MINISTERIUM FÜR INNERES, DIGITALISIERUNG UND MIGRATION
B A D E N - W Ü R T T E M B E R G

Postfach 10 34 65 • 70029 Stuttgart
E-Mail: poststelle@im.bwl.de
FAX: 0711/231-5000

An die
Präsidentin des Landtags
von Baden-Württemberg
Frau Muhterem Aras MdL
Haus des Landtags
Konrad-Adenauer-Str. 3
70173 Stuttgart

Datum 23.10.2017

[redacted]

Aktenzeichen SD-0141.5/1/103
-
(Bitte bei Antwort angeben)

nachrichtlich
Staatsministerium
Ministerium für Finanzen
Ministerium der Justiz und für Europa
Ministerium für Wirtschaft, Arbeit und Wohnungsbau

Antrag der Abgeordneten Nico Weinmann u. a. FDP/DVP
- Die sogenannte Cyberwehr in der Sicherheitsarchitektur des Landes
- Drucksache 16/2737
Ihr Schreiben vom 2. Oktober 2016, Az.: I/2.3

Sehr geehrte Frau Landtagspräsidentin,

das Ministerium für Inneres, Digitalisierung und Migration nimmt im Einvernehmen mit dem Ministerium für Finanzen, dem Ministerium für Wirtschaft, Arbeit und Wohnungsbau und dem Ministerium der Justiz und für Europa zu dem Antrag wie folgt Stellung:

Vorbemerkung

Um die im Kontext der Cyberwehr Baden-Württemberg geplanten Aktivitäten umfassend bewerten zu können, bedarf es zunächst der Darstellung der aktuellen Gefahrensituation mit folgenden Problemfeldern:

- die Anzahl der gezielten Angriffe auf ausgewählte Unternehmen nimmt zu,
- Spezialisten für IT-Sicherheit fehlen teilweise und es existiert kein standardisierter Umgang mit Sicherheitsvorfällen,
- insbesondere kleine und mittlere Unternehmen sowie Handwerksbetriebe haben einen erhöhten Beratungs-, Schulungs- und Unterstützungsbedarf,
- es fehlt ein umfassendes Lagebild in Baden-Württemberg, da keine verbindlichen Meldestrukturen bei Sicherheitsvorfällen existieren (außer bei Betreibern von so genannten Kritischen Infrastrukturen wie Energie, Telekommunikation, Gesundheit, Ernährung etc.).

Im Einzelnen:

Unternehmen sind in zunehmendem Maße Angriffen aus dem Internet ausgesetzt. Waren diese Angriffe bis vor einigen Jahren meist ungezielte Massenattacken, nimmt die Zahl der gezielten Angriffe auf ausgewählte Unternehmen oder Behörden inzwischen Jahr für Jahr zu. Vor allem in Baden-Württemberg geraten viele Unternehmen als heimliche („Hidden Champions“) oder bekannte Weltmarktführer in den Fokus solcher Angriffe. Insbesondere zielgerichtete Angriffe auf mehrere Unternehmen können dabei einen erheblichen Schaden für den baden-württembergischen Wirtschaftsstandort verursachen. Der Branchenverband Bitkom e.V. schätzt aktuell den durch Spionage, Sabotage und Datendiebstahl entstehenden Schaden für die Deutsche Wirtschaft auf 55 Milliarden Euro pro Jahr.

Zielgerichtete Angriffe sind aus mehreren Gründen besonders gefährlich: Sie sind viel schwieriger zu entdecken, weil sie keine identischen Muster aufweisen, die bei Massenattacken sofort auffallen. Sie sind professionell vorbereitet, werden von „professionellen“ Hackern mit tiefgehenden fachspezifischen Kompetenzen durchgeführt und nutzen z. T. unveröffentlichte Schwachstellen ausgewählter, in der Ziel-Organisation eingesetzter IT-Systeme. Hinzu kommen IT-Angriffe in Form von staatlich gelenkter oder nachrichtendienstlich gesteuerter Spionage und Sabotage. Eine Attribution der „Hacker“ zu z. B. fremden Staaten und deren Nachrichtendienste, organisierter Kriminalität oder Wettbewerbs-

spionage – mit durchaus unterschiedlichen Vorgehensweisen, Mitteln und Methoden – ist oftmals schwierig. So verwenden Nachrichtendienste mittlerweile Software aus dem kriminellen Untergrund zur Nachrichtenbeschaffung und für elektronische Angriffe.

Das Fehlen von IT-Sicherheitsspezialisten verschärft häufig die Lage. Es gibt in Deutschland derzeit nur wenige Unternehmen, die die Kompetenz und Erfahrung besitzen, auf einen Sicherheitsvorfall schnell und angemessen zu reagieren mit dem Ziel, den laufenden Betrieb wiederaufzunehmen, bspw. verschlüsselte Kundendaten wiederherzustellen und Beweise für die Ermittlungsarbeit zu sichern. Für die betroffenen Unternehmen ist es daher schwierig, in einer Notsituation zügig Kontakt zu ausreichend qualifizierten Anbietern aufzunehmen. Zudem haben viele Anbieter nur wenig qualifiziertes Personal, das sie kurzfristig für einen Notfalleinsatz bereitstellen können.

Der Landtag wolle beschließen,
die Landesregierung zu ersuchen
zu berichten

1.
welche Stellung die Cyberwehr in der Sicherheitsarchitektur des Landes einnehmen wird;

Zu 1.:

In Kooperation mit dem Digitalen Innovationszentrum (DIZ), dem CyberForum e.V. und dem FZI Forschungszentrum Informatik soll ab kommendem Jahr in der Region Karlsruhe das Pilotprojekt „Cyberwehr“ umgesetzt werden. Die Cyberwehr soll insbesondere kleine und mittlere Unternehmen und Handwerksbetriebe in IT-Notfallsituationen in einem 7x24h-Dienst beraten, zur Notfallbewältigung zertifizierte Personen vermitteln, Sensibilisierungsmaßnahmen anbieten und strategische Lagebilder erstellen (siehe Ziffer 2).

<u>Bestehende Sicherheitsarchitektur in Baden-Württemberg</u>

Informationssicherheitsorganisation der Landesverwaltung und CERT BWL

Die Landesverwaltung hat mit der zum 1. Mai 2017 in Kraft getretenen Verwaltungsvorschrift zur Informationssicherheit eine strategische Neuausrichtung im Bereich der

Informationssicherheit auf den Weg gebracht. Ressortübergreifend wurden Informationssicherheitsbeauftragte eingesetzt, um als strategisches Steuerungsinstrument ein sogenanntes „Informationssicherheitsmanagementsystem“ (ISMS) nach den Standards des Bundesamtes für Sicherheit in der Informationstechnik (BSI) in enger Kooperation mit den für die operative Informationssicherheit zuständigen Rechenzentren der Landesverwaltung einzuführen. Hierfür wurden vom Landtag im Staatshaushaltsplan 2017 30 Personalstellen genehmigt.

Als eine von vielen organisatorischen Maßnahmen steht zeitnah die Neukonzipierung des CERT BWL (Computer Emergency Response Team) an. Hierbei gilt es unter anderem, innerhalb der Landesverwaltung verbindliche Meldewege für Sicherheitsvorfälle einzuführen und reaktive Maßnahmen für Sicherheitsvorfälle in die Wege zu leiten. Außerdem müssen Meldewege zu Einrichtungen des Bundes und der Länder (Verwaltungs-CERT-Verbund VCV) geschaffen und ausgestaltet werden. Darüber hinaus soll das CERT BWL auch eine enge Vernetzung zu anderen Informationssicherheits-organisationen in Baden-Württemberg anbieten und gewährleisten. Neben weiteren Einrichtungen des Landes (z.B. Polizei, LKA/ZAC) sollen weitere wichtige Organisationen Dritter und mittelfristig auch die Kommunen Baden-Württembergs in diese Vernetzung mit einbezogen werden.

Das CERT BWL bildet die Schnittstelle der Sicherheitsorganisation der Landesverwaltung zur künftigen Cyberwehr aus. Durch die gemeinsame Erfassung aktueller Lagen und durch gegenseitigen Austausch bei aktuellen Cyberbedrohungen profitieren alle Partner gleichermaßen. Mit dem gewählten Vorgehen und den in der Umsetzung befindlichen Maßnahmen werden die Beschlüsse des IT-Planungsrates, gesetzliche Verpflichtungen sowie Vorgaben der Europäischen Union umgesetzt.

Polizei

Die baden-württembergische Polizei hat schon früh einen strategischen Fokus auf die Bekämpfung der Gefahren im Netz gelegt. Bereits 2012 wurde beim Landeskriminalamt Baden-Württemberg eine eigene Abteilung Cybercrime und Digitale Spuren ins Leben gerufen – heute arbeiten dort rund 130 Spezialisten in interdisziplinären Teams für die Sicherheit im Netz. In der Folge wurde auf Grundlage eines Beschlusses der Innenministerkonferenz die Zentale Ansprechstelle Cybercrime (ZAC) beim Landeskriminalamt eingerichtet. Das Team der ZAC steht für die Bürgerinnen und Bürger sowie Betroffene von Cybercrime aus der Wirtschaft, Verwaltung und Wissenschaft als

kompetenter Ansprechpartner zur Verfügung. Mit inzwischen über 600 Kontaktaufnahmen im Jahr hat sich die ZAC insbesondere auch zunehmend in der Unternehmenslandschaft als eine anerkannte und hochprofessionelle Einheit für die Bekämpfung von Cybercrime etabliert. Die ZAC ist auf Bundes-, Landes- und internationaler Ebene mit wichtigen Ansprechpartnern aus Wirtschaft, Wissenschaft und Behörden vernetzt. Zudem ist sie seit Jahren auch im präventiven Bereich tätig und beteiligt sich regelmäßig an IT-Sicherheitsveranstaltungen zusammen u. a. mit den Industrie- und Handelskammern sowie Wirtschaftsverbänden.

Im Mittelpunkt der ZAC-Aktivitäten steht die Sicherung von Beweisen für die Strafverfolgung (repressiver Ansatz), die Betreuung von Kooperationen und Allianzen, die Veröffentlichung von Warnmeldungen, die landesweite Steuerung von Informationen und tagesaktuelle Auswertung, die Durchführung von Awareness-Veranstaltungen und die Koordinierung der Task-Force Digitale Spuren des LKA. Die Aufgabe der ZAC ist es nicht, den von einer Cyber-Attacke betroffenen Betrieb wieder funktions- und arbeitsfähig zu machen, so beispielsweise verschlüsselte Daten zu entschlüsseln und Kundendaten wiederherzustellen („digitaler Tatortreiniger“).

In jedem der zwölf regionalen Polizeipräsidien wurden Anfang 2014 Kriminalinspektionen 5-„Cybercrime“ nach dem Vorbild der Abteilung im Landeskriminalamt eingerichtet. Ihre Mitarbeiterinnen und Mitarbeiter sind u. a. Spezialisten für die Bekämpfung der Cybercrime, Datenanalyse und Digitale Forensik.

Landesamt für Verfassungsschutz

Das LfV ist auch für die Bekämpfung geheimdienstlicher Aktivitäten anderer Staaten zuständig. Hierzu zählt auch die Abwehr elektronischer Angriffe mit mutmaßlich nachrichten-dienstlichem Hintergrund, die in den letzten Jahren spürbar zugenommen haben. Die Organisationseinheit Spionageabwehr des LfV steht potenziell Betroffenen im Fall von Cyberangriffen oder anderweitigen Spionageaktivitäten aufklärend und beratend zur Verfügung. Die Spionageabwehr beim LfV hat zahlreiche Einzelfälle und Fallkomplexe zu elektronischen Angriffen bearbeitet, die sich gegen Behörden, Unternehmen oder Einzelpersonen in Baden-Württemberg richteten.

Neben der repressiven Spionageabwehr der Strafverfolgungsbehörden nimmt das LfV Aufgaben der präventiven Spionageabwehr wahr und hat im Zusammenhang mit dem Behörden- und Wirtschaftsschutz einen Präventions- und Beratungsauftrag. Die

herausragende Bedeutung der Prävention bei der Bekämpfung der Wirtschaftsspionage wurde vom LfV frühzeitig erkannt. Durch verschiedene Maßnahmen des Wirtschaftsschutzes werden betroffene Unternehmen breitflächig unterstützt. So sind die Arbeitsbereiche Wirtschaftsschutz und Behördenschutz des LfV u. a. damit befasst, Unternehmen, Hochschulen und Behörden über die Spionagebedrohung aufzuklären und im Hinblick auf vorbeugende Schutzmaßnahmen zu beraten.

Der Arbeitsbereich Wirtschaftsschutz steht mit rund 650 Unternehmen, Kammern und Verbänden, die an einer festen Verbindung zum LfV interessiert sind, in Kontakt. Speziell über Vortragsveranstaltungen und Messeauftritte wird darüber hinaus regelmäßig eine Vielzahl weiterer Vertreter der o. g. Bereiche erreicht. Darüber hinaus unterhält das LfV zahlreiche Kontakte zu unterschiedlich organisierten Gremien überregionaler Stellen und Einrichtungen des Staates und der Wirtschaft.

Sicherheitsforum Baden-Württemberg

Das Sicherheitsforum Baden-Württemberg ist ein bereits im Jahr 2000 gegründetes unabhängiges Gremium aus Firmen, Forschungseinrichtungen, Verbänden, Kammern und Behörden. Das erklärte Ziel des Sicherheitsforums ist es, einen Beitrag dazu zu leisten, den Schutz der Wirtschaft vor Spionagetätigkeiten zu verstärken. Dazu findet u. a. ein fachlicher Austausch statt und es werden gemeinsame Sensibilisierungsveranstaltungen durchgeführt. Das Sicherheitsforum gibt Tipps und Hinweise, mit denen Unternehmen auf die Risiken und Schäden aufmerksam gemacht werden sollen, die ihnen durch ungewollten Know-how-Abfluss drohen. Seit 2007 vergibt das Sicherheitsforum im Zwei-Jahres-Rhythmus den Sicherheitspreis Baden-Württemberg für herausragende Projekte der betrieblichen Sicherheit mit Zielrichtung Know-how-Schutz. Die Aktivitäten des Sicherheitsforums zielen auf Beratung und Sensibilisierung ab. Aufgabe des Sicherheitsforums ist es nicht, Unternehmen, die Opfer von Cyberspionage sind, durch konkrete Hilfe vor Ort zu unterstützen.

Mitglieder des Sicherheitsforums sind: Allianz für Sicherheit in der Wirtschaft Baden-Württemberg e.V., Baden-Württembergischer Handwerkstag, Baden-Württembergischer Industrie- und Handelskammertag, Daimler AG, EnBW Energie Baden-Württemberg AG, Ministerium für Inneres, Digitalisierung und Migration Baden-Württemberg, Karlsruher Institut für Technologie, Landesamt für Verfassungsschutz Baden-Württemberg, Landeskriminalamt Baden-Württemberg, Landesverband der Baden-Württembergischen

Industrie e.V., Ministerium für Wirtschaft, Arbeit und Wohnungsbau Baden-Württemberg, SAP AG, Steinbeis-Stiftung, VDMA Baden-Württemberg.

Stellung der Cybewehr in der bestehenden Sicherheitsarchitektur

Die Cyberwehr Baden-Württemberg wird ein strategischer und operativer Partner der genannten Stellen in der bestehenden Sicherheitsarchitektur des Landes sein. Die jeweiligen Schnittstellen zur Cyberwehr werden dabei noch zu definieren sein. Ziel ist es, auch durch eine bessere Verzahnung der Aktivitäten ein genaueres und besseres Lagebild der Cybersicherheit im Land zu erstellen. Bei der im vierten Quartal 2017 anstehenden Neukonzeption des CERT BWL werden alle Kooperations- und Informationsschnittstellen entsprechend berücksichtigt. Die Zusammenführung bestehender Aktivitäten ebenso wie die Abgrenzung zu gegebenen Zuständigkeiten der beteiligten Akteure folgt dem bisher erarbeiteten Säulenkonzept „Prävention, Reaktion und Repression“.

2. *wie sie die Zusammenarbeit der Cyberwehr mit dem Verfassungsschutz und der Polizei, insbesondere dem Landeskriminalamt, konkret ausgestalten wird;*

Zu 2.:

Die Cyberwehr ist eines der Modellvorhaben aus der im Juli beschlossenen Digitalisierungsstrategie digital@bw der Landesregierung, deren Finanzierung - vorbehaltich der Entscheidungen des Haushaltsgesetzgebers - bis zum Ende der Legislaturperiode ausgelegt ist. Ziel ist es, insbesondere kleine und mittlere Unternehmen bei Cyber-Attacken eine schnelle Hilfe an die Hand zu geben, die es ihnen ermöglicht, ihre Geschäftstätigkeit schnellstmöglich wiederaufzunehmen und weiteren Schaden zu verhindern. Damit sollen derzeit bestehende Lücken in der Angebotsstruktur geschlossen und die Cybersicherheit bei kleinen und mittleren Unternehmen sowie Handwerksbetrieben erhöht werden. Die Cyberwehr wird ein Pilotvorhaben in der Technologieregion Karlsruhe.

Die Aktivitäten in der Pilotregion in Karlsruhe sollen in einem Steuerungsgremium fachlich begleitet werden, dem Vertreter des Konsortiums aus Karlsruhe, des LKA, des LfV, weitere Vertreter des Ministeriums für Inneres, Digitalisierung und Migration und des Ministeriums der Justiz und für Europa sowie des Ministeriums für Wirtschaft, Arbeit und Wohnungsbau unter der Koordinierung der Stabsstelle für Digitalisierung angehören

werden. Es soll sichergestellt werden, dass die beteiligten Stellen und Partner ihre Aktivitäten zur Stärkung der Cybersicherheit im Land koordiniert und vernetzt umsetzen.

3. *inwieweit durch die Cyberwehr Aufgaben beim Landesamt für Verfassungsschutz und der Polizei wegfallen oder das Landesamt für Verfassungsschutz und die Polizei entlastet werden;*

Zu 3.:

Ziel des Cyberwehr-Notfall-Einsatzes ist es, von Cyberattacken betroffene Unternehmen dabei zu unterstützen, ihren Betrieb zeitnah wieder aufzunehmen (z. B. Kundendaten zu entschlüsseln) und die erforderlichen IT-Sicherheitsmaßnahmen durchzuführen („digitaler Tatortreiniger“). Diese Aufgabenwahrnehmung fällt weder in die Zuständigkeit der Polizei noch des Landesamtes für Verfassungsschutz.

4. *welche hoheitlichen Befugnisse die Cyberwehr beziehungsweise Angehörige der Cyberwehr haben werden;*

Zu 4.:

Die schnelle Eingreiftruppe (Cyberwehr-Notfall-Team) wird überwiegend aus Experten der freien Wirtschaft rekrutiert. Hoheitliche Befugnisse werden auf die Experten der Wirtschaft nicht übertragen, da sie, wie bereits dargestellt, die Funktion des „digitalenTatortreinigers“ ohne repressiven Ansatz übernehmen werden. Sobald sich bei Cyberwehr-Notfall-Einsätzen Anhaltspunkte für eine Straftat ergeben, soll mit Einverständnis der betroffenen (angegriffenen) Unternehmen die ZAC des Landeskriminalamts hinzugezogen werden. Nur letztere handelt hoheitlich.

5. *welchen Stellenwert die Strafverfolgung bei der Arbeit der Cyberwehr haben wird;*

Zu 5.:

Siehe Ausführungen zu Ziffer 4.

6*. wie viele Personen beim Landesamt für Verfassungsschutz, bei der Polizei und bei weiteren Behörden derzeit in ihrem Hauptaufgabenfeld mit der Cybersicherheit, dem Schutz vor Cyberangriffen und Wirtschaftsspionage beschäftigt sind;*

Zu 6.:

Das LfV verfügt über drei Experten auf dem Themenfeld nachrichtendienstlich gesteuerter Cyberspionage und -sabotage. Diese werden im Einzelfall von weiteren Mitarbeitern des IT-Sicherheitsmanagements und des beratend tätigen Wirtschaftsschutzteams fachtechnisch unterstützt.

Bei der Polizei Baden-Württemberg stehen für die Bekämpfung der Cybercrime in den spezialisierten Einheiten landesweit über 450 Mitarbeiterinnnen und Mitarbeiter zur Verfügung. Mit Cybersicherheit, dem Schutz vor Cyberangriffen und Wirtschaftsspionage im engeren Sinne beschäftigen sich fünf Mitarbeiter beim Landeskriminalamt, die Präventions- und Awarenessvorträge bei Unternehmen und Behörden anbieten.

Die Informationssicherheitsorganisation der Landesverwaltung umfasst neben den in den Rechenzentren tätigen operativen Informationssicherheitsbeauftragten und Administratoren auch die in den einzelnen Ressorts im Staatshaushaltsplan 2017 geschaffenen 30 Stellen.

7. *über wie viele Stellen beziehungsweise wie viel Personal die Cyberwehr verfügen soll (darzustellen auch mittels Unterteilung in Beamte, Angestellte mit Tarifbindung, freie Mitarbeiter und außertariflich bezahltes Personal);*

Zu 7.:

Das Projekt soll mit 20 Experten für das Einsatzteam starten.

8. *inwieweit dabei auf Personal aus dem Landesamt für Verfassungsschutz und der Polizei zurückgegriffen werden soll;*

Zu 8.:

Siehe Ausführungen zu Ziffer 2.

9. *inwieweit Staatsanwälte der Cyberwehr angehören sollen;*

Zu 9.:

Das Ministerium der Justiz und für Europa soll mit Projektbeginn 2018 in das Steuerungsgremium der Cyberwehr Baden-Württemberg aufgenommen werden.

10. *in welchem Maße sie die Spitzen von Landesamt für Verfassungsschutz, Polizei, insbesondere dem Landeskriminalamt, und Justiz in ihre Planungen zur Cyberwehr eingebunden hat (aufzuzeigen unter anderem mittels Angabe der Tage, an denen sie beziehungsweise Angehörige des Innenministeriums mit den Spitzen von Landesamt für Verfassungsschutz, Polizei und Justiz konkret zur geplanten Cyberwehr kommuniziert haben);*

Zu 10.:

In den vergangenen Wochen wurden zwei Workshops mit Vertretern der Sicherheitsbehörden auf Arbeitsebene durchgeführt. Die leitenden Mitarbeiter des Innenministeriums und des Justizministeriums stehen in ständigem Kontakt.

11.
in welchem Maße sie Vertreter der Wirtschaft, wie beispielsweise Industrie- und Handelskammern in ihre Planungen zur Cyberwehr eingebunden hat (aufzuzeigen unter anderem mittels Angabe der Tage, an denen sie beziehungsweise Angehörige des Innenministeriums mit Vertretern der Wirtschaft konkret zur geplanten Cyberwehr kommuniziert haben);

Zu 11.:

Das Konsortium aus Karlsruhe hat zahlreiche Gespräche sowohl mit einzelnen Vertretern der Wirtschaft wie auch mit der IHK Karlsruhe, welche die digitalen Themen unter den IHKen in Baden-Württemberg koordiniert, geführt. Die IHK Karlsruhe hat eine Umfrage zu den Bedarfen der Unternehmen bei der Cybersicherheit durchgeführt, welche die IT-Themen (Cyberatacken) als vordringlich identifiziert hat (etwa ein Drittel der bisherigen rund 120 Rückmeldungen). Mit der eigentlichen Akquise und Schulung sowie Qualifizierung von Experten der Cyberwehr soll mit Beginn des Piloten in Karlsruhe begonnen werden. Darüber hinaus haben einige Unternehmen auf Grund der Ankündigungen in der Presse Kontakt mit dem Konsortium aufgenommen.

Herr Ministerialdirektor Stefan Krebs (CIO/CDO) hat am 2. März 2017 mit den Vertretern des CyberForum Karlsruhe, FZI, DIZ und Unternehmenvertretern über das Konzept des

Pilotprojekts Cyberwehr Karlsruhe im Ministerium für Inneres, Digitalisierung und Migration gesprochen. Am 11. Oktober fand ein CyberWehr-Gipfel in Karlsruhe statt.

12.
wie die Zusammenarbeit mit Cyber-Spezialisten aus Wirtschaft und Forschung organisatorisch ausgestaltet werden soll;

Zu 12.:

Vertreter der Forschung und der Wirtschaft sollen in das Steuerungsgremium der Cyberwehr Baden-Württemberg aufgenommen werden. Zudem sind zwei Forschungsprojekte mit den Schwerpunkten „Internet der Dinge“ und „autonomes Fahren“ geplant, die neben der Wirtschaft auch Erkenntnisse für die Arbeit der Strafverfolgungsbehörden generieren sollen.

13. *inwieweit Vertreter der Wirtschaft ihre Unterstützung signalisiert und konkretisiert haben;*

Zu 13.:

In das Konzept Cyberwehr sind die Erfahrungen und Bedarfe von Unternehmen des Netzwerks CyberForum in Karlsruhe eingeflossen. Stand heute startet das Projekt mit 20 Experten für das Notfall-Team. Die weitere Akquise soll, wie unter Ziffer 11 festgehalten, mit Projektstart ab 2018 beginnen.

14. *wie viele zusätzliche Stellen für Cybersicherheit und den Schutz vor Cyberangriffen und Wirtschaftsspionage sie beim Landesamt für Verfassungsschutz und der Polizei mit dem Haushalt 2017 geschaffen hat.*

Zu 14.:

Mit den Sonderprogrammen zur Bekämpfung des islamistischen Terrorismus wurden in den vergangenen drei Jahren 40 Neustellen im Bereich der Polizei für IT-Experten, Datenanalysten und Spezialisten für die Bekämpfung der Cybercrime geschaffen. Hiervon entfallen 13 Stellen auf den Haushalt 2017 (Sofortprogramm zur Intensivierung der Bekämpfung des islamistischen Terrorismus).

Mit freundlichen Grüßen

gez. Thomas Strobl
Minister für Inneres, Digitalisierung und Migration