Bayerischer Landtag

17. Wahlperiode

17.02.2017 17/14918

Schriftliche Anfrage

der Abgeordneten **Verena Osgyan**
BÜNDNIS 90/DIE GRÜNEN
vom 18.11.2016

IT-Sicherheit und Cyberabwehr in Bayern

Die Zuständigkeiten für IT-Sicherheit und Cyberabwehr in Bayern sind auf drei Ministerien aufgeteilt. In diesem wichtigen Bereich ist ein konzertiertes Handeln der Ministerien, eine reibungslose Kooperation des Freistaats mit dem Bund und ein effizienter Einsatz der verfügbaren finanziellen Mittel dringend nötig. Die Einrichtung des neuen Landesamts für IT-Sicherheit war in dem bisherigen Maßnahmenpaket „Bayern Digital“ der Staatsregierung nicht vorgesehen und lässt befürchten, dass es sich hier um ein Schaufensterprojekt handelt, das zu Reibungsverlusten, Kompetenzunklarheiten und Mittelverschwendung führt.

Ich frage die Staatsregierung:

1.1 Wie sieht die Cybersicherheitsstrategie des Freistaats Bayern aus?
1.2 Inwiefern ist die Cybersicherheitsstrategie des Freistaats mit dem Bund abgestimmt?
1.3 Wann begannen die Planungen für ein neues Landesamt für IT-Sicherheit?

2.1 Wer wurde bei den Planungen für das neue Landesamt beteiligt?
2.2 Wie soll das neue Landesamt für IT-Sicherheit organisiert sein (Organisationsaufbau, Aufgabenbereiche und jeweils geplante Personalausstattung für die einzelnen Bereiche)?
2.3 Wie sieht der Aufbaustab aus, der bereits im November 2016 eingerichtet sein soll?

3.1 Welches jährliche Budget ist für den Aufbau der Behörde bis 2025 eingeplant (bitte Aufschlüsselung nach Jahren)?
3.2 Welche Eingruppierungen sind für die zweihundert, für das neue Landesamt geplanten, Stellen vorgesehen?
3.3 Wie wird die Zusammenarbeit des Landesamts für IT-Sicherheit mit dem Kompetenzzentrum Cybercrime beim Bayerischen Landeskriminalamt (Zentrale Ansprechstelle Cybercrime beim Bayerischen Landeskriminalamt – ZAC), der Zentralstelle Cybercrime Bayern (ZCB) bei der Generalstaatsanwaltschaft Bamberg, dem Cyber-Allianz-Zentrum des Landesamts für Verfassungsschutz (CAZ) und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) garantiert?

4.1 Welche Aufgaben soll das neue Landesamt übernehmen, die nicht durch die bereits bestehenden Einrichtungen auf Landes- und Bundesebene übernommen werden könnten?
4.2 Inwieweit orientiert sich der Freistaat bei Vorgaben an seine Behörden an den Mindeststandards, die das BSI für die IT in den Bundesbehörden festlegt?
4.3 Wie stellt die Staatsregierung sicher, dass es im Bereich „Kritischer Infrastrukturen“ – hier fungiert das BSI als zentrale Meldestelle – keine Überschneidungen zwischen dem neuen Landesamt für IT-Sicherheit und dem BSI gibt?

5.1 Inwiefern unterscheiden sich die Aufgaben, die das neue Landesamt für IT-Sicherheit nun übernehmen soll, von jenen, die bisher vom Bayern-CERT, das beim Landesamt für Finanzen in München angesiedelt ist, übernommen werden?
5.2 Soll Bayern-CERT in seinem bisherigen Umfang und mit seinen bisherigen Aufgaben, insbesondere auch Internetangebote der Behörden und Kommunen vor Hackerangriffen zu schützen, nach der Einrichtung des neuen Landesamtes so weiterbestehen?
5.3 Mit welchem jährlichen Budget ist Bayern-CERT bisher ausgestattet?

6.1 Wie viele Mitarbeiterinnen und Mitarbeiter umfasst Bayern-CERT?
6.2 Mit welchen Unternehmen der bayerischen IT-Sicherheitsindustrie wird das neue Landesamt für IT-Sicherheit kooperieren?
6.3 Mit welchen Einrichtungen aus der Wissenschaft wird das neue Landesamt für IT-Sicherheit kooperieren?

7.1 Wie wird die laut Staatsminister Dr. Markus Söder „enge Kooperation mit der Wissenschaft und der bayerischen IT-Sicherheitsindustrie“ mit dem neuen Landesamt ausgestaltet sein?
7.2 Warum ist das Staatsministerium der Finanzen, für Landesentwicklung und Heimat (StMFLH) bisher kein Kooperationspartner des Bavarian IT Security & Safety Cluster?
7.3 Wie bewertet die Staatsregierung die Aufteilung der Kompetenzen im Bereich IT-Sicherheit auf drei Ministerien?

8.1 Bis wann soll der Ausbau des Fraunhofer-Instituts in Garching zu einem Sicherheitskompetenzzentrum von nationaler und europäischer Bedeutung, wie im Konzept „Digital Bavaria“ angekündigt, abgeschlossen sein?
8.2 Auf wie viel belaufen sich die finanziellen Mittel, die für den Ausbau des Sicherheitskompetenzzentrums zur Verfügung gestellt wurden?
8.3 Welche Aufgaben kommen dem Sicherheitskompetenzzentrum zu?

Antwort

des Staatsministeriums der Finanzen, für Landesentwicklung und Heimat
vom 27.12.2016

1.1 Wie sieht die Cybersicherheitsstrategie des Freistaats Bayern aus?

In Abstimmung mit dem Staatsministerium des Innern, für Bau und Verkehr (StMI) wird die Frage wie folgt beantwortet:

Die Verfügbarkeit des Cyberraums und der Schutz der darin vorhandenen Daten sind in unserer zunehmend vernetzten Welt zu einer existenziellen Frage (des 21. Jahrhunderts) geworden. Deshalb ist es eine gemeinsame Herausforderung für Staat, Wirtschaft und Gesellschaft, für ein hohes Maß an Cybersicherheit zu sorgen. Die Gewährleistung von Cybersicherheit ist ein zentrales Querschnittsthema, das alle Gesellschaftsbereiche angeht.

Auch wenn die primäre Verantwortung für die Sicherheit der eigenen Daten und die Integrität der eigenen IT-Systeme beim jeweiligen Nutzer liegt, kommt dem Staat eine Schutzfunktion zu.

Um dieser Verantwortung im Freistaat Bayern gerecht zu werden, hat die Staatsregierung im April 2013 die Bayerische Cybersicherheitsstrategie beschlossen. Mit dem ressortübergreifenden Konzept sollen die staatliche Handlungsfähigkeit geschützt und die Sicherheitsbehörden gestärkt werden. Im Fokus stehen zudem der Schutz der Wirtschaft vor Cyberspionage und -sabotage sowie der Schutz der Bürgerinnen und Bürger durch Beratung und Sensibilisierung. Mit der Strategie werden alle für die Cybersicherheit relevanten Akteure vernetzt.

Das StMI berichtet dem Landtag jährlich zur Umsetzung der Bayerischen Cybersicherheitsstrategie (vgl. Beschlüsse vom 23.10.2014, Drs. 17/3664 und 17/3665). Wegen der Einzelheiten wird auf die Berichte vom 29.12.2014 und 27.11.2015 verwiesen. Der Bericht für das Jahr 2016 wird dem Landtag bis spätestens 31.12.2016 zugeleitet.

1.2 Inwiefern ist die Cybersicherheitsstrategie des Freistaats mit dem Bund abgestimmt?

In Abstimmung mit dem StMI wird die Frage wie folgt beantwortet:

Das Bundesministerium des Innern (BMI) hat die Länder im Rahmen der Fortschreibung der Cybersicherheitsstrategie der Bundesregierung beteiligt. Das StMI gab zu einem Eckpunktepapier des BMI – nach Einbindung der betroffenen Ressorts – eine fachliche Stellungnahme ab und nahm an einer Bund-Länder-Besprechung am 07.04.2016 im BMI teil.

1.3 Wann begannen die Planungen für ein neues Landesamt für IT-Sicherheit?

Mit den konkreten Planungen wurde im August 2016 unmittelbar nach dem Beschluss des Kabinetts begonnen, ein Landesamt für Sicherheit in der Informationstechnik zu gründen.

2.1 Wer wurde bei den Planungen für das neue Landesamt beteiligt?

An den Planungen werden die betroffenen Ressorts, insbesondere das StMI und das Staatsministerium für Wirtschaft und Medien, Energie und Technologie (StMWi) und der Datenschutzbeauftragte des Freistaats beteiligt.

2.2 Wie soll das neue Landesamt für IT-Sicherheit organisiert sein (Organisationsaufbau, Aufgabenbereiche und jeweils geplante Personalausstattung für die einzelnen Bereiche)?

Die organisatorische Ausgestaltung wird derzeit erarbeitet. Neben der Beratung und Information zum sicheren Umgang mit IT wird die Angriffsfrüherkennung, die Abwehr von Cyberangriffen, die Analyse kompromittierter IT-Systeme und die Weiterentwicklung der Sicherheitskonzepte der Verwaltungsnetze zu den Aufgabenschwerpunkten gehören. Das neue Landesamt für IT-Sicherheit (LSI) wird neben den klassischen Aufgaben der Hacker- und Cyberabwehr auch Sicherheitsaufgaben für andere Institutionen wie die staatlichen Rechenzentren – den BayernServer – übernehmen. Das LSI wird auch Bürgerinnen und Bürgern als kompetente Beratungsstelle zur Verfügung stehen und regelmäßig zur aktuellen Gefahrenlage über die gängigen Informationskanäle informieren. Daneben wird das LSI auch den Kommunen hilfreiche praktische Informationen zur Absicherung ihrer IT-Systeme bereitstellen. Das LSI soll künftig die Kommunen nicht nur beraten, sondern ganz konkrete IT-Sicherheitsdienstleistungen erbringen.

Das LSI soll bis zum Jahr 2025 sukzessive mit bis zu 200 Stellen ausgestattet werden.

2.3 Wie sieht der Aufbaustab aus, der bereits im November 2016 eingerichtet sein soll?

Es besteht ein Lenkungsausschuss, der sich aus fachlich betroffenen Angehörigen des Staatsministeriums der Finanzen, für Landesentwicklung und Heimat (StMFLH) und der Personalvertretung zusammensetzt.

3.1 Welches jährliche Budget ist für den Aufbau der Behörde bis 2025 eingeplant (bitte Aufschlüsselung nach Jahren)?

Im Doppelhaushalt 2017/2018 stehen für den Aufbau des LSI insgesamt 15 Mio. Euro zur Verfügung, davon 5 Mio. Euro in 2017 und 10 Mio. Euro in 2018. Darüber hinaus sind Verpflichtungsermächtigungen für Mieten vorgesehen.

3.2 Welche Eingruppierungen sind für die zweihundert, für das neue Landesamt geplanten, Stellen vorgesehen?

Über künftige Stellen und deren Bewertung wird in künftigen Haushalten entschieden.

3.3 Wie wird die Zusammenarbeit des Landesamts für IT-Sicherheit mit dem Kompetenzzentrum Cybercrime beim Bayerischen Landeskriminalamt (Zentrale Ansprechstelle Cybercrime beim Bayerischen Landeskriminalamt – ZAC), der Zentralstelle Cybercrime Bayern (ZCB) bei der Generalstaatsanwaltschaft Bamberg, dem Cyber-Allianz-Zentrum des Landesamts für Verfassungsschutz (CAZ) und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) garantiert?

Über die künftige Zusammenarbeit mit diesen Stellen wird in Abstimmung mit den zuständigen Ressorts entschieden.

4.1 Welche Aufgaben soll das neue Landesamt übernehmen, die nicht durch die bereits bestehenden Einrichtungen auf Landes- und Bundesebene übernommen werden könnten?

Siehe Antwort auf Frage 2.2.

4.2 Inwieweit orientiert sich der Freistaat bei Vorgaben an seine Behörden an den Mindeststandards, die das BSI für die IT in den Bundesbehörden festlegt?

Eine Orientierung an den BSI-Standards erfolgt im Rahmen der Vorgaben der für Bund und Länder verbindlichen Leitlinie für Informationssicherheit des IT-Planungsrats.

4.3 Wie stellt die Staatsregierung sicher, dass es im Bereich „Kritischer Infrastrukturen" – hier fungiert das BSI als zentrale Meldestelle – keine Überschneidungen zwischen dem neuen Landesamt für IT-Sicherheit und dem BSI gibt?

Das BSI ist kraft Bundesrechts die zentrale Meldestelle für Betreiber Kritischer Infrastrukturen in Angelegenheiten der Sicherheit der Informationstechnik (vgl. § 8 b des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik). Überschneidungen zu den landesrechtlichen Zuständigkeiten des neuen LSI sind deshalb nicht zu erwarten.

5.1 Inwiefern unterscheiden sich die Aufgaben, die das neue Landesamt für IT-Sicherheit nun übernehmen soll, von jenen, die bisher vom Bayern-CERT, das beim Landesamt für Finanzen in München angesiedelt ist, übernommen werden?

Das Bayern-CERT wird mit seinen Aufgaben in das neue Landesamt integriert und bildet den Kern der neuen Sicherheitsbehörde.

5.2 Soll Bayern-CERT in seinem bisherigen Umfang und mit seinen bisherigen Aufgaben, insbesondere auch Internetangebote der Behörden und Kommunen vor Hackerangriffen zu schützen, nach der Einrichtung des neuen Landesamtes so weiterbestehen?

Siehe Antwort auf Frage 5.1.

5.3 Mit welchem jährlichen Budget ist Bayern-CERT bisher ausgestattet?

In den Jahren 2015 und 2016 war das CERT mit ca. 1,5 Mio. Euro ausgestattet.

6.1 Wie viele Mitarbeiterinnen und Mitarbeiter umfasst Bayern-CERT?

Derzeit sind 11 Mitarbeiter beim Bayern-CERT beschäftigt.

6.2 Mit welchen Unternehmen der bayerischen IT-Sicherheitsindustrie wird das neue Landesamt für IT-Sicherheit kooperieren?

Konkrete Kooperationsvereinbarungen mit einzelnen Unternehmen können erst nach Gründung des Landesamts geschlossen werden.

6.3 Mit welchen Einrichtungen aus der Wissenschaft wird das neue Landesamt für IT-Sicherheit kooperieren?

Konkrete Kooperationsvereinbarungen mit einzelnen Einrichtungen können erst nach Gründung des Landesamts geschlossen werden.

7.1 Wie wird die laut Staatsminister Dr. Markus Söder „enge Kooperation mit der Wissenschaft und der bayerischen IT-Sicherheitsindustrie" mit dem neuen Landesamt ausgestaltet sein?

Die enge Kooperation mit der Wissenschaft und der bayerischen IT-Sicherheitsindustrie soll primär als Know-how-Transfer zwischen den Kooperationspartnern ausgestaltet werden. So können die Anforderungen der Verwaltung an IT-Sicherheitsprodukte und deren Weiterentwicklung schnell und ohne Reibungsverlust an die Forschung und Entwicklung herangetragen werden. Ferner wird sichergestellt, dass das neue Landesamt am Stand der Technik als hochmodernes Anti-Hacker-Zentrum agieren kann.

7.2 Warum ist das Staatsministerium der Finanzen, für Landesentwicklung und Heimat (StMFLH) bisher kein Kooperationspartner des Bavarian IT Security & Safety Cluster?

Das StMFLH arbeitet bei der Stärkung der IT-Sicherheit in den Kommunen eng mit dem Cluster zusammen. So hat etwa der IT-Beauftragte der Staatsregierung im IT-Planungsrat einen Beschluss herbeigeführt, der eine vom Cluster erarbeitete Vorgehensweise für das IT-Sicherheitsmanagement in Kommunen als gleichwertig zu den BSI-Standards anerkennt.

7.3 Wie bewertet die Staatsregierung die Aufteilung der Kompetenzen im Bereich IT-Sicherheit auf drei Ministerien?

IT-Sicherheit betrifft alle Bereiche des staatlichen Handelns. Die im Bereich IT-Sicherheit auf drei Ministerien verteilten Kompetenzen orientieren sich an den grundsätzlichen Zuständigkeitsbereichen der betroffenen Ministerien. Die ressortübergreifende Verantwortung für die Funktionsfähigkeit der staatlichen IT-Nutzung liegt beim IT-Beauftragten der Staatsregierung. Mit der Bayerischen Cybersicherheitsstrategie wurde die ressortübergreifende Zusammenarbeit im Bereich Cybersicherheit seit Mitte 2013 intensiviert. Auf die jährlichen Berichte des StMI zur Umsetzung der Bayerischen Cybersicherheitsstrategie wird verwiesen (Berichte vom 27.11.2015 und 29.12.2014 zu den Landtagsdrucksachen 17/3664 und 17/3665).

8.1 Bis wann soll der Ausbau des Fraunhofer-Instituts in Garching zu einem Sicherheitskompetenzzentrum von nationaler und europäischer Bedeutung, wie im Konzept „Digital Bavaria" angekündigt, abgeschlossen sein?

In Abstimmung mit dem StMWI wird die Frage wie folgt beantwortet: Das Förderprojekt zum Ausbau des Fraunhofer-Instituts läuft bis zum 31.05.2020.

8.2 Auf wie viel belaufen sich die finanziellen Mittel, die für den Ausbau des Sicherheitskompetenzzentrums zur Verfügung gestellt wurden?

In Abstimmung mit dem StMWI wird die Frage wie folgt beantwortet: Die Mittel belaufen sich auf 4.536.378,00 €.

8.3 Welche Aufgaben kommen dem Sicherheitskompetenzzentrum zu?

In Abstimmung mit dem StMWI wird die Frage wie folgt beantwortet:

Zum Ausbau des Fraunhofer AISEC in Garching zu einem Sicherheitskompetenzzentrum von nationaler und europäischer Bedeutung werden Sicherheitslabore auf höchstem technologischen Niveau eingerichtet und weitere Kompetenzfelder besetzt, die im Zusammenhang mit der Digitali-

sierung für die Innovationsfähigkeit der bayerischen Wirtschaft von höchster Wichtigkeit sind.

Ergänzend dazu wird mit dem Kompetenzzentrum für Cybersicherheit, das ebenfalls bei AISEC angesiedelt ist, der Technologietransfer spezifisch für kleine und mittlere Unternehmen (KMU) ausgebaut. Dies erfolgt in Anwenderlabors, die zum einen Test- und Analysezwecken dienen, zum anderen für Industriepartner als Testlabore und Schulungslabore zur Verfügung gestellt werden sollen.