



Schriftliche Anfrage

des Abgeordneten **Gerd Mannes AfD**
vom 09.09.2019

Förderung der Cybersicherheit in Bayern

Ich frage die Staatsregierung:

- 1.1 Wie schätzt die Staatsregierung den aktuellen Zustand der Cybersicherheit der Wirtschaft in Bayern ein?
- 1.2 Wie steht es aus Sicht der Staatsregierung um die Cybersicherheit der Bürger in Bayern?
- 1.3 Wie steht es aus Sicht der Staatsregierung um die Cybersicherheit der Behörden in Bayern?

- 2.1 Wie schätzt die Staatsregierung den aktuellen Zustand der Cybersicherheit der Landesregierung ein?
- 2.2 Welche Strategie verfolgt die Staatsregierung im Bereich der Cybersicherheit (bitte erläutern und falls vorhanden Strategieplan nennen)?

- 3.1 Welche Förderprogramme im Bereich der Cybersicherheit laufen aktuell (bitte Beschreibung, Haushaltstitel und ausgeschöpfte Mittel seit 2010 pro Jahr angeben)?
- 3.2 Welche Förderprogramme im Bereich der Cybersicherheit sind für die Zukunft geplant?

4. In welchen themenübergreifenden, breiteren Förderprogrammen wurde unter anderem die Cybersicherheit unterstützt (bitte Beschreibung, Haushaltstitel und ausgeschöpfte Mittel seit 2010 pro Jahr angeben)?

5. Hat die Staatsregierung Kenntnis über Fördermaßnahmen der EU im Bereich der Cybersicherheit in Bayern (bitte – falls bekannt – Fördermaßnahmen mit Förderhöhe auflisten)?

6. Hat die Staatsregierung Kenntnis über Fördermaßnahmen des Bundes im Bereich der Cybersicherheit in Bayern (bitte – falls bekannt – Fördermaßnahmen mit Förderhöhe auflisten)?

Antwort

des Staatsministeriums des Innern, für Sport und Integration im Einvernehmen mit dem Staatsministerium der Finanzen und für Heimat, dem Staatsministerium für Wirtschaft, Landesentwicklung und Energie sowie dem Staatsministerium für Digitales

vom 14.10.2019

- 1.1 Wie schätzt die Staatsregierung den aktuellen Zustand der Cybersicherheit der Wirtschaft in Bayern ein?**
- 1.2 Wie steht es aus Sicht der Staatsregierung um die Cybersicherheit der Bürger in Bayern?**
- 1.3 Wie steht es aus Sicht der Staatsregierung um die Cybersicherheit der Behörden in Bayern?**

Zu den Beschlüssen Drs. 17/3664 und 17/3665 berichtet das Staatsministerium des Innern, für Sport und Integration jährlich zur Evaluation der Bayerischen Cybersicherheitsstrategie und zu Cybercrime in Bayern – soweit darüber hinaus die IT-Sicherheit von Behörden angesprochen ist, gemeinsam mit dem Staatsministerium der Finanzen und für Heimat – unter Einbindung aller Ressorts. Dieser Bericht, der mit Schreiben vom 18.01.2019 an den Landtag übermittelt wurde, stellt für das Berichtsjahr 2018 eine umfassende Bewertung im Sinne der Fragestellungen dar. Für den Bereich der Cyberkriminalität darf darüber hinaus auf den Pressebericht zur Polizeilichen Kriminalstatistik Bayern 2018 verwiesen werden, welcher unter www.polizei.bayern.de/content/6/4/9/pks_pressebericht_2018.pdf öffentlich abrufbar ist. Eine darüber hinausgehende, unterjährige Auswertung der Polizeilichen Kriminalstatistik findet nicht statt.

- 2.1 Wie schätzt die Staatsregierung den aktuellen Zustand der Cybersicherheit der Landesregierung ein?**

Auf die Antwort zu Fragen 1.1 bis 1.3 wird verwiesen.

- 2.2 Welche Strategie verfolgt die Staatsregierung im Bereich der Cybersicherheit (bitte erläutern und falls vorhanden Strategieplan nennen)?**

Die Staatsregierung stellte bereits mit der im Jahr 2013 auf den Weg gebrachten Cybersicherheitsstrategie die Weichen für ein konsequentes Vorgehen gegen Angriffe aus der Cyberwelt. Kernziele der Bayerischen Cybersicherheitsstrategie sind:

- Schutz der Bürgerinnen und Bürger durch Beratung und Sensibilisierung,
- Schutz der staatlichen Handlungsfähigkeit, Stärkung der Sicherheitsbehörden,
- Schutz der Wirtschaft vor Spionage und Sabotage,
- Vernetzung aller für Cybersicherheit wichtigen Akteure.

Im Juli 2013 wurde das Cyber-Allianz-Zentrum (CAZ) beim Landesamt für Verfassungsschutz errichtet. Seit seiner Gründung hat sich das CAZ als zentraler, vertrauenswürdiger und kompetenter Ansprechpartner für Unternehmen, Hochschulen und Betreiber kritischer Infrastrukturen etabliert, wenn es um elektronische Angriffe mit Spionage- oder Sabotagehintergrund geht. Freiwillig gemeldete Vorfälle werden forensisch-technisch untersucht und nachrichtendienstlich bewertet. Mit (anonymisierten) Warnhinweisen werden andere Unternehmen informiert, um die ggf. eigene Betroffenheit feststellen bzw. sich gegen entsprechende Angriffe schützen zu können.

Angesichts der Herausforderung der Cyberkriminalität hat die Staatsregierung auch schon frühzeitig mit umfangreichen Maßnahmen bei der Bayerischen Polizei reagiert. Neben der Einrichtung eines eigenen Fachdezernats beim Landeskriminalamt und der Zentralen Ansprechstelle Cybercrime (ZAC) im Januar 2014 wurden zum 01.03.2017 auch flächendeckend bei grundsätzlich jeder Kriminalpolizeiinspektion „Cybercrime“-Kommissariate eingerichtet. Darüber hinaus wurde als wichtiger Baustein der Cybercrime-Bekämpfung in Bayern die spezielle Laufbahn für IT-Kriminalisten geschaffen. Studierte Informatikerinnen und Informatiker werden hierbei in einer einjährigen polizeifachlichen Unterweisung zu Polizeivollzugsbeamten ausgebildet. So wird technisches Wissen mit polizeilichen Rechten und Kenntnissen kombiniert, um auch professionellen Straftätern auf Augenhöhe begegnen zu können. Die Aus- und Fortbildung der Polizei

im Bereich Cybercrime wird so intensiviert und die Ermittlungseinheiten werden mit externer IT-Expertise verstärkt.

Darüber hinaus besteht seit dem 01.01.2015 bei der Generalstaatsanwaltschaft Bamberg die Zentralstelle Cybercrime Bayern (ZCB). Diese Zentralstelle ist bayernweit zuständig für die Bearbeitung herausgehobener Ermittlungsverfahren im Bereich der Cyberkriminalität. Sie ermittelt in Zusammenarbeit mit den entsprechenden Spezialisten der bayerischen Polizei oder des Bundeskriminalamts und mit internationalen Partnern z. B. bei Angriffen auf bedeutende Wirtschaftszweige oder bei Verfahren aus dem Bereich der organisierten Cyberkriminalität. Auch dann, wenn bei Verfahren der Allgemeinkriminalität ein hoher Ermittlungsaufwand im Bereich der Computer- und Informationstechnik abzuarbeiten ist, werden die Staatsanwälte der Zentralstelle tätig. Seit dem 01.08.2018 ist die ZCB zudem für herausgehobene Fälle der Wirtschaftscyberkriminalität zuständig. Die bearbeiteten Fälle sind vielfältig: Sie reichen von Hackerangriffen über Fälle des Vorkassebetrugs im Internet, z. B. durch professionelle sog. Fake-Shops, und Fälle von Ransomware bis hin zum Handel mit Waffen, Drogen, Falschgeld und Kinderpornografie im Darknet.

Auch hat die Staatsregierung in den letzten Jahren wesentliche Maßnahmen umgesetzt, um die IT-Sicherheit der Verwaltung weiter zu verbessern. Hervorzuheben ist insbesondere die Gründung des Landesamts für Sicherheit in der Informationstechnik (LSI) zum 01.12.2017. Mit der Gründung der Behörde geht insbesondere auch eine massive personelle Verstärkung im sogenannten CERT-Bereich (Computer Emergency Response Team) einher. Bayern hebt sich gerade in diesem Punkt im Kreis der Länder deutlich ab. Das LSI ist mit ausreichend Befugnissen ausgestattet, um IT-Sicherheit im Bayerischen Behördennetz durchsetzen zu können (vgl. Art. 12 ff Bayerisches E-Government-Gesetz – BayEGovG). Als weitere Maßnahmen sind die deutliche Anhebung des Verschlüsselungsniveaus im Bayerischen Behördennetz im Zuge der letzten Ausschreibung sowie die laufende Etablierung von IT-Sicherheitsprozessen in den Behörden zu erwähnen. Im Verwaltungs-CERT-Verbund werden zudem wertvolle Informationen zu konkreten Gefährdungen zwischen den Ländern untereinander und mit dem Bund ausgetauscht.

Auch im kommunalen Bereich ist dem Thema IT-Sicherheit große Aufmerksamkeit zu widmen. Die Staatsregierung verfolgt deshalb beispielsweise den Ansatz, die kommunale Familie von den Erfahrungen der Sicherheitsorganisation des Freistaates profitieren zu lassen und eine speziell auf behördliche Bedürfnisse zugeschnittene Unterstützung anzubieten. Insbesondere unterstützt das LSI die Kommunen mit Informations- und Vernetzungsangeboten und berät bei konkreten Fragestellungen individuell und herstellerunabhängig. Um den Einstieg in das Thema IT-Sicherheit zu erleichtern und Orientierung zu geben, vergibt das LSI seit Mai 2019 zudem das Siegel „Kommunale IT-Sicherheit“ an Kommunen, die grundlegende Maßnahmen umgesetzt haben. Zudem arbeitet die Staatsregierung darauf hin, wesentlich mehr Gemeinden den Anschluss an das sichere Behördennetz zu ermöglichen.

Im Ministerrat vom 26.02.2019 wurde die Initiative „Online – aber sicher!“ gestartet, um die Cybersicherheit noch weiter gehend zu stärken und fortzuentwickeln. Diese enthält insgesamt 35 Maßnahmen, deren Umsetzung unter Federführung des Staatsministeriums für Digitales zügig vorangetrieben wird. Ein Schwerpunkt des umfassenden Maßnahmenpaketes ist es, die Bürgerinnen und Bürger, Unternehmen und Kommunen beim Schutz ihrer Daten zu unterstützen und im konkreten Einzelfall schnell und unbürokratisch zu helfen.

Als gemeinsame Initiative des Staatsministeriums des Innern, für Sport und Integration und des Staatsministeriums für Digitales wurde eine Hotline für IT-Notfälle eingerichtet. Bürgerinnen und Bürger können sich beim Verdacht von Angriffen auf ihre IT an die kompetenten Ansprechpartner des Landeskriminalamtes wenden und erhalten schnell und unbürokratisch Hilfe.

3.1 Welche Förderprogramme im Bereich der Cybersicherheit laufen aktuell (bitte Beschreibung, Haushaltstitel und ausgeschöpfte Mittel seit 2010 pro Jahr angeben)?

Seit Juli 2015 fördert das Staatsministerium des Innern, für Sport und Integration die bayerischen Kommunen bei der Einführung eines Informationssicherheits-Managementsystems (ISMS). Mit dem Förderprogramm soll rasch und nachhaltig ein hohes IT-Sicherheitsniveau in der bayerischen Kommunalverwaltung erreicht werden.

Insgesamt wurden für das Förderprogramm von 2015–2020 rd. 12 Mio. Euro im Haushalt bereitgestellt (Haushaltstitel: Kap. 0303 Tit. 633 03 und Tit. 547 09). In der Förderperiode 2015/2016 wurden hieraus Fördermittel in Höhe von 753.073,00 Euro, in der Förderperiode 2017/2018 in Höhe von 2.642.163,00 Euro und im Jahr 2019 bislang in Höhe von 311.409,21 Euro (Stand: 23.09.2019) bewilligt.

3.2 Welche Förderprogramme im Bereich der Cybersicherheit sind für die Zukunft geplant?

Zu neuen Förderprogrammen im Bereich der Cybersicherheit gibt es noch keine Festlegungen.

4. In welchen themenübergreifenden, breiteren Förderprogrammen wurde unter anderem die Cybersicherheit unterstützt (bitte Beschreibung, Haushaltstitel und ausgeschöpfte Mittel seit 2010 pro Jahr angeben)?

Der Digitalbonus (Haushaltstitel: Kap. 0703 Tit. 683 01) hat sich zu einem wichtigen wirtschaftspolitischen Instrument entwickelt. Er unterstützt die Unternehmen, sich für die Herausforderungen der digitalen Welt zu rüsten. Gefördert werden digitale Produkte, Prozesse und Dienstleistungen sowie Investitionen in die IT-Sicherheit.

Die Nachfrage nach dem Digitalbonus ist immens. Seit Start des Programms im Oktober 2016 gingen bayernweit über 11.800 Anträge auf Förderung ein. Mit mehr als 131 Mio. Euro an beantragten Zuschüssen wurden bereits Investitionen von über 380 Mio. Euro angestoßen. Davon entfallen 2.555 Anträge auf den Förderbereich 2.2, in dem IT-Sicherheitsprojekte gefördert werden.

Insgesamt wurden im Förderbereich IT-Sicherheit 21,1 Mio. Euro beantragt, davon wurden bereits knapp 14 Mio. Euro bewilligt.

Darüber hinaus wurden Projekte mit Bezug zum Themenbereich IT-Sicherheit im Rahmen folgender Förderprogramme unterstützt:

- Bayerisches Förderprogramm für Forschung und Entwicklung Informations- und Kommunikationstechnik IUK (bzw. seit 01.07.2019 das Bayerische Verbundforschungsprogramm [BayVFP] – Förderlinie Digitalisierung, Schwerpunkt Informations- und Kommunikationstechnik). Nähere Informationen zum Förderprogramm inkl. Förderrichtlinie sind unter www.iuk-bayern.de abrufbar. Die Finanzierung erfolgt aus Kap. 07 03 Tit. 686 69 sowie Tit. 685 69.
- Bayerisches Förderprogramm für Forschung und Entwicklung Mikrosystemtechnik MST (bis 31.12.2015), danach Bayerisches Förderprogramm für Forschung und Entwicklung Elektronische Systeme ESB (bzw. seit 01.07.2019 das Bayerische Verbundforschungsprogramm [BayVFP] – Förderlinie Digitalisierung, Schwerpunkt Elektronische Systeme). Nähere Informationen zum Förderprogramm inkl. Förderrichtlinie sind unter www.elsys-bayern.de abrufbar. Die Finanzierung erfolgt aus Kap. 07 03 Tit. 683 67.
- Förderung von Forschungs- und Technologievorhaben im Rahmen des nationalen zivilen Luftfahrtforschungsprogramms (LuFo Bund) in der jeweils aktuell gültigen Fassung. Anwendung in Bayern über gemeinsame Notifizierung des Programms durch die EU-Kommission für Bund und Länder. Nähere Informationen beim zuständigen Projektträger, dem PT DLR Luftfahrtforschung und -technologie unter www.dlr.de/pt-lf. Die Finanzierung erfolgt aus Kap. 07 03 Tit. 683 65 und Kap. 07 03 Tit. 686 60.
- Bayerisches Programm zur Förderung technologieorientierter Unternehmensgründungen (BayTOU); nähere Informationen zum Förderprogramm inkl. Förderrichtlinie sind unter www.stmwi.bayern.de/service/foerderprogramme/technologiefoerderung/ abrufbar. Die Finanzierung erfolgt aus Kap. 07 03 Tit. 683 64.
- Bayerisches Technologieförderungsprogramm plus (BayTP+) seit 01.07.2019, vorher Bayerisches Technologieförderungsprogramm; nähere Informationen zum Förderprogramm inkl. Förderrichtlinie sind unter www.stmwi.bayern.de/service/foerderprogramme/technologiefoerderung/ abrufbar. Die Finanzierung erfolgt aus Kap. 07 03 Tit. 893 65.
- Fördergrundsätze Modellregionen Elektromobilität MOD (Programmlaufzeit: 15.08.2011–31.12.2014); nähere Informationen zu den Modellregionen Elektromo-

- SHARCS, Information and Communication Technologies, 321.250 Euro, <http://cordis.europa.eu/project/id/644571>
- FutureTPM, Secure societies – Protecting freedom and security of Europe and its citizens, 320.575 Euro, <http://cordis.europa.eu/project/id/779391>
- CONCORDIA, Cyber security cOMpeteNce fOr Research anD Innovation, 2.344.612,50 Euro, <http://cordis.europa.eu/project/id/830927>
- SPARTA, Strategic programs for advanced research and technology in Europe, 1.552,517,50 Euro, <http://cordis.europa.eu/project/id/830892>
- CyberSec4Europe, Cyber Security Network of Competence Centres for Europe, 493.711,25 Euro, <http://cordis.europa.eu/project/id/830929>

6. Hat die Staatsregierung Kenntnis über Fördermaßnahmen des Bundes im Bereich der Cybersicherheit in Bayern (bitte – falls bekannt – Fördermaßnahmen mit Förderhöhe auflisten)?

Das Bundesministerium für Bildung und Forschung hat die VDI/VDE-IT GmbH mit der Projektträgerschaft Kommunikationssysteme; IT-Sicherheit beauftragt. Laut dieser wurden in Bayern im Rahmen der nachfolgend genannten Bekanntmachungen/Förderaufrufe bayerische Projektpartner jeweils insgesamt in der angegebenen Höhe gefördert. Es ist dabei jeweils die Höhe der bewilligten Zuwendungen angegeben. In der Datenauswertung wurden nur aktuell laufende Projekte berücksichtigt:

- Anwendungsszenarien der Quantenkommunikation: 3.410.457 Euro
- IT-Sicherheit und Autonomes Fahren: 5.073.303 Euro
- Privatheit und informationelle Selbstbestimmung in der digitalen Arbeitswelt: 1.585.630 Euro
- Selbstschutz: 486.636 Euro
- Erkennung und Aufklärung von IT-Sicherheitsvorfällen: 2.672.494 Euro
- Hightech für IT-Sicherheit: 7.437.948 Euro
- Initiativvorhaben: 6.505.772 Euro
- KMU-innovativ: Informations- und Kommunikationstechnologie (IKT): 3.481.801 Euro
- Post-Quanten-Kryptografie: 3.889.297 Euro
- Privacy Forum: 727.896 Euro
- Quantenkommunikation: 3.030.440 Euro
- QuantERA: 540.084 Euro
- Sendate-Programm: 1.394.845 Euro