden („Take-down“).

- Im Kontext des IT-Sicherheitsgesetzes und des Schutzes der kritischen Infrastrukturen wurde auch die Koordinierungsstelle KRITIS (KoSt-KRITIS) im Bereich Brand- und Katastrophenschutz im Jahr 2015 um eine Stelle verstärkt.

- Seit einiger Zeit wird im LfV ein Konzept zur Abwehr von elektronischen Angriffen mit nachrichtendienstlichem Hintergrund, sog. Cyberangriffen, umgesetzt.

- Das LfV hat zum Aufbau des Arbeitsbereiches „Digitaler Wirtschaftsschutz“ zwei Stellen g.D. eingerichtet.

- Das LfV führte zahlreiche Sensibilisierungsmaßnahmen (Vorträge, Einzelgespräche in Firmen, IHK’en und anderen Verbänden und Arbeitskreisen) zum Thema Aufbau und Struktur sowie Methodik von Cyberangriffen durch.

- Eine deutliche Zunahme von Verdachtsmeldungen betreffend Cyberspionage ist festzustellen. Die in der Bearbeitung der Verdachtsfälle gewonnenen Erkenntnisse fließen nicht nur in weitere Beratungs- und Vortragstätigkeiten des LfV ein, sondern werden an andere vom LfV betreute Unternehmen zum Schutz der eigenen IT weitergegeben. Daraufhin wurden bereits einzelne Systeme vom Netz genommen und ausgetauscht, oder weitere Untersuchungen durch private IT-Sicherheitsdienstleister vorgenommen.

- Direkt erreichen die Informationen des LfV Hessen mittlerweile über 100 Unternehmen und Einrichtungen in Hessen, über Multiplikatoren (Verbände und IT-Dienstleister) können insgesamt weit über 300 Unternehmen über aktuelle Gefahren informiert werden.

Insbesondere vor dem Hintergrund asymmetrischer Cyber-Angriffe sind die bisher ergriffenen Schritte zur Bekämpfung der Cybercrime, zum digitalen Wirtschaftsschutz richtig, bedürfen aber der koordinierten Weiterentwicklung.

Perspektivisch drängen sich neben der Bündelung von Expertisen auch Zentralisierungen von Infrastrukturen auf, um den umfangreichen und sich schnell entwickelnden Herausforderungen des Internets und weiterer Dienste erfolgreich begegnen zu können. Um einen effizienten Ressourceneinsatz und größtmögliche Wirkung entfalten zu können, sind ausdrücklich Kooperationen mit weiteren Sicherheitsbehörden des Bundes und der Länder zu prüfen.

Um den zukunftsorientierten Auf- und Ausbau der Cyberkompetenz der Sicherheitsbehörden in Hessen zu forcieren, soll im Landespolizeipräsidium ein „Cyber-Kompetenzteam“ eingerichtet werden.

Dieses soll zum einen die Planung und Weiterentwicklung der hessischen Sicherheitsarchitektur in Sachen Bekämpfung der Cybercrime vorantreiben und sicherstellen, dass diese Entwicklungen im Einklang mit den Überlegungen anderer Bundesländer und dem Bund stehen. Dazu bedarf es intensiven Austauschs und Abstimmung im Rahmen der bundesweiten Strukturen. Zum anderen müssen die sicherheitsbehördlichen Bedarfe gebündelt, analysiert und ggf. priorisiert betrachtet werden, um einen Vorschlag zur innovativen Ergänzung und zukunftsoffenen Fortschreibung der bereits bestehenden Bausteine auch unter Berücksichtigung von Forschungsergebnissen und Marktentwicklungen zu erstellen.

Um diesen Aufgabenbereich in der Polizeiabteilung des HMdIS etablieren und abbilden zu können, werden acht Planstellen zugewiesen. Die Leitung dieses „Cyber-Kompetenzteams“ soll wegen des Schwerpunkts Bekämpfung der Cyberkriminalität der Polizei obliegen.

Zu ergänzen ist Expertise aus dem nachrichtendienstlichen Aufgabenbereich, der Bekämpfung von Cybercrime und/oder dem polizeilichen Staatsschutz, Informationstechnik/Big-Data Analyse sowie den Sozial- und Rechtswissenschaften.

Die Wertigkeit der Stellen soll im h.D. in der Spitze A15/16, nachfolgend A 14 bzw. entsprechende Entgeltgruppe sowie A 12/13 im g.D. bzw. entsprechende Entgeltgruppe angesiedelt sein.

Wiesbaden,

Für die Fraktion der CDU
Der Fraktionsvorsitzende

Michael Boddenberg

Für die Fraktion BÜNDNIS 90/DIE GRÜNEN
Der Fraktionsvorsitzende

Mathias Wagner (Taunus)