Deutscher Bundestag **Drucksache 18/10839**

18. Wahlperiode 16.01.2017

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Jan Korte, Frank Tempel, Dr. André Hahn, weiterer Abgeordneter der Fraktion DIE LINKE.
– Drucksache 18/10682 –

Cyber-Sicherheitsstrategie der Bundesregierung

Vorbemerkung der Fragesteller

Am 9. November 2016 hat die Bundesregierung eine Neufassung ihrer Cyber-Sicherheitsstrategie verabschiedet, die nun auch als Bundestagsdrucksache (18/10395) vorliegt. Zugleich wurde der „Bericht zur Lage der IT-Sicherheit in Deutschland 2016“ vorgelegt. Der Bericht listet eine Reihe von Gefährdungen für die Sicherheit und Integrität informationstechnischer Systeme auf, die auf kriminelles und staatliches bzw. geheimdienstliches Handeln zurückgehen.

Die Steigerung der IT-Sicherheit wird als „gemeinsame Verantwortung“ von „Staat, Wirtschaft, Wissenschaft und Gesellschaft“ bezeichnet, hier seien „enge Zusammenarbeit und Koordinierung“ notwendig (Bundestagsdrucksache 18/10395, S. 4). Betont wird der „kooperative Ansatz“ von Staat und Wirtschaft in der IT-Sicherheit. So schlägt die Strategie statt der Einführung verbindlicher und klarer Zulassungsregelungen für neue IT-Produkte die „Einführung eines Gütesiegels für IT-Sicherheit“ vor, an dem sich Firmen und private Nutzerinnen und Nutzer bei ihren Kaufentscheidungen orientieren sollen. Nur verbrämt enthält die Cyber-Sicherheitsstrategie die Aussage, dass solche Zertifizierungen zukünftig durch die IT-Unternehmen selbst entwickelt werden sollen und sie die Zertifizierung am Ende womöglich selbst vornehmen sollen („verstärkte Involvierung und Akkreditierung von Unternehmen sowie deren vertiefte Integration in den Zertifizierungsprozess“, S. 6). Vor allem im Handlungsfeld „Gemeinsamer Auftrag von Staat und Wirtschaft“ wird an vielen Stellen aus Sicht der Fragestellerin offenbar, dass staatlichen Einrichtungen schlicht die Fähigkeiten und Ressourcen fehlen, um die Sicherheit und Integrität informationstechnischer Systeme in der Bundesrepublik Deutschland sichern zu können, also eine klassische staatliche Aufgabe der Gefahrenabwehr erfüllen zu können: Statt klarer Vorgaben sollen bei der Umsetzung des IT-Sicherheitsgesetzes „Mindeststandards und Meldewege gemeinsam mit der Wirtschaft erarbeitet, umgesetzt und fortentwickelt“ werden (S. 8); „zukünftig“ sollen „private IT-Sicherheitsdienstleister im Bedarfsfall stärker als in anderen Bereichen staatlichen Handelns eingebunden“ werden (S. 9); für den Informationsaustausch soll „eine Kooperationsplattform für Staat und Wirtschaft“ institutionalisiert werden (S. 9), statt klare Berichtspflichten der Unternehmen zu jeglichen sicherheitsrelevanten Vorfällen zu schaffen.

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern vom 12. Januar 2017 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

Im Handlungsfeld „Leistungsfähige und nachhaltige gesamtstaatliche Cyber-Sicherheitsarchitektur“ wäre der Ort, um eine Strategie zu beschreiben, mit der sich staatliche Stellen aus der strukturellen Abhängigkeit von privaten IT-Sicherheitsdienstleistern befreien können. Unter vielversprechenden Überschriften wie „Die Fähigkeit zur Analyse und Reaktion vor Ort stärken“ finden sich jedoch ausschließlich Verweise auf bereits gebildete oder noch zu gründende Spezialeinheiten, die lediglich bei besonders schwerwiegenden IT-Sicherheitsvorfällen in die betroffenen Behörden ausrücken. Zur Frage, wie Rechenzentren und andere IT-Struktureinheiten von Bundesbehörden bis zur kommunalen Verwaltung selbst in ihren (sicherheitsrelevanten) IT-Fähigkeiten gestärkt werden können, findet sich hingegen wenig bis nichts. Als einzige Einrichtung, die sich gezielt mit der Vermittlung von Spezialwissen im Bereich der Cyber-Sicherheit befassen und Ausbildungskapazitäten aufbauen soll, wird die Universität der Bundeswehr München benannt (S. 14). Die Bundeswehr soll außerdem ihre „besondere Expertise, Fähigkeiten und Ressourcen“ in Form der Amtshilfe anderen Behörden zur Verfügung stellen – dabei aber wiederum durch Privatunternehmen unterstützt werden (S. 12). Das klingt einerseits nicht schlüssig, andererseits ist zu befürchten, dass die Bundeswehr auch im Inland zum zentralen Akteur der Cyber-Sicherheit wird.

1. Welche Formate der Aus-, Fort- und Weiterbildung für Auszubildende und Beschäftigte der Behörden des Bundes enthalten derzeit welche Elemente mit Bezug zu IT-Sicherheit (bitte nach den jeweiligen Abschlusszertifikaten auflisten)?

Die Antwort zur Frage 1 ist der Anlage 1 zu entnehmen.*

Die Zuordnung der Formate der Ausbildung zu den Ressorts in Anlage 1 richtet sich nach der Eigenschaft als Verordnungsgeber, also der Zuständigkeit für den Erlass der jeweiligen Ausbildungsregelungen.

Die Bundesakademie für öffentliche Verwaltung (BAköV) ist die zentrale ressortübergreifende Fortbildungseinrichtung des Bundes und Qualifizierungsdienstleister für alle Bundesbehörden. Sie gehört organisatorisch zum Bundesministerium des Innern.

Bundesnachrichtendienst (BND)

Die Beantwortung der Frage 1 kann aus Gründen des Staatswohls nicht offen erfolgen. Einzelheiten zu den Aus-, Fort- und Weiterbildungsmaßnahmen sowie den Aufgaben einzelner Dienststellen können in diesem Zusammenhang nicht öffentlich dargestellt werden, da aus ihrem Bekanntwerden sowohl staatliche als auch nichtstaatliche Akteure Rückschlüsse auf Personalentwicklung, die Fähigkeiten und Methoden der Behörde ziehen könnten. Dies kann für die wirksame Erfüllung der gesetzlichen Aufgaben der Nachrichtendienste und damit für die Interessen der Bundesrepublik Deutschland nachteilig sein. Deshalb sind die entsprechenden Informationen als Verschlusssache gemäß der VSA mit dem VS-Grad „VS-Nur für den Dienstgebrauch“ eingestuft. **

* Von der Drucklegung der Anlage 1 wurde abgesehen.
Diese ist als Anlage auf Bundestagsdrucksache 18/10839 auf der Internetseite des Deutschen Bundestages abrufbar.

** Das Bundesministerium des Innern hat die Antwort als „VS – Nur für den Dienstgebrauch“ eingestuft.
Die Antwort ist im Parlamentssekretariat des Deutschen Bundestages hinterlegt und kann dort von Berechtigten eingesehen werden.

Bundesministerium der Justiz und für Verbraucherschutz (BMJV)

Anzumerken ist hinsichtlich der Fort- und Weiterbildungsformate, dass sowohl im BMJV als auch im Geschäftsbereich entsprechende Maßnahmen stattfinden. Die Fort- und Weiterbildung der verantwortlichen Beschäftigten (IT-Sicherheitsbeauftragten) ist laut Umsetzungsplan Bund, der im September 2007 vom Kabinett verabschiedet wurde, verpflichtend umzusetzen. Darüber hinaus ist dort auch die Sensibilisierung der IT-Nutzer und Schulungen von Administratoren gefordert. In allen Gerichten und Behörden im Geschäftsbereich sind entsprechende Prozesse etabliert.

2. Wie viele Beschäftigte von Bundesbehörden haben in den Jahren 2015 und 2016 eine Fortbildung zu Fragen der IT-Sicherheit erhalten (bitte nach Geschäftsbereichen und Träger für beide Jahre getrennt auflisten)?

In die Abfrage wurden die Bundesbehörden (oberste und Behörden des jeweiligen Geschäftsbereichs) einbezogen.

Erfasst wurden fachspezifische Fortbildungen von Beschäftigten, die sich mit IT-Sicherheit beschäftigen. Allgemeine Sensibilisierungsmaßnahmen für alle Beschäftigten wurden nicht erfasst.

Es wurden geschult:

Bundeskanzleramt (BKAmt):

2015: Neun Beschäftigte bei der BAköV,

2016: Zwei Beschäftigte bei der BAköV.

Bundesministerium der Verteidigung (BMVg):

In den Jahren 2015 und 2016: Grundsätzlich werden alle Soldatinnen, Soldaten, Beamtinnen, Beamte, Arbeitnehmerinnen und Arbeitnehmer der Bundeswehr jährlich zum Thema IT-Sicherheit belehrt. Dies erfolgt in der Regel auf der Basis eines Web Based Trainings.

Zusätzlich im Jahr 2016: sieben Beschäftigte von der BAköV.

Auswärtiges Amt (AA):

2015: 49 Beschäftigte, davon elf vom AA, 16 vom Bundesamt für Sicherheit in der Informationstechnik (BSI), fünf von der BAköV und 17 von der Firma Secunet., 2016 96 Beschäftigte, davon 33 vom AA, 21 vom BSI, 13 von der BAköV und 29 von der Firma Secunet.

Die Beauftragte der Bundesregierung für Kultur und Medien (BKM):

2015: 29 Beschäftigte, davon elf von der BAköV und 18 von der Fa. Consectra GmbH,

2016: Drei Beschäftigte, davon einer von der BAköV, einer vom TÜV Saarland und einer von der HiScout GmbH (Cyber Allianz).

Bundesministerium für Bildung und Forschung (BMBF):

2015: Drei Beschäftigte von der BAköV,

2016: Drei Beschäftigte von der BAköV.

Presse- und Informationsamt der Bundesregierung:

2015: 22 Beschäftigte, davon 13 von der BAköV, einer von der Behördenspiegel Gruppe, einer vom PC College, vier von der Fastlane GmbH, einer von der novaCapta Software & Consulting Köln und zwei von der Comparex AG.)

2016: 89 Beschäftigte, davon 14 von der BAköV, drei von der ITACS GmbH (Import Trade Auxiliary Communication System), zwei von Digital Media Konferenz 2016, zwölf von der Vera Software GmbH, zwei vom Beschaffungsamt des Bundesministeriums des Innern (BMI), einer von der Berliner Journalistenschule, einer von explido GmbH, fünf von P&I AG, neun von GFN AG, drei von Fastlane GmbH, 22 von Softed System GmbH, einer von der Cyber Akademie, neun von Materna, vier von der ComConsultant Akademie und einer vom TÜV-Rheinland.

Bundesministerium für Ernährung und Landwirtschaft (BMEL):

2015: 43 Beschäftigte, davon 15 von der BAköV,

2016: 32 Beschäftigte, davon 17 von der BAköV.

Als weitere Träger wurden genannt:

– Europäische Akademie für Steuern, Wirtschaft und Recht,

– Genua GmbH,

– DFN e. V (Verein zur Förderung eines Deutschen Forschungsnetzes).

Bundesministerium für Wirtschaft und Energie (BMWi):

2015: gesamt 56, davon 23 von der BAköV, 32 von der Bundesnetzagentur

(BNetzA) und einer von der SySS GmbH;

2016: gesamt 58, davon 23 von der BAköV, 14 von der BNetzA, 14 von der EDC Weiterbildungsacademy GmbH, einer von der DFN e. V., einer von dem Studieninstitut in Bad Münder, einer von Heise, einer vom ProPress Verlag GmbH, einer von der Berufsschule MMBBS (Multi Media Berufsbildende Schulen), einer von SM LAN Software Training und einer von ComConsult.

Bundesministerium für Familie, Senioren, Frauen und Jugend (BMFSFJ):

2015: Ein Beschäftigter von der BAköV;

2016: Drei Beschäftigte von der BAköV.

Bundesnachrichtendienst (BND):

2015: 182 Beschäftigte, davon 121 Teilnehmer interner Lehrgänge, neun von der BAköV und 52 bei externen Trägern;

2016: 130 Beschäftigte davon 73 Teilnehmer interner Lehrgänge, zwei von der BAköV und 55 bei externen Trägern.

Bzgl. der externen Träger kann keine weitergehende Beantwortung erfolgen.

Begründung: Eine weitergehende Beantwortung der Frage kann aus Gründen des Staatswohls nicht erfolgen. Einzelheiten zu den Trägern externer Lehrgänge können in diesem Zusammenhang nicht dargestellt werden, da aus ihrem Bekanntwerden sowohl staatliche als auch nicht staatliche Akteure Rückschlüsse auf Personalentwicklung, die Fähigkeiten und Methoden oder ggf. Mitarbeiternamen der Behörde ziehen könnten. Dies kann für die wirksame Erfüllung der gesetzlichen Aufgaben der Nachrichtendienste, für den Mitarbeiterschutz und damit für die Interessen der Bundesrepublik Deutschland nachteilig sein.

Bundesministerium für Verkehr und digitale Infrastruktur (BMVI):

2015: 345, davon 38 von der BAköV, 15 von der ML Consulting, einer von der HM Training Solution, vier von der ExperTeach GmbH, 34 von der Secunet Security Networks GmbH, zwölf von der New Elements GmbH, einer vom Euroforum, zwei von Oracle, einer von der TÜV Süd Akademie, einer von der Bechtle GmbH & Co KG, sieben vom BSI, zwei vom Behördenspiegel, einer von der Cyber Akademy GmbH, einer von DGI, zwei von der SCN GmbH, einer von der Comparex Akademie, zwei von der Sophos UTM GmbH, zwei von der Soft Ed System GmbH, einer vom Ministerium für Inneres und Kommunales NRW, einer von der Stiftung Caesar, zwei vom TÜV Süd, 39 intern und 175 ohne Angabe.

2016: 539, davon 90 von der BAköV, elf von ML Consulting, zwei von HM Training Solution, einer von der ExperTeach GmbH, einer vom Fraunhofer SIT, einer von der ComConsult Akademie, sechs von der Cyber Akademie GmbH, neun von der Init AG, einer von Thiele, drei von der Comparex Akademie, 26 von der Fa. PMCS, zwei von der Megasoft/Netmon GmbH, 35 von der Secunet Security Networks AG, einer von der TÜV Süd Akademie, einer von der Bechtle GmbH & Co KG, einer von der ComConsult Research GmbH, einer vom Behördenspiegel, einer von der CBT Training & Consulting GmbH, einer von der IDC Central Europe GmbH, 237 vom BSI, zwei von Symantec, zwei vom Hasso Plattner Institut, Potsdam, 71 intern und 33 ohne Angabe.

Bundesministerium für Gesundheit (BMG):

2015: Zehn Beschäftigte, davon sieben von der BAköV, einer von HM Training Solutions, einer von der hauseigenen Entwicklung und vom einer TÜV Rheinland;

2016: 16 Beschäftigte, davon neun von der BAköV, einer von der hauseigenen Entwicklung, zwei von Symantec und vier von der GFU Cyrus AG Köln.

BMJV:

2015: Zwei Beschäftigte von der BAköV;

2016: Drei Beschäftigte von der BAköV.

Bundesministerium für Arbeit und Soziales (BMAS):

2015: 70 Beschäftigte davon sechs von der BAköV und 64 von privaten Trägern.

2016: 110 Beschäftigte davon fünf von der BAköV und 105 von privaten Trägern.

Die Veranstaltungen der privaten Träger wurden überwiegend über die Firma Consectra GmbH und secunet Security Networks AG realisiert.

Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit (BMUB):

2015: neun Beschäftigte, davon sechs von der BAköV, einer von Heise und zwei vom Behörden Spiegel;

2016: sieben Beschäftigte von der BAköV.

Bundesministerium der Finanzen (BMF):

2015: 267 Beschäftigte, davon 53 BAköV und 214 Bildungs- und Wissenschaftszentrum der Bundesfinanzverwaltung (BFV);

2016: 314, davon 75 BAköV und 239 Bildungs- und Wissenschaftszentrum der BFV.

Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung (BMZ):

2015: Drei Beschäftigte, davon drei von der BAköV und davon einer von FastLane und Genua;

2016: Vier Beschäftigte, davon 4 BAköV und davon einer von FastLane.

Bundesministerium des Innern (BMI):

2015: 367 Beschäftigte, davon 78 Beschäftigte von der BAköV und 289 von externen Trägern (eine Aufschlüsselung nach den jeweiligen externen Schulungsträgern ist aufgrund der Vielzahl der beauftragten Schulungsträger nicht darstellbar).

2016: 483 Beschäftigte, davon 69 von der BAköV und 414 von externen Trägern (eine Aufschlüsselung nach den jeweiligen externen Schulungsträgern ist aufgrund der Vielzahl der beauftragten Schulungsträger nicht darstellbar).

3. Was ist unter einem „möglichst breite(n) Zugang zum neuen Studiengang ‚Cyber-Sicherheit' an der Universität der Bundeswehr in München" (Bundestagsdrucksache 18/10395, S. 14) genau zu verstehen?

   a) Für welche Behörden soll dieser Studiengang geöffnet werden?

Der universitäre Master-Studiengang Cybersicherheit richtet sich im Kern an Offiziere und zivile Angehörige der Bundeswehr, die über einen einschlägigen Bachelor-Abschluss oder einen gleichwertigen Abschluss verfügen. Daneben soll auch im Rahmen freier Kapazitäten Angehörigen anderer Bundesressorts und Bundesbehörden mit derselben Qualifikation der Zugang zum Studium an der Universität der Bundeswehr München (UniBw M) eröffnet werden.

   b) Mit welchen Immatrikulationszahlen rechnet die Bundesregierung aufgrund entsprechender Bedarfsanmeldungen aus dem Geschäftsbereich des Bundesministeriums der Verteidigung?

Der prognostizierte Bedarf liegt bei etwa 70 Absolventinnen und Absolventen pro Jahr.

c) Für wie viele Studentinnen und Studenten insgesamt soll der geplante Studiengang offen stehen?

Die derzeitigen Planungen gehen von einem Master-Studiengang mit insgesamt maximal 120 Studierenden pro Jahr aus.

d) Wie weit ist die Konzeption dieses Studiengangs fortgeschritten, und was werden wesentliche Lerninhalte sein?

Derzeit erfolgt die Erarbeitung des Curriculums, der Modulhandbücher und der Fachprüfungsordnung (FPO) für den neuen Master-Studiengang Cyber-Sicherheit. Ziel ist es, bis Oktober 2017 die staatliche Anerkennung des neuen Studiengangs und die Genehmigung der FPO zu erhalten. Die Akkreditierung des neuen Studiengangs soll bis Mai 2019 erfolgen.

Inhalte des Studiengangs:

Der neue Master-Studiengang Cyber-Sicherheit hat einen Umfang von 120 Leistungspunkten European Credit Transfer System (ECTS), die sich wie folgt aufteilen:

- Pflichtmodule: 57
- Wahlpflichtmodule: frei wählbar im Umfang von mind. 23
- MINT[1]-Seminar: Fünf
- Studium plus-Anteile (Anteile aus dem verpflichtenden Studium generale): Fünf
- Masterarbeit.

Mit dem großen Pflichtanteil soll gewährleistet werden, dass alle Absolventinnen und Absolventen des Master-Studiengangs Cyber-Sicherheit über ein breites Wissen in allen wichtigen Teilgebieten dieses Themas verfügen.

e) Sollen innerhalb des Studiengangs auch diejenigen Lerninhalte, die der Aneignung offensiver Fähigkeiten in der Cyber-Abwehr dienen, den zivilen Absolventinnen und Absolventen offen stehen?

Es ist nicht geplant, innerhalb des Master-Studiengangs Cyber-Sicherheit offensive Fähigkeiten zu vermitteln. Daher werden alle Lerninhalte sowohl den militärischen als auch den zivilen Studierenden zur Verfügung stehen.

4. Was ist konkret unter dem Begriff „Cyber-Cluster“ (S. 14) zu verstehen (institutionell, räumlich, zeitlich, Zweck und Arbeitsgegenstand), und wie sollen diese „Cyber-Cluster“ konkret zur Gewinnung von IT-Fachkräften für die öffentliche Verwaltung nutzbar gemacht werden?

Die Etablierung eines Cyber-Clusters soll den Austausch und die Zusammenarbeit mit (Sicherheits-)Behörden des Bundes und der Länder, den Ressorts, der Industrie, den Wissenschaftseinrichtungen und weiteren gesellschaftlichen Institutionen sicherstellen (z. B. über die Durchführung von Tagungen, Foren, Kooperationen oder mit Dienstleistungen für andere Institutionen). Der essentielle Aus-

[1] zusammenfassende Bezeichnung von Unterrichts- und Studienfächern beziehungsweise Berufen aus den Bereichen Mathematik, Informatik, Naturwissenschaft und Technik.

bau der Forschung zum Thema Cyber-Sicherheit an der UniBw M (elf neue Professuren, neue Mitarbeiter und Labore) innerhalb des Cyber-Clusters fördert vor allem die Grundlagenforschung und dient als Basis für die universitäre Ausbildung von in den einschlägigen Ressorts dringend benötigten Fachkräften für Cyber-Sicherheit sowie für die anwendungsbezogene Entwicklung von innovativen und gesellschaftlich relevanten (Sicherheits-)Technologien und Produkten.

5. Gibt es über die Idee, „die Arbeitgeberattraktivität des Öffentlichen Dienstes offensiver darzustellen“, hinaus noch Ideen, wie die Attraktivität des öffentlichen Dienstes gerade für IT-Fachkräfte gezielt gesteigert werden kann?

Der monetäre Anreiz ist nicht der alleinige, aber ein wichtiger Faktor bei der Gewinnung von IT-Fachkräften. Ein zweiter, zunehmend wichtiger Faktor ist das Arbeitsumfeld des öffentlichen Dienstes: Geregelte Arbeitszeiten sowie langfristige Perspektiven und Einkommenssicherheit haben bei Bewerbern einen hohen Stellenwert. Gerade bei IT-Kräften ist die bei entsprechender Aufgabenwahrnehmung bestehende Verbeamtungsmöglichkeit ein geeignetes Mittel, um Fachkräfte zu gewinnen und langfristig zu halten.

Eine abwechslungsreiche und fordernde Aufgabe wirkt für Bewerber ebenfalls attraktiv. Wenn möglich sollte die Arbeitszeit noch flexibler werden, um die Vereinbarkeit von Familie und Beruf weiter zu stärken.

Zudem hat der IT-Planungsrat den Leitfaden „IT-Personal für die öffentliche Verwaltung gewinnen, binden und entwickeln“ erarbeitet. Dieser enthält ressortübergreifende Empfehlungen für die Verwaltungen von Bund, Ländern und Kommunen, wie IT-Personal für die öffentliche Verwaltung gewonnen, an sie gebunden und weiter entwickelt werden kann.

Beispielhaft sei hier die Bundeswehr erwähnt. Die Bundeswehr steht auf dem Arbeitsmarkt mit allen Behörden des Öffentlichen Dienstes im Wettbewerb um die besten Köpfe, gerade im Bereich der Fachkräfte, so auch im Bereich der IT-Spezialisten. Über die sogenannte Attraktivitätsoffensive hat Frau Bundesministerin der Verteidigung, Dr. Ursula von der Leyen, seit dem Jahr 2014 einen deutlichen Fokus auf den Attraktivitätsgedanken des „Arbeitgebers Bundeswehr“ gelegt. In diesem Zusammenhang sind mit dem im Mai 2015 verabschiedeten Artikelgesetz gesetzliche und über die „Agenda Attraktivität – Aktiv. Attraktiv. Anders.“ eine Reihe von untergesetzlichen Maßnahmen ergriffen worden, um die Attraktivität des Arbeitgebers Bundeswehr in Gänze zu stärken. Ergänzt werden diese Überlegungen durch das Strategieprogramm 2025 zur Personalstrategie der Bundeswehr, das mittelbar u. a. durch die Betrachtung von flexiblen Karrieremodellen auch auf die speziellen Herausforderungen im Bereich Cyber/IT reflektiert. Im Zuge des Aufbaus des neuen Organisationsbereichs „Cyber und Informationsraum“ zum 1. April 2017 sind insbesondere IT-Fachkräfte von großer Bedeutung. Im Zuge dessen wird, ergänzend zu den generellen Überlegungen, untersucht, welche Maßnahmen geeignet sind, dieses wenige Personal für eine Tätigkeit in der Bundeswehr zu gewinnen und in der Folge auch zu halten. Unterstützt werden diese Aktivitäten durch gezielte Werbemaßnahmen des Beauftragten für die Arbeitgebermarke der Bundeswehr (z. B. +Digitale Kräfte+ in 2016). Die Bundeswehr stellt sich somit den Herausforderungen, die durch die vielfältigen Rahmenbedingungen den angesprochenen „war for talents“ speziell für der Öffentlichen Dienst so brisant gestalten.

6. Entspricht es der Tatsache, dass es keine Möglichkeit der Eingruppierung für Absolventinnen und Absolventen mit einem abgeschlossenen Informatikstudium in eine Beamtenlaufbahn gibt?

   Wenn ja, wie soll eine Abhilfe geschaffen werden?

Durch die Dienstrechtsreform 2009 wurde das System der bis dahin bestehenden Laufbahnen grundlegend bereinigt und spezielle Fachrichtungslaufbahnen wurden abgeschafft, um einen flexiblen Personaleinsatz zu ermöglichen. Gemäß § 6 Absatz 2 Bundeslaufbahnverordnung bestehen beim Bund nur noch neun Laufbahnen, in die alle Abschlüsse eingeordnet werden können. Dies gilt auch für IT-Abschlüsse. Absolventinnen und Absolventen mit einem abgeschlossenen Informatikstudium können – bei Vorliegen der übrigen Voraussetzungen – in einer Laufbahn des Bundes verbeamtet werden.

7. Was ist konkret gemeint, wenn in der Cyber-Sicherheitsstrategie von der Durchführung von „Netzwerkoperationen“ (S. 11) durch staatliche Stellen die Rede ist?

Im Falle schwerwiegender Cyber-Angriffe, gegen die mit den klassischen präventiven Maßnahmen (z. B. Firewall, Virenschutz, usw.) in der notwendigen Zeit nicht nachhaltig vorgegangen werden kann, ist zu prüfen, unter welchen rechtlichen, einschließlich völkerrechtlichen, Rahmenbedingungen und mit welchen technischen Möglichkeiten Netzwerkoperationen durch staatliche Stellen durchgeführt werden könnten, solche Cyber-Angriffe abzuwehren bzw. rechtzeitig zu unterbinden. Dabei meint „Netzwerkoperationen“ insbesondere auch aktive technische Maßnahmen und Handlungen, die im Einzelfall geeignet, erforderlich und verhältnismäßig sein sollen.

8. Was sind in diesem Zusammenhang die von der Bundesregierung oder nachgeordneten Stellen zugrunde gelegten Szenarien von „schwerwiegenden Cyber-Angriffen“?

In diesem Zusammenhang sind mit „schwerwiegend“ solche Szenarien gemeint, bei denen die Wirkung des Cyber-Angriffs ein erhebliches Ausmaß erreicht (zum Beispiel, wenn sehr viele Bürgerinnen und Bürger in Deutschland negativ betroffen werden oder wenn die angegriffenen Schutzgüter und Institutionen besonders wichtige sind oder etwa das Ausmaß der wirtschaftlichen Schäden besonders hoch liegt). Dies können insbesondere auch Cyber-Angriffe sein, die zum Ziel haben, großflächige Ausfälle oder Störungen in den Kritischen Infrastrukturen in Deutschland hervorzurufen.

Insgesamt ist die Frage, in welchen Szenarien entsprechende Gegenmaßnahmen erfolgen könnten, Gegenstand laufender Prüfungen (siehe Antwort zu Frage 7).

9. Was meint die Bundesregierung konkret mit der besonderen „Expertise, Fähigkeiten und Ressourcen“, die die Bundeswehr „in Form der Amtshilfe (…) auch anderen staatlichen Akteuren nutzbar“ (S. 12) machen könnte?

Die Bundeswehr ist wie alle Behörden des Bundes und der Länder gemäß Artikel 35 Absatz 1 des Grundgesetzes (GG) zur gegenseitigen Amtshilfe verpflichtet. Dabei kommt insbesondere eine technisch-logistische oder personelle Unterstützung in Betracht. Ausgeschlossen ist im Rahmen von Amtshilfe der Einsatz der Streitkräfte als Organ der vollziehenden Gewalt unter Androhung oder Anwendung hoheitlichen Zwangs. Die ersuchende Behörde entscheidet, welche Unterstützungsleistungen im Rahmen der Amtshilfe angefordert werden.

Die Ausrichtung der Cybersicherheitsstrategie folgt einem ressortgemeinsamen und gesamtstaatlichen Lösungsansatz unter Führung des BMI. Die Bundeswehr wird sich hier mit ihren Fähigkeiten lageabhängig einbringen.

10. Soll die Bundeswehr auch in solchen Amtshilfevorgängen auf Leistungen ziviler Unternehmen zurückgreifen, und wenn ja, wozu ist dann noch das Amtshilfekonstrukt notwendig?

Amtshilfe findet ausschließlich zwischen Behörden statt. Ein Rückgriff auf Leistungen ziviler Unternehmen wäre vertraglich zwischen dem Unternehmen und der Behörde, die die Leistungen in Anspruch nimmt, zu regeln. Die Zusammenarbeit mit der Bundeswehr Informationstechnik GmbH BWI (seit 28. Dezember 2016 Inhousegesellschaft des BMVg) bleibt hiervon unberührt.

11. Wie weit ist der Aufbau einer „Cyber-Reserve“ bei der Bundeswehr bereits vorangeschritten?

a) Wie ist sie in die Aufbauorganisation der Bundeswehr eingegliedert?

Als Grundlage für den Aufbau der „Cyber-Reserve“ wurde im BMVg ein Konzept für die personelle Unterstützung der Cyber-Community der Bundeswehr erarbeitet. Der abgestimmte Entwurf befindet sich derzeit im Billigungsgang.

Die Aufstellung des Kommandos Cyber- und Informationsraum befindet sich in Vorbereitung. Im Rahmen dieser Vorbereitungen werden auch die Dienstposten für Reservisten und deren Anforderungsprofile ausgeplant, so dass erst nach erfolgter Ausplanung Umfangszahlen benannt werden können.

Festzuhalten bleibt, dass bereits Reservisten und Ungediente für eine Mitarbeit in der Cyber-Reserve ihr Interesse anzeigen. Diese Interessenten haben ihren Ansprechpartner im Referat Reservistenangelegenheiten, so dass sichergestellt ist, dass dieses Reservoir aus Spezialisten aus der freien Wirtschaft nicht in der Planungsphase verloren geht. Sie werden per Newsletter regelmäßig über den Fortgang der Planung informiert.

b) Wie viele Reservisten sind für diese Cyber-Reserve gemeldet und mit welchen Vorläufen einziehbar?

Die Besetzung des neuen Bereiches erfolgt im Schwerpunkt zunächst durch „Bestandspersonal“. Aufgrund des querschnittlichen Bedarfes aller Organisationsbereiche auch an IT-Spezialisten und der noch bevorstehenden Aufstellung CIR im April 2017, ist aktuell eine konkrete Zuordnung von externen Einstellungen zum künftigen Cyber-Bereich nicht möglich.

Für die Cyber-Reserve gelten keine gesonderten Regelungen in Bezug auf Einberufung. Es gelten somit die allgemeinen Regelungen für alle Reservistinnen und Reservisten.

c) Was sind die rechtlichen Voraussetzungen zum Einsatz einer solchen Reservisteneinheit?

Auf die Antwort zu Frage 11b wird verwiesen.

d) Gibt es bereits konkretere Überlegungen zum Aufbau ziviler ehrenamtlicher Strukturen in Anlehnung an eine solche „Cyber-Reserve“, beispielsweise hinsichtlich der organisatorischen Anknüpfung an eine Behörde oder Organisation mit Sicherheitsaufgaben, der Mitgliedergewinnung etc.?

Nein.

12. Wie erklärt die Bundesregierung das völlige Fehlen – sowohl in der Sicherheitsstrategie als auch im Bericht zur IT-Sicherheitslage – einer Betrachtung der zunehmenden Angreifbarkeit von Computersystemen zum Überwachen und Steuern technischer Prozesse (Supervisory Control and Data Acquisition, SCADA), die nicht Teil Kritischer Infrastrukturen im Regelungsbereich des IT-Sicherheitsgesetzes sind, aber dennoch weitgehende Auswirkungen auf das zivile Leben haben können (bspw. Verkehrsleittechnik, Gebäudeleittechnik)?

Die Cybersicherheitsstrategie enthält zahlreiche Maßnahmen zur Sensibilisierung und Unterstützung der deutschen Wirtschaft in Fragen der Cyber-Sicherheit. Zudem wird die Ausweitung der Präventions- und Reaktionspflichten, die mit dem IT-Sicherheitsgesetz für die Betreiber Kritischer Infrastrukturen eingeführt wurden, auch andere Unternehmen, die von hoher gesellschaftlicher Relevanz sind, geprüft.

13. Welche Behörden des Bundes befassen sich derzeit schwerpunktmäßig mit dem Schutz insbesondere webbasierter SCADA, sieht die Bundesregierung hierfür in naher Zukunft Bedarf an zusätzlichen Ressourcen (Personal, Analysetools etc.), und wenn ja, bei welcher Behörde?

Das BSI befasst sich im Rahmen der Cyber-Sicherheit für die Industrie unter anderem auch mit webbasierter SCADA. Die webbasierten Systeme stellen dabei nur einen Teil der gesamten industriellen Automatisierungstechnik dar.

Inwieweit die Fortentwicklung zur Industrie 4.0, die zunehmenden Vernetzung der Industrie und die steigenden Zertifizierungen von Produkten in diesem Bereich zu einem zusätzlichen Ressourcenbedarf führen, bleibt abzuwarten. Dieser würde sich vor allem durch mögliche Unterstützungen bei Sicherheitsvorfällen und der Erarbeitung von Empfehlungen für Präventivmaßnahmen niederschlagen.

14. Welche Behörden des Bundes einschließlich der Nachrichtendienste erstellen Lagebilder über die Bedrohungslage im Netz, und worin unterscheiden sich diese Lagebilder sowohl untereinander als auch von dem im Nationalen Cyber-Abwehrzentrum erstellten Lagebild?

Die am Cyber-AZ beteiligten Behörden BSI, Bundesamt für Verfassungsschutz (BfV), Bundeskriminalamt (BKA), BND, Bundespolizei (Bpol), Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw), BITS, Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), Militärischer Abschirmdienst (MAD) und Zollkriminalamt (ZKA) tauschen sich im dortigen Rahmen über die Ihnen vorliegenden Erkenntnisse und Informationen zu tagesaktuellen Sachverhalten aus. Auf dieser Basis wird werktäglich die gemeinsame „Cyber-Lage“ des Cyber-AZ erstellt und an die beteiligten Behörden, deren Fachaufsichten, den Nationalen Cyber-Sicherheitsrat und weitere Behörden versendet.

Darüber hinaus werden durch die Behörden folgende spezifische Lagebilder erstellt:

Das aktuelle Lagebild zur IT-Sicherheit wird im Nationalen IT-Lagezentrum des BSI erstellt. Das BSI veröffentlicht darüber hinaus jährlich den Bericht „Lage der IT-Sicherheit in Deutschland“.

Der BND erstellt Lagebilder, die Bedrohungen aus dem Ausland gegen die Bundesrepublik Deutschland wiedergeben.

Das BKA erstellt das Bundeslagebild Cybercrime im jährlichen Turnus. Beim Cybercrime-Lagebild des BKA liegt der Fokus in der strafrechtlichen Betrachtung des Phänomens. Hier werden Daten aus dem polizeilichen Hellfeld (PKS) sowie aus einschlägigen Studien und Untersuchungen anderer Stellen berücksichtigt. Zudem werden phänomenologische Darstellungen vorgenommen und Lagetrends beschrieben.

Das BfV besitzt die Zuständigkeit für die Aufklärung und Abwehr von Cyberangriffen durch Extremisten, Terroristen und fremde Nachrichtendienste, die auf natürliche und juristische Personen im Inland sowie deutsche diplomatische Vertretungen und deren Mitarbeiter im Ausland verübt werden. Dazu erstellt das BfV entsprechende auf diesen Auftrag abgestimmte Lagebilder. Lagebilderkenntnisse des BfV fließen in die Lagebilder des Cyber-Abwehrzentrums mit ein, soweit der Zuständigkeitsbereich des BfV betroffen ist.

Die Cyber-Sicherheitslage der Bundeswehr wird durch das Computer Emergency Response Team der Bundeswehr (CERTBw) geführt. Es unterscheidet sich von Lagebildern anderer Behörden dadurch, dass es lediglich die spezifischen Belange des IT-Systems der Bundeswehr umfasst.

15. Erstellt das Bundesamt für Verfassungsschutz (BfV) oder eine andere Behörde des Bundes bereits jetzt einen Spionageabwehrbericht, und enthält dieser einen Berichtsteil zur Cyber-Spionage bzw. Cyber-Sicherheit?

    Wenn ja, in welchem Turnus wird der Bericht erstellt, und welchen Gremien des Deutschen Bundestages wird dieser vorgelegt?

Erkenntnisse der Cyber-Abwehr veröffentlicht das BfV regelmäßig als eigenes Kapitel im jährlich vom BMI herausgegebenen Verfassungsschutzbericht.

Der BND erstellt Berichte, die auf das Thema Cyber-Spionage eingehen. Für diese gibt es keinen festgelegten Turnus.

Daneben erscheint einmal im Quartal die mit dem BfV, BSI und BKA gemeinsam erstellte „Sonderausgabe“ Cyber-Sicherheit.

16. Wie lassen sich die Aufgaben zwischen Bundesamt für Sicherheit in der Informationstechnik (BSI) und BfV im Rahmen der Cyber-Sicherheit genau abgrenzen, und welche Änderungen sind diesbezüglich ggf. vorgesehen?

Gemäß § 1 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) ist das BSI zuständig für die Informationssicherheit auf nationaler Ebene.

Seine Aufgaben werden insbesondere definiert durch:

- § 3 BSIG, nach dem das BSI u. a. für die Abwehr von Gefahren für die IT des Bundes, für die Zertifizierung, für die Entwicklung und Konzeption von Prüfungs- und Bewertungskriterien/-verfahren zuständig ist,
- § 4 BSIG als zentrale Meldestelle für die Sicherheit in der IT des Bundes,
- § 5 BSIG, nach dem Protokolldaten und Daten, die an den Schnittstellen der Kommunikationstechnik des Bundes anfallen, automatisiert auswerten dürfen,
- § 7 BSIG, nach dem das BSI Warnungen an die Öffentlichkeit und Betroffene richten darf,
- § 7a BSIG, nach dem das BSI informationstechnische Produkte und Systeme untersuchen darf und
- §8b BSIG, nach dem BSI die zentrale Meldestelle für Kritische Infrastrukturen in Angelegenheiten der IT-Sicherheit ist.

Das BfV hingegen hat im Rahmen des § 3 des Gesetzes über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz (BVerfSchG) die Aufgabe der Beobachtung und Aufklärung nachrichtendienstlicher, extremistischer und terroristischer Cyberaktivitäten. Das bietet bei der Erarbeitung von Gefährdungsprognosen einen über die rein technische Betrachtung hinausgehenden und damit umfassenderen Blickwinkel.

Die gesetzlichen Aufgaben von Behörden unterliegen einer ständigen Evaluierung und werden regelmäßig der sich verändernden Anforderungslage angepasst.

17. Wie sollen die eigenen „Bewertungs- und Auswertungsfähigkeiten“ (S. 10) des Cyber-Abwehrzentrums (Cyber-AZ) geschaffen werden, und wie viele Mittel stehen im Haushalt 2017 hierzu bereit (bitte nach Personal- und Sachmitteln getrennt angeben)?

Die Schaffung von eigenen „Bewertungs- und Auswertungsfähigkeiten“ ist Gegenstand des derzeit laufenden Weiterentwicklungsprozesses zum Cyber-AZ. Da dieser noch andauert, kann zum jetzigen Zeitpunkt keine Aussage zur weiteren inhaltlichen Ausgestaltung getroffen werden.

18. Was wird sich infolge der Cyber-Sicherheitsstrategie in der Zusammenarbeit von Cyber-AZ und Bundeswehr ändern?

Das Cyber-AZ soll unter Federführung des Bundesministeriums des Innern zu einer Institution weiterentwickelt werden, die ressortgemeinsam handelt, erforderliche Aktivitäten koordiniert und das IT-Krisenmanagement für Deutschland übernimmt. Die Bundeswehr ist unmittelbar im Cyber-AZ vertreten. Die konkrete Einbindung der Bundeswehr in die künftigen Prozesse und Verfahren des Cyber-AZ wird im Rahmen des Weiterentwicklungsprozesses definiert.

19. Hat die Bundesregierung geprüft, inwieweit es sinnvoll ist, die Früherkennung von Bedrohungen aus dem Cyber-Raum bei einer Behörde zu bündeln, wenn nein, warum nicht, und wenn ja, mit welchem Ergebnis?

Cybersicherheit kann nur im gesamtstaatlichen Handeln ressortübergreifend erzielt werden. Daher tauschen sich alle Bundesbehörden, die im Rahmen ihrer jeweiligen gesetzlichen Aufgaben für die verschiedenen Bereiche der IT-Sicherheit

zuständig sind, regelmäßig über die Bedrohungslage aus und koordinieren ihre jeweiligen Maßnahmen über das Cyber-AZ.

Die Bündelung aller dieser Aufgaben bei einer Behörde ist hierbei nicht zielführend, da die verfassungsgemäßen Aufgaben der einzelnen Ressorts, besonders deutlich am Beispiel des BMVg, eine Spezialisierung im jeweiligen Bereich erfordern.

20. Sind die Darstellungen der Bundesregierung zur Vorgehensweise des Bundesnachrichtendienstes (BND) zum Signals Intelligence Support to Cyber Defense und zur Erstellung aktueller Lagebilder dahingehend zu verstehen, dass der BND dabei auf private Unternehmen oder Honorarkräfte zurückgreift, und welche Maßnahmen sind geplant, um hierfür ausreichend eigene personelle Ressourcen aufzubauen?

Der BND greift zur Erstellung von Lagebildern weder auf Honorarkräfte noch auf private Unternehmen zurück. Lediglich zur Informationsgewinnung über Cyber-Angriffe und technische Entwicklungen im Bereich IT und Cyber werden im Einzelfall und nach Bedarf externe Dienstleistungen genutzt.

21. Welche Angaben kann die Bundesregierung nach Abschluss der parlamentarischen Beratung des Haushalts 2017 hinsichtlich des Personalbedarfs für die Mobile Incident Response Teams (MIRT) des BSI, der Quick Reaction Forces (QRF) des Bundeskriminalamtes (BKA) und des Cyber-Teams des BfV und der Art der Personalgewinnung machen (Nachfrage zur Antwort der Bundesregierung auf die Kleine Anfrage auf Bundestagsdrucksache 18/9445, Antwort zu Frage 17d)?

Das BSI hat für die Mobile Incident Response Teams (MIRTs) zehn Stellen erhalten. Aktuell sollen diese durch interne Ausschreibung besetzt werden. Anschließend werden die noch offenen Stellen extern ausgeschrieben.

Die Quick Reaction Force im BKA befindet sich seit Juli 2016 im Probewirkbetrieb. Es ist vorgesehen, das Konzept im Juni 2017 zu evaluieren. Erst nach Abschluss des Probewirkbetriebes und Fertigstellung des Evaluationsberichts können Aussagen über mögliche personalwirtschaftliche Konsequenzen getroffen werden.

Das Cyber-Team des BfV wird sich bedarfsorientiert aus dem Personal der Referatsgruppe „Cyberabwehr“ zusammensetzen. Der personelle Aufwuchs für den Bereich Cyberabwehr insgesamt wird durch interne Umsetzungen und Weiterqualifizierung des Personals erfolgen. In der Hauptsache ist jedoch beabsichtigt, Fachkräfte für diesen Bereich über externe Stellenbesetzungsverfahren zu gewinnen. Entsprechende Ausschreibungen für alle Laufbahngruppen (hD, gD und mD) sind bzw. werden in Kürze veröffentlicht. Die gesamte Thematik Cyberabwehr steht im Fokus personalwirtschaftlicher Maßnahmen und wird in der Personalverwaltung entsprechend mit höchster Priorität bearbeitet. Der Bereich Spionage- und Cyberabwehr erfährt dadurch eine deutliche Stärkung.

22. Was ist konkret unter dem „Ausbau datenschutzkonformer Sensorik zur Anomalieerkennung im Netz“ (Bundestagsdrucksache 18/10395, S. 9) zu verstehen, und welche Rolle soll dabei den Providern genau zukommen?

Unter „datenschutzkonformer Sensorik zur Anomalieerkennung“ versteht die Bundesregierung den Einsatz bestimmter technischer Mittel, um Cyberangriffe

im deutschen Internet festzustellen. Dies beinhaltet unter anderem die Detektion von Schadprogrammen oder DDoS-Angriffe (Distributed Denial of Service).

Als technische Mittel sind z. B. Intrusion Detection Systeme und Honeypots denkbar. Der Einsatz dieser Systeme muss so gestaltet sein, dass die berechtigten Datenschutzinteressen der Kunden nicht gefährdet werden.

Die genaue Ausgestaltung der Rolle der Provider kann erst im Rahmen von Gesprächen mit den Providern festgelegt werden.

Ziel ist es, mit Unterstützung der deutschen Internet Provider einen genaueren Überblick über schwerwiegende Angriffe (z. B. DDoS-Angriffe) im Internet zu bekommen. Die Rolle der Provider ist es, die notwendigen technischen Maßnahmen zu implementieren und die generierten Daten anonymisiert bzw. pseudonymisiert zu erfassen, um eine Lagebewertung vorzunehmen.

23. Was genau ist im Unterschied dazu unter einem kontinuierlichen Sicherheits- und Anomaliemonitoring zu verstehen, wie es nach dem Haushaltsplanentwurf des Bundesministeriums des Innern (Einzelplan 06, Schwerpunktepapier zum Regierungsentwurf 2017, S. 195) für technische Monitoring-Fähigkeiten des BSI im Bereich der mobilen Netzwerke vorgesehen ist?

Ziel dieser Maßnahme ist der Schutz der Mobilkommunikation innerhalb der Bundesverwaltung. Daher geht es bei dem Vorhaben zur Etablierung eines kontinuierlichen Sicherheits- und Anomaliemonitoring (Einzelplan 06, Schwerpunktepapier zum Regierungsentwurf 2017, S. 195), um den Schutz zugelassener mobiler Lösungen der Bundesverwaltung. Neben zugelassenen Lösungen werden verstärkt sogenannte Commercial off-the-shelf-Produkte (COTS) bei der Mobilkommunikation innerhalb der Bundesverwaltung eingesetzt. Deshalb müssen die Möglichkeiten des BSI zur Abwehr von Schadprogrammen und Gefahren für die Kommunikationstechnik des Bundes gemäß § 5 BSIG erweitert werden.

24. Warum hat die Bundesregierung die Frage 20 auf Bundestagsdrucksache 18/9334 nach Plänen für einen Ausbau einer „Sensorik im Netz“ mit „Nein“ beantwortet, obwohl die nun verabschiedete Cyber-Sicherheitsstrategie genau eine solche Formulierung enthält?

In der Kleinen Anfrage auf Bundestagsdrucksache 18/9334 wurde nach Plänen gefragt, wonach das BMI zusammen mit Providern die „Sensorik im Netz“ ausbauen will. Entsprechende Pläne gibt es im BMI nicht. In der Cyber-Sicherheitsstrategie 2016 geht es um Maßnahmen der Provider zur Erkennung von Cyber-Bedrohungen. Hierzu (als Maßnahmen der Provider) ist der Ausbau datenschutzkonformer Sensorik im Netz ein wirksames Mittel. Die Zusammenarbeit zwischen Staat und Provider soll sich auf die gemeinsame Nutzung dieser Daten in datenschutzkonformer Art begrenzen.

25. Welche Mittel für Forschung und Entwicklung im Bereich der IT-Sicherheit stehen in diesem und im kommenden Jahr im Bundeshaushalt zur Verfügung?

Im Einzelplan 30, Titel 3004/683 20 „Kommunikationssystem, IT-Sicherheit“ sind im Haushaltsjahr 2016 Mittel in Höhe von 36,0 Mio. Euro und im Haushaltsjahr 2017 Mittel in Höhe von 42,0 Mio. Euro veranschlagt.

Die Höhe der Haushaltsmittel für Forschung und Entwicklung im Bereich der IT-Sicherheit ist für das BSI nicht festgelegt. Forschungs- und Entwicklungsaufträge

werden aus Kapitel 0623, Titel 532 04 (Behördenspezifische fachbezogene Verwaltungsausgaben) gezahlt. Allerdings werden aus diesem Titel auch Studien und andere fachbezogene Dienstleistungen finanziert. Der Titelansatz beträgt:

Titelansatz im Haushalt 2016: 30 535 Euro

Titelansatz im Haushalt 2017: 39 360 Euro.

26. Welche gemeinsamen Forschungsprojekte und -plattformen von Hochschulen, außeruniversitären Forschungseinrichtungen (Industrieforschung) und „anderen Partnern aus der Wirtschaft“ (Bundestagsdrucksache 18/10395, S. 9) bestehen derzeit, in denen neue Produkte und Dienstleistungen im Bereich Cyber-Sicherheit entwickelt werden, und welche Planungen für solche Kooperationen bestehen für die nahe Zukunft?

Die angefragten laufenden Forschungsvorhaben sind in der beigefügten Anlage 2 aufgelistet.*

Ab 2017 sind weitere Projekte auf der Basis der BMBF-Bekanntmachungen „Erkennung und Aufklärung von IT-Sicherheitsvorfällen“, „Hightech für IT-Sicherheit“, „IT-Sicherheit für autonomes Fahren“ und „Privatheit in der digitalen Arbeitswelt“ geplant.

An den beiden Universitäten der Bundeswehr werden in aktuell laufenden Projekten (Forschungsprojekten) mit anderen Hochschulen und außeruniversitären Forschungseinrichtungen keine konkreten Produkte und Dienstleistungen entwickelt, die über den Status als Prototyp hinausgehen. In Hinblick auf die Etablierung des Cyber-Clusters Universität der Bundeswehr München sollen zukünftig (frühestens jedoch erst ab dem Jahr 2018) verschiedene Innovationen/Dienstleistungen und Produkte (aus den Forschungsschwerpunkten) entstehen. Ziel ist es, die Entwicklung derartiger Produkte entlang der gesamten Wertschöpfungskette zu unterstützen.

27. In welchem Umfang werden Mittel für die Forschung im Bereich Cyber-Sicherheit aus dem EU-Forschungsförderprogramm „Horizon 2020“ für Projekte in Deutschland in Anspruch genommen (bitte nach Projektträgern auflisten und jeweils beteiligte Stellen des Bundes benennen)?

Insgesamt wurden bislang aus dem „Horizon 2020“-Programmteil „Digital Security“ 19,8 Mio. Euro an deutsche Projektpartner bewilligt (berücksichtigt sind alle Ausschreibungen 2014/2015/2016 bis Einreichungsfrist 12. April 2016).

Diese 19,8 Mio. Euro verteilen sich auf die Empfängergruppen wie folgt:

- 8,3 Mio. Euro an 18 Partner aus der Privatwirtschaft,
- 5,7 Mio. Euro an 10 Partner aus Forschungsorganisationen,
- 5,1 Mio. Euro an 11 Partner aus Hochschulen und
- 0,7 Mio. Euro an 2 Partner aus Öffentlichen Einrichtungen.

Eine Aufschlüsselung nach Projektträgern und beteiligten Bundesstellen ist nicht möglich, da die Mittel von der Europäischen Kommission direkt bewilligt und an die betroffenen Konsortien über den jeweiligen Projektkoordinator vergeben werden.

* Von der Drucklegung der Anlage 2 wurde abgesehen.
Diese ist als Anlage auf Bundestagsdrucksache 18/10839 auf der Internetseite des Deutschen Bundestages abrufbar.

Anlage 1

Cybersicherheitsstrategie der Bundesregierung

Formate der Ausbildung

Ressort	**Ausbildungsgang/ Laufbahn**	**Bezeichnung des Abschlusses**[2]	**Elemente mit Bezug zur IT-Sicherheit (z. B. Lehrveranstaltung, Unterrichtseinheit)**
Die Beauftragte der Bundesregierung für Kultur und Medien	Gehobener Archivdienst des Bundes	Diplom-Archivar/in (FH) (Laufbahnbefähigung für den gehobenen Archivdienst)	Lehrveranstaltung zur IT-Sicherheit (durch IT-Sicherheitsbeauftragte) während des Praktikums im BArch
Die Beauftragte der Bundesregierung für Kultur und Medien	Höherer Archivdienst des Bundes	Assessor/in des Archivdienstes (Laufbahnbefähigung für den höheren Archivdienst)	Lehrveranstaltung zur IT-Sicherheit (durch IT-Sicherheitsbeauftragte) während des berufspraktischen Studiums im BArch

Formate der Fort- und Weiterbildung[3]
Die Beauftragte der Bundesregierung für Kultur und Medien

Keine

[2] Sofern vorhanden. In der Laufbahnausbildung im mittleren Dienst fehlen entsprechende Abschlussbezeichnungen.
[3] einschl. Fachfortbildung mit IT-Sicherheitselementen

Formate der Ausbildung

Ressort	**Ausbildungsgang/ Laufbahn**	**Bezeichnung des Abschlusses**	**Elemente mit Bezug zur IT-Sicherheit (z. B. Lehrveranstaltung, Unterrichtseinheit)**

Formate der Fort- und Weiterbildung
Presse- und Informationsamt der Bundesregierung

Keine

Formate der Fort- und Weiterbildung

Ressort	**Fortbildungsveranstaltung (Titel)**	**Fortbildungsträger**	**Elemente mit Bezug zur IT-Sicherheit (z. B. Lehrveranstaltung, Unterrichtseinheit)**
BMBF	IT in der Bundesverwaltung	BAköV	• Aktuellste Entwicklungen und Tendenzen bei der Nutzung von IT, Hardware und Software • Diskussion zu IT-Lösungen in den Behörden und Ressorts • Architektur und Standards für die IT in der Bundesverwaltung
BMBF	Jahrestagung für IT-Sicherheitsbeauftragte der Bundesbehörden	BAköV	• IT-Sicherheit in der Bundesverwaltung: neue Entwicklungen und Trends • Nationaler Plan zum Schutz der Informationsinfrastrukturen und dessen Umsetzung
BMBF	IT-Sicherheit in der Bundesverwaltung	BAköV	• Vorstellung neuer Entwicklungen im Bereich der Informationssicherheit
BMBF	Fachtagung IT-Sicherheitsrecht für Behörden	BAköV	• Überblick über den Rechtsrahmen der IT-Sicherheit anhand praxisrelevanter Leitfragen • Rechtsgrundlagen und Rechtsquellen des „IT-Sicherheitsrechts“ • Verantwortlichkeiten für das Management • Verantwortlichkeiten für den IT-Sicherheitsbeauftragten bzw. das IT-Sicherheitsmanagement
BMBF	Verschlüsselung und Elektronische Signatur	BAköV	• Bedingungen und Anforderungen der sicheren und nachvollziehbaren Kommunikationsbeziehungen • Technische Gestaltung einer sicheren Umgebung für den Datenaustausch und die elektronische Kommunikation • Stufen der elektronischen Signatur • Grundlagen kryptischer Verfahren • Infrastrukturen für die sichere Nutzung von Verschlüsselung und Signatur • rechtliche Grundlagen für die sichere Gestaltung von Kommunikation und Datenaustausch • Einsatz von Verschlüsselung und Signatur in der Verwaltung - aktueller Stand • besondere Anwendungen wie z. B. Massensignaturen oder SSL-Serverzertifikate • Einbindung von Verschlüsselungssystemen in den Geschäftsprozess • Basiskomponente: Virtuelle Poststelle (VPS) mit den Funktionen Signatur und Verschlüsselung
BMBF	Workshop-Reihe für IT-Sicherheitsbeauftragte	BAköV	• Mindeststandards für die IT-Sicherheit des Bundes

Formate der Fort- und Weiterbildung

Ressort	**Fortbildungsveranstaltung (Titel)**	**Fortbildungsträger**	**Elemente mit Bezug zur IT-Sicherheit (z. B. Lehrveranstaltung, Unterrichtseinheit)**
BMG	Hardening Microsoft Environments	HM Training Solutions	Schwerpunkte: - Credential Theft & Credential Reuse - Active Directory Absicherung & Monitoring Zertifikat: Teilnahmebescheinigung
BMG	Sensibilisierung zu den Themen IT-Sicherheit und Datenschutz	ML Consulting GmbH (Abruf aus BAköV-Vertrag)	- Die Rolle der IT- Fachkraft in der Informationssicherheit - Der Sicherheitsvorfall (Diskussion anhand eines virtuellen Beispiels) - Informationssicherheit und Datenschutz - Maßnahmen der Grundschutzkataloge - Zertifizierungen Zertifikat: - kein
BMG	Online- IT-Sicherheits-Training	Eigenentwicklung	Modulares Selbststudium zu den Themen - Sicherer Umgang mit E-Mails und E-Mail-Verschlüsselung - Bedrohung durch Computerviren - Passworte und Social Engineering - Surfen im Internet - Umgang mit vertraulichen Informationen (Datenschutz) - Mobile Endgeräte, WLAN und Wechselträgermedien - Verhalten am Arbeitsplatz Teilnehmer: Alle Neueinstellungen inklusive Hospitanten/-innen und Auszubildende

Formate der Ausbildung

Ressort	**Ausbildungsgang/ Laufbahn**	**Bezeichnung des Abschlusses**	**Elemente mit Bezug zur IT-Sicherheit (z. B. Lehrveranstaltung, Unterrichtseinheit)**
BMI	Mittlerer nichttechnischer Dienst in der allgemeinen und inneren Verwaltung des Bundes	-	Fachgebiet „Informationstechnik“: - Datenschutz - Informationssicherheit
BMI	Studiengang Verwaltungsmanagement - Gehobener nichttechnischer Dienst in der allgemeinen und inneren Verwaltung des Bundes	Diplom-Verwaltungswirt/in	Fachgebiet „Grundlagen Datenschutz und Informationssicherheit“: - Datenschutz - Informationssicherheit
BMI	Gehobener -Verwaltungsinformatikdienst des Bundes	Diplom-Verwaltungswirt/in	Modul „Grundlagen der IT-Sicherheit“: - Schadsoftware - Gegenmaßnahmen - Verhaltensweisen Modul „IT-Sicherheit“: - Wesentliche Bedrohungen für die Bundesverwaltung - Kryptographie - Grundfunktionen vertrauenswürdiger Systeme - Einführung in forensische Methoden -Netzwerksicherheit - Digitale Signaturen und Public-Key-Infrastrukturen (PKI) - Management der IT-Sicherheit in der Bundesverwaltung
BMI	Höherer Dienst an wissenschaftlichen Bibliotheken des Bundes	Diplom-Bibliothekar/in	Fachgebiet „Informationstechnik“: - Datenschutz - Informationssicherheit
BMI	Fachangestellte/r für Bäderbetriebe	Fachangestellte/r für Bäderbetriebe	Berufsbildposition „Durchführen von Verwaltungsarbeiten im Bad“: - Datenschutz
BMI	Kaufmann/Kauffrau für Büromanagement	Kaufmann/Kauffrau für Büromanagement	Berufsbildpositionen „Büroprozesse/Informationsmanagement“, „Geschäftsprozesse/Personalbezogene Aufgaben“, „Personalwirtschaft/Personalsachbearbeitung“, „Arbeitsorganisation/Datenschutz und Datensicherheit“: - Datenschutz, Datensicherheit, Datensicherung und Datenpflege

Ressort	Ausbildungsgang/ Laufbahn	Bezeichnung des Abschlusses	Elemente mit Bezug zur IT-Sicherheit (z. B. Lehrveranstaltung, Unterrichtseinheit)
BMI	Verwaltungsfachangestellte/r Fachrichtung Bundesverwaltung	Verwaltungsfachangestellte/r Fachrichtung Bundesverwaltung	Berufsbildposition „Informations- und Kommunikationssysteme“: - Datenschutz, Datensicherheit, Datensicherung und Datenpflege
BMI	Fachangestellte/r für Medien- und Informationsdienste	Fachangestellte/r für Medien- und Informationsdienste	Berufsbildposition „Informations- und Kommunikationssysteme“: - Datenschutz und Datensicherheit
BMI	Geomatiker/in, Vermessungstechniker/in	Geomatiker/in, Vermessungstechniker/in	diverse Berufsbildpositionen: - Datensicherung, Datensicherheit, Datenschutz, und Datenpflege
BMI	Mittlerer Polizeivollzugsdienst in der Bundespolizei	-	PFAD Grundeinweisung APC IT-Systeme BPOL IT-Grundlagenvermittlung pol. Datenverarbeitung, Schulung in Fahndungssystemen
BMI	Gehobener Polizeivollzugsdienst in der Bundespolizei	Diplomverwaltungswirt/in	Grundeinweisung APC IT-Systeme BPOL, IT-Grundlagenvermittlung pol. Datenverarbeitung Schulung in Fahndungssystemen
BMI	Masterstudiengang Öffentliche Verwaltung - Polizeimanagement - Höherer Polizeivollzugsdienst in der Bundespolizei	Master of Arts (M.A.)	Grundeinweisung APC, IT-Systeme BPOL, IT-Grundlagenvermittlung pol. Datenverarbeitung, Schulung in Fahndungssystemen
BMI	Studiengang Kriminalvollzugsdienst im Bundeskriminalamt - Gehobener Kriminaldienst des Bundes	Bachelor of Arts (B.A.)	Modul 10 (Polizeiliche Informationserhebung und -verwendung, Phänomen Cybercrime) vermittelt Grundlagen zum Datenschutz und zur Informationssicherheit.
BMI	Masterstudiengang Öffentliche Verwaltung - Polizeimanagement - Höherer Kriminaldienst des Bundes	Master of Arts (M.A.)	Grundeinweisung APC, IT-Systeme, IT-Grundlagenvermittlung pol. Datenverarbeitung, Schulung in Fahndungssystemen

Formate der Fort- und Weiterbildung

Ressort	**Fortbildungsveranstaltung (Titel)**	**Fortbildungsträger**	**Elemente mit Bezug zur IT-Sicherheit (z. B. Lehrveranstaltung, Unterrichtseinheit)**
BMI	Studiengang Master of Public Administration (MPA)	Hochschule des Bundes für öffentliche Verwaltung	Modul „Allgemeines Verwaltungshandeln – Public Management“: - Umgang mit Daten in der Bundesverwaltung einschließlich europäischer Rahmenbedingungen - Bundesdatenschutzgesetz - Unionsrechtliche Vorgaben Modul „Digitale Verwaltung“: - Kritische Infrastrukturen - Standards und Normen für Informationssicherheit - Organisation der Informationssicherheit - Kosten und Nutzen von Investitionen in Informationssicherheit - Datenschutzrecht
BMI	Fortbildung zur/zum Verwaltungsfachwirt/in	Bundesverwaltungsamt	Prüfungsbereich „Recht des öffentlichen Dienstes/Datenschutz“: - Grundlagen und Bedeutung des Datenschutzes - Datenschutzmaßnahmen und Rechte der Betroffenen
BMI	IT-Sicherheitsbeauftragte in der Bundesverwaltung I – Basis / Zertifikat IT-Sicherheitsbeauftragter I	BAköV	Seminar
BMI	IT-Sicherheitsbeauftragte in der Bundesverwaltung I – Basis Kompakt / Zertifikat IT-Sicherheitsbeauftragter I	BAköV	Seminar
BMI	IT-Sicherheitsbeauftragte in der Bundesverwaltung II - Aufbau	BAköV	Seminar
BMI	IT-Sicherheitsbeauftragte in der Bundesverwaltung III – Expert – Zertifikat IT-Sicherheitsbeauftragter III - Aufbau	BAköV	Studie
BMI	Sensibilisierungskampagne und Schulungen in IT-Sicherheitsfragen	BAköV	Seminar
BMI	Informationstechnik, Informationssicherheit und Internet in der modernen Verwaltung	BAköV	Seminar

Ressort	Fortbildungsveranstaltung (Titel)	Fortbildungsträger	Elemente mit Bezug zur IT-Sicherheit (z. B. Lehrveranstaltung, Unterrichtseinheit)
BMI	Arbeiten mit dem IT-Grundschutztool des BSI	BAköV	Seminar
BMI	Verschlüsselung und elektronische Signatur	BAköV	Seminar
BMI	Materieller und IT-Geheimschutz	BAköV	Seminar
BMI	Grundlagenwissen für Administratoren in der öffentlichen Verwaltung	BAköV	Seminar
BMI	Vertiefung Windows Netzwerke	BAköV	Seminar
BMI	Vertiefung Linux Netzwerke	BAköV	Seminar
BMI	IT-Sicherheitsaspekte in heterogenen Netzwerken	BAköV	Seminar
BMI	Daten- und Informationssicherheit bei Einsatz mobiler Geräte	BAköV	Seminar
BMI	Computer-Forensik in Theorie und Praxis	BAköV	Seminar
BMI	Sensibilisierung und Simulation von Angriff und Verteidigung im Netzwerk	BAköV/BSI	Workshop
BMI	Möglichkeiten der Sensibilisierung im Bereich social engineering	BAköV	Workshop
BMI	Mindeststandards für die IT-Sicherheit des Bundes	BAköV/BSI	Workshop
BMI	Sensibilisierungskampagne „Sicher gewinnt!“ - Informationssicherheit am Arbeitsplatz – Bundes-Informationssicherheits-Schein	BAköV	Seminar/Live Hacking
BMI	Sensibilisierungskampagne „Sicher gewinnt!“ - Elektronische Lernwelt „Informationssicherheit am Arbeitsplatz“ – Bundes-Informationssicherheits-Schein	BAköV	Webbasiertes Training
BMI (BPOL)	Cobit Foundation 5.0 inkl. Abschlusszertifikat nach Prüfung	Serview GmbH	Seminar
BMI (BPOL)	Windows Forensic Analysis	SANS Institute	Seminar

Ressort	**Fortbildungsveranstaltung (Titel)**	**Fortbildungsträger**	**Elemente mit Bezug zur IT-Sicherheit (z. B. Lehrveranstaltung, Unterrichtseinheit)**
BMI (BPOL)	Advanced Digital Computer Forensik	SANS Institute	Seminar
BMI (BPOL)	Sicherheit in IP-Netzen	Experteach GmbH	Seminar
BMI (BPOL)	OTRS Master	Linuxhotel GmbH	Seminar
BMI (BPOL)	Software X-Ways	X Ways Software Technology GmbH	Seminar
BMI (BPOL)	Hacker-Labor für Netzwerkadministratoren	Genua GmbH	Seminar
BMI (BPOL)	Entwicklung sicherer Webanwendungen	Hackattack IT Security GmbH	Seminar
BMI (BPOL)	Heise Security Tour	Heise Medien GmbH	Workshop
BMI (BPOL)	Hacking Methoden in der Praxis	Comparex AG	Seminar
BMI (BPOL)	Mobile Schädlinge	Heise Medien GmbH	Webinar
BMI (BPOL)	Netzwerk- und WLAN-Sicherheit	Cyberakademie GmbH	Seminar
BMI (BPOL)	Wireshark Schulung	Experteach GmbH	Seminar
BMI (BPOL)	Oracle Database Performance Training	Robotron Datenbank-Software GmbH	Seminar
BMI (BPOL)	Sicherheit für Linux Server	New Elements GmbH	Seminar
BMI (BPOL)	Administering Windows Server 2012	Piwinger & Lau EDV Schulungs- und Beratungszentrum GmbH	Seminar
BMI (BPOL)	ItWatch Enterprise Security Suite (itWess)	ITWatch GmbH	Seminar
BMI (BPOL)	Netzwerkanalyse/ Troubleshooting	IT Innovations GmbH	Seminar
BMI (BPOL)	Checkpoint Security Administration	Computacenter AG & Co OHG	Seminar
BMI (BPOL)	Administratorenschulung für SINA-Core	Secunet Security Networks AG	Seminar
BMI (BPOL)	iOS Exploitation Training	Sektion Eins GmbH	Seminar
BMI (BPOL)	TCP/IT Netzwerkgrundlagen	PC College GbR	Seminar

Ressort	Fortbildungsveranstaltung (Titel)	Fortbildungsträger	Elemente mit Bezug zur IT-Sicherheit (z. B. Lehrveranstaltung, Unterrichtseinheit)
BMI (BPOL)	Netzwerktechnik Grundlagen	Computer Systeme Kebel	Seminar
BMI (BPOL)	Smartphone Security and Forensics	National Training POC der Bundeswehr	Seminar
BMI (BPOL)	Hacking Mobile Devices	Hackattack IT Security GmbH	Seminar
BMI (BPOL)	Informationstechnik, Informationssicherheit und Internet in der modernen Verwaltung - Grundlagen und Anwendung	BPOLAK	Lehrgang
BMI (BPOL)	GS-Tool - Arbeiten mit dem Grundschutztool des BSI	BAköV	Lehrgang
BMI (BPOL)	Fortbildungslehrgänge für IT-Systemadministratoren Spezialkenntnisse AD-Disaster-Recovery, IT-Grundversorgung Disaster	BPOLAK	Lehrgang
BMI (BPOL)	Fortbildungslehrgang für Sachbearbeiter IKT (BPOL)	Bundespolizeiakademie (BPOLAK)	Inhalt: - u. a. aktuelle Themen aus dem Bereich IKT-Sicherheit
BMI (BPOL)	Verwendungslehrgang zum IT-Sicherheitsbeauftragten (BPOL)	Bundespolizeiakademie (BPOLAK)	Inhalt: - BSI Tool und BPOL IT-Sicherheitskonzepte
BMI (BPOL)	Fortbildungslehrgang für IT-Sicherheitsbeauftragte (BPOL)	Bundespolizeiakademie (BPOLAK)	Inhalt: - IT-Strukturanalyse - Risiko- und Schwachstellenanalyse - BSI Tool und BPOL IT-Sicherheitskonzepte
BMI (BPOL)	Fortbildungslehrgang für IT-Sicherheitsbeauftragte / IT-Systemadministratoren - Modul Netzsicherheit (BPOL)	Bundespolizeiakademie (BPOLAK)	Inhalt: - Hacker Tools und Techniken - Penetration Testing / Netzwerksicherheit - Risiko- und Schwachstellenanalyse - Schutzmaßnahmen
BMI (BPOL)	Fortbildungslehrgang für IT-Sicherheitsbeauftragte / IT-Systemadministratoren - Modul Forensik (BPOL)	Bundespolizeiakademie (BPOLAK)	Inhalt: - Incident Response / aktuelle Angriffe - Schadsoftware allgemein - Auswertung und Analyse kompromittierter IT-Systeme - Schutzmaßnahmen

Ressort	**Fortbildungsveranstaltung (Titel)**	**Fortbildungsträger**	**Elemente mit Bezug zur IT-Sicherheit (z. B. Lehrveranstaltung, Unterrichtseinheit)**
BMI (BPOL)	Fortbildungslehrgang für IT-Sicherheitsbeauftragte / IT-Systemadministratoren - Modul Viren, Würmer und Trojaner, Disaster Recovery (BPOL)	Bundespolizeiakademie (BPOLAK)	Inhalt: - Analyse und Beseitigung von Schadsoftware - System-Wiederherstellung - Antiviren-Tools
BPOL BMI (BPOL)	Fortbildungslehrgang für Fachpersonal IT-Sicherheit - Spezialkenntnisse Grundschutztool SAVe (BPOL)	Bundespolizeiakademie (BPOLAK)	Inhalt: - Umgang und Praxis SAVe - Grundschutzkataloge BSI - Sicherheitskonzepte
BMI (BPOL)	Verwendungslehrgang zum Bearbeiter IKT und Sachbearbeiter IKT ohne Stabsfunktion - Einweisungslehrgang (BPOL)	Bundespolizeiakademie(BPOLAK)	Inhalt: - u. a. Grundkenntnisse IKT-Sicherheit
BMI (BPOL)	IKST-Syst-IT-SiBe	Bundespolizeipräsidium (BPOLP)	- behördeninterner Workshop mit Bezügen zur IT-Sicherheit
BMI (BPOL)	Verschlüsselung und Elektronische Signatur	Bundesakademie für öffentliche Verwaltung (BAköV)	- Seminar für den Zertifikatserhalt der IT-Sicherheitsbeauftragten
BMI (BPOL)	IT-Sicherheitsaspekte in heterogenen Netzwerken	Bundesakademie für öffentliche Verwaltung (BAköV)	- Seminar für IT-Verantwortliche, IT-Sicherheitsbeauftragte
BMI (BPOL)	IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung	Bundesakademie für öffentliche Verwaltung (BAköV)	- Seminar für Beschäftigte im IT-Sicherheitsmanagement
BMI (BPOL)	Jahrestagung für IT-Sicherheitsbeauftragte der Bundesbehörden	Bundesakademie für öffentliche Verwaltung (BAköV)	- Workshop für den Zertifikatserhalt der IT-Sicherheitsbeauftragten
BMI (BPOL)	Workshopreihe für IT-Sicherheitsbeauftragte	Bundesakademie für öffentliche Verwaltung (BAköV)	- Workshop für IT-Verantwortliche, IT-Sicherheitsbeauftragte
BMI (BPOL)	Workshopreihe „Sichere IT in der Bundesverwaltung“	Bundesakademie für öffentliche Verwaltung (BAköV)	- Workshop für IT-Verantwortliche, IT-Sicherheitsbeauftragte
BMI (BPOL)	Daten- und Informationssicherheit beim Einsatz mobiler Geräte	Bundesakademie für öffentliche Verwaltung (BAköV)	- Seminar für IT-Sicherheitsbeauftragte
BMI (BPOL)	IT-Security Workshop genulab	Genua mbH	- IT-Sicherheitslehrgang bei externem Anbieter
BMI (BPOL)	IT-Sicherheit von mobilen Endgeräten in öffentlichen Institutionen	Europäische Akademie für Steuern, Wirtschaft & Recht	- IT-Sicherheitslehrgang bei externem Anbieter

Formate der Ausbildung

Ressort	**Ausbildungsgang/ Laufbahn**	**Bezeichnung des Abschlusses**	**Elemente mit Bezug zur IT-Sicherheit (z. B. Lehrveranstaltung, Unterrichtseinheit)**
AA	mittlerer, gehobener und höherer Dienst	-	IT-Sicherheit im Rahmen des laufbahnübergreifenden „Zirkeltrainings“

Formate der Fort- und Weiterbildung

Ressort	**Fortbildungsveranstaltung (Titel)**	**Fortbildungsträger**	**Elemente mit Bezug zur IT-Sicherheit (z. B. Lehrveranstaltung, Unterrichtseinheit)**
AA	Sicherheit und Geheimschutz	AA	Lehrveranstaltung (BSI-Vortrag zur Sicherheit bei Nutzung von IT und mobiler Kommunikation) Lehrveranstaltung (Livehacking; Vorführung einer spezialisierten Firma)
AA	Regionalforum für Sicherheitsbeauftragte	AA	Lehrveranstaltung (BfV-Vortrag zu Cyberangriffen)
AA	14. Deutscher IT-Sicherheitskongress des BSI; Teilnahme des Referatsleiters 1-IT-SI	BSI	Dreitägiger Fachkongress zum Thema
AA	Kanzlerseminar (2015/2016)	AA	Vortrag IT-Sicherheit
AA	Einführung für Geheimschutz- und Sabotageschutzbeauftragte und deren Mitarbeiter/innen aus Bundes- und Landesbehörden (2016)	BfV	Vortrag IT-Sicherheit
AA	Seminar Sicherheit und Geheimschutz (2015/2016)	Fa. Life Hacking	Vortrag IT-Sicherheit
AA	Konferenz der Sicherheitsberater (2015/2016)	AA	Vortrag IT-Sicherheit
AA	Diverse IT-Fortbildungsveranstaltungen (2015/2016)	BAköV	Hauptthematisch oder am Rande themenübergreifender IT-Fortbildungen

Formate der Ausbildung

Ressort	**Ausbildungsgang/ Laufbahn**	**Bezeichnung des Abschlusses**	**Elemente mit Bezug zur IT-Sicherheit (z. B. Lehrveranstaltung, Unterrichtseinheit)**
BMVI	Vorbereitungsdienst für den gehobenen Wetterdienst des Bundes	Diplom-Meteorologe (FH) / Diplom-Meteorologin (FH) (Dipl.-Met.(FH))	1. „IT-Sicherheit im DWD“, 2. „Informationsverarbeitung“, Grundstudium Brühl, 3. im Studiengebiet „IT-Anwendungen in der Meteorologie“ (insgesamt 95 UStd.) wird „operationelle IT“ im Hauptstudium unterrichtet zzgl. themenbezogenen Lerninhalten zur IT-Sicherheit.
BMVI	Vorbereitungsdienst für den mittleren Wetterdienst des Bundes	X	1. IT-Sicherheit im DWD, 2. IT-Systeme + Anwendungen, „der IT-Arbeitsplatz“ mit themenbezogenen Lerninhalten zur IT-Sicherheit.

Formate der Fort- und Weiterbildung

Ressort	**Fortbildungsveranstaltung (Titel)**	**Fortbildungsträger**	**Elemente mit Bezug zur IT-Sicherheit (z. B. Lehrveranstaltung, Unterrichtseinheit)**
BMVI	Sichere Nutzung der Internetdienste	DWD	
BMVI	Hausstruktur / Informationssicherheit	BMVI / Wifa	Vermittlung von geltenden Regeln zur Informationssicherheit
BMVI	Verwaltungsfachwirt/Verwaltungsfachwirtin	BMVI	Datenschutz
BMVI	Wasserbaumeister/Wasserbaumeisterin	BMVI	Bestimmungen Datenschutz
BMVI	Geprüfte Vergabefachkraft	BMVI	Datenschutz
BMVI	Seevermessungstechniker/Seevermessungstechnikerin	BMVI	Datensicherheit Keine Stundenvorgabe

Formate der Ausbildung

Ressort	**Ausbildungsgang/ Laufbahn**	**Bezeichnung des Abschlusses**	**Elemente mit Bezug zur IT-Sicherheit (z. B. Lehrveranstaltung, Unterrichtseinheit)**
BMVg	Vorbereitungsdienst höherer technischer Verwaltungsdienst in der Bundeswehrverwaltung – Fachrichtung Wehrtechnik –	Laufbahnbefähigung für den höheren technischen Verwaltungsdienst	Lehrgang „Aufgaben und Organisation der Bundeswehr und Statusfragen“, Lehrgang „Fachtechnische Grundlagen Informationstechnik und Elektronik“
BMVg	Vorbereitungsdienst gehobener nichttechnischer Verwaltungsdienst in der Bundeswehrverwaltung an der Hochschule des Bundes für öffentliche Verwaltung – Fachbereich Bundeswehrverwaltung	Diplomverwaltungswirtin/-wirt (FH), Laufbahnbefähigung für den gehobenen nichttechnischen Verwaltungsdienst	Studienplan – Grundstudium Studiengebiet II. - Verwaltung als wirtschaftliche Institution - Studienfach II.4 – Verwaltungsinformatik
BMVg	Vorbereitungsdienst gehobener technischer Verwaltungsdienst in der Bundeswehrverwaltung – Fachrichtung Wehrtechnik –	Laufbahnbefähigung für den gehobenen technischen Verwaltungsdienst	Lehrgang „Aufgaben und Organisation der Bundeswehr und Statusfragen“, Lehrgang „Fachtechnische Grundlagen einzelner wehrtechnischer Fachgebiete“
BMVg	Vorbereitungsdienst mittlerer technischer Verwaltungsdienst in der Bundeswehrverwaltung – Fachrichtung Wehrtechnik –	Laufbahnbefähigung für den mittleren technischen Verwaltungsdienst	Datenverarbeitungslehrgang und Abschlusslehrgang Fachgebiet „Informationstechnik und Elektronik“
BMVg	Vorbereitungsdienst gehobener Dienst der Fernmelde- und Elektronischen Aufklärung des Bundes	Laufbahnbefähigung für den gehobenen nichttechnischen Verwaltungsdienst	Praxisbezogene Lehrveranstaltung
BMVg	Vorbereitungsdienst mittlerer Dienst der Fernmelde- und Elektronischen Aufklärung des Bundes	Laufbahnbefähigung für den mittleren nichttechnischen Verwaltungsdienst	Grund- und Abschlusslehrgang
BMVg	Offizierslaufbahn (Studium)	Bachelor of Science (Informatik)	Praktikum IT-Sicherheit
BMVg	Offizierslaufbahn (Studium)	Bachelor of Science (Mathematical Engineering)	Wahlpflichtgruppe: IT, Kommunikation und Sicherheit (Praktikum IT-Sicherheit)

Ressort	**Ausbildungsgang/ Laufbahn**	**Bezeichnung des Abschlusses**	**Elemente mit Bezug zur IT-Sicherheit (z. B. Lehrveranstaltung, Unterrichtseinheit)**
BMVg	Offizierslaufbahn (Studium)	Master of Science (Informatik)	Vorlesung Sicherheit in der Informationstechnik + Wahlpflichtmodul - Vertiefung: Cyber Defence und Management
BMVg	Offizierslaufbahn (Studium)	Master of Science (Mathematical Engineering)	Wahlpflichtmodul - Vertiefung: IT-Sicherheit und Kommunikationssysteme
BMVg	Offizierslaufbahn (Studium)	Master of Science (Wirtschaftsinformatik)	Wahlpflichtmodul -Vertiefung: Technologie- und Innovationsmanagement (Vorlesung: Sicherheit in der Informationstechnik)

Formate der Fort- und Weiterbildung

Ressort	**Fortbildungsveranstaltung (Titel)**	**Fortbildungsträger**	**Elemente mit Bezug zur IT-Sicherheit (z. B. Lehrveranstaltung, Unterrichtseinheit)**
BMVg	IT-Sicherheit in der Bundeswehr - Kryptoverwalter Bundeswehr	Führungsunterstützungsschule der Bundeswehr	Verwendungslehrgang
BMVg	IT-Sicherheit in der Bundeswehr -Weiterbildung ITSiBeDSt	Führungsunterstützungsschule der Bundeswehr	Weiterbildungslehrgang
BMVg	IT-Sicherheit in der Bundeswehr - Weiterbildung Kryptoverwalter	Führungsunterstützungsschule der Bundeswehr	Weiterbildungslehrgang
BMVg	IT-Sicherheit in der Bundeswehr - ITSiBe in Einsatz/Übung	Führungsunterstützungsschule der Bundeswehr	Verwendungslehrgang
BMVg	IT-Sicherheit in der Bundeswehr - IT-Sicherheitsgehilfe	Führungsunterstützungsschule der Bundeswehr	Verwendungslehrgang
BMVg	IT-Sicherheit in der Bundeswehr # ITSiBe Proj Teil 2	Bildungszentrum der Bundeswehr	Fortbildung
BMVg	IT-Sicherheit in der Bundeswehr -Deltaschulung Grundschutztool Projekt	Bildungszentrum der Bundeswehr	Fortbildung
BMVg	IT-Sicherheit in der Bundeswehr # ITSiBe Proj Teil 1	Bildungszentrum der Bundeswehr	Fortbildung
BMVg	Cyber Defence NATO CIS Security Officer(INFOSEC Vers. 2.0)(ID NO 280)	NATO Communications And Information Systems School (NCISS), Latina	Verwendungslehrgang
BMVg	Sicherheit in der Informationstechnik (IT-Sicherheit)	Bildungszentrum der Bundeswehr	Fortbildung
BMVg	Weiterbildung S6 Offizier	Führungsunterstützungsschule der Bundeswehr	Fortbildung
BMVg	S6 Feldwebel	Führungsunterstützungsschule der Bundeswehr	Verwendungslehrgang
BMVg	S6 Offizier	Führungsunterstützungsschule der Bundeswehr	Verwendungslehrgang
BMVg	IT-Sicherheit in der Bundeswehr ITSiBe Dienststelle	Führungsunterstützungsschule der Bundeswehr	Verwendungslehrgang
BMVg	IT-Offizier Streitkräfte		Verwendungslehrgang
BMVg	Weiterbildung S6 Feldwebel Einheitsebene	Führungsunterstützungsschule der Bundeswehr	Fortbildung

Formate der Fort- und Weiterbildung

Ressort	**Fortbildungsveranstaltung (Titel)**	**Fortbildungsträger**	**Elemente mit Bezug zur IT-Sicherheit (z. B. Lehrveranstaltung, Unterrichtseinheit)**
BMJV und Geschäftsbereich	Diverse Informationsveranstaltungen, wie z. B. Live-hacking und IT-Sicherheitstag für alle Beschäftigten	BAköV	Sensibilisierung hinsichtlich Thema IT-Sicherheit
	Fortbildungsprogramm zum Erwerb des Zertifikats IT-Sicherheitsbeauftragter der Bundesverwaltung und weitere Fortbildungen zum Erhalt des Zertifikats	BAköV	verpflichtende Fortbildung für IT-Sicherheitsbeauftragte in den Behörden der BV
	Schulungen für Administratoren, in denen Sicherheitsaspekte betrachtet werden		
	IT-Ersteinweisung für neue Beschäftigte, in der Belange der IT-Sicherheit betrachtet und vermittelt werden		Vermittlung von Kenntnissen und Regelungen/Festlegungen des Hauses bzgl. Informationssicherheit
	Bereitstellung der Lernwelt Informationssicherheit am Arbeitsplatz im Intranet		Vermittlung von Kenntnissen bzgl. Informationssicherheit
	Sensibilisierungsveranstaltung für Führungskräfte		

Formate der Ausbildung

Ressort	**Ausbildungsgang/ Laufbahn**	**Bezeichnung des Abschlusses**	**Elemente mit Bezug zur IT-Sicherheit (z. B. Lehrveranstaltung, Unterrichtseinheit)**
BMAS	Verordnung über die Berufsausbildung zum/zur Sozialversicherungsfachangestellten	Sozialversicherungsfachangestellte, Fachrichtung: - allgemeine Krankenversicherung - gesetzliche Unfallversicherung - gesetzliche Rentenversicherung - knappschaftliche Sozialversicherung - landwirtschaftliche Sozialversicherung	• Seminar Datenschutz • Seminar IT-Sicherheit
BMAS	Verordnung über die Berufsausbildung Fachangestellte/r für Arbeitsmarktdienstleistungen	Fachangestellte/r für Arbeitsmarktdienstleistungen	• Seminar Datenschutz • Seminar IT-Sicherheit

Formate der Fort- und Weiterbildung[4]

Ressort	**Fortbildungsveranstaltung (Titel)[5]**	**Fortbildungsträger**	**Elemente mit Bezug zur IT-Sicherheit (z. B. Lehrveranstaltung, Unterrichtseinheit)**
BMF	Informationssicherheit im BMF	BMF	Lehrveranstaltung für das Haus BMF
BMF	Zertifikatslehrgang „IT-Sicherheitsbeauftragte/r“	BITKOM Akademie	Lehrveranstaltung
BMF	Grundschutzmethodik für IT-Fachverfahren	Bildungs- und Wissenschaftszentrum der BFV	
BMF	Informationssicherheit Technik Aufbau	Bildungs- und Wissenschaftszentrum der BFV	
BMF	Informationssicherheit Vertiefung	Bildungs- und Wissenschaftszentrum der BFV	
BMF	IT-Sicherheitsbeauftragte/r (IT-SB) Teil 1	Bildungs- und Wissenschaftszentrum der BFV	
BMF	IT-Sicherheitsbeauftragte/r Teil 2	Bildungs- und Wissenschaftszentrum der BFV	
BMF	Lokaler Ansprechpartner für IS (LAIS)	Bildungs- und Wissenschaftszentrum der BFV	
BMF	Technik für IT-SB / LAIS	Bildungs- und Wissenschaftszentrum der BFV	
BMF	Fragen zur IT-Sicherheit	BAköV	

[4] einschl. Fachfortbildung mit IT-Sicherheitselementen
[5] mit Angabe des Zertifikats, sofern vorhanden

Anlage 2
(Cybersicherheitsstrategie der Bundesregierung)

Thema	Laufzeit	
CISPA: Center for IT-Security, Privacy and Accountability at Saarland University	01.10.2011	31.07.2020
Verbundprojekt: Center for Research in Security and Privacy Darmstadt - **CRISP** - (ehem. European Center for Security and Privacy by Design (EC-SPRIDE)	01.10.2011	30.09.2019
Kompetenzzentrum für angewandte Sicherheitstechnologie (**KASTEL**)	01.10.2011	30.09.2019
Verbundprojekt: Photonische Fehler- und Angriffsanalyse von Sicherheitsstrukturen und Sicherheitsfunktionen - **Photon FX²** -	01.07.2013	31.12.2016
Verbundprojekt: Secure Partitioning of application Logic In a Trustworthy Cloud - **SPLITCloud** -	01.07.2014	31.03.2017
Verbundprojekt: Securing the Financial Cloud - **SFC** -	01.03.2014	30.09.2017
Verbundprojekt: Vertrauenswürdige Cloud-Services durch dynamische Zertifizierung: Next Generation Certification - **NGCert** -	01.10.2014	30.09.2017
Verbundprojekt: Privacy-erhaltende Methoden und Werkzeuge für Cloud-basierte Geschäftsprozesse - **PREsTiGE** -	01.03.2014	28.02.2017
Privatheit im Wandel - **Privacy-Panel** -	01.11.2013	31.10.2017
Verbundprojekt: Untersuchung zur Kartografie und Analyse der Privacy-Arena - **Privacy-Arena** -	01.11.2013	31.12.2016
Verbundprojekt: Forum: Privatheit und selbstbestimmtes Leben in der digitalen Welt - **ForPri** -	01.12.2013	31.03.2017
Verbundprojekt: Forum: Privatheit und selbstbestimmtes Leben in der Digitalen Welt - **Privacy-Forum** -	01.10.2014	31.03.2017
Verbundprojekt: Quanten-Repeater-Plattformen auf der Basis von Halbleitern - **Q.com-Halbleiter** -	01.05.2014	30.04.2017
Verbundprojekt: Informationstheorie des Quanten-Repeaters - **Q.com-Nachrichtentechnik** -	01.05.2014	30.04.2017
Verbundprojekt: Quanten-Repeater-Plattform mit Methoden der Quantenoptik - **Q.com-Quantenoptik** -	01.05.2014	30.04.2017
KMU-innovativ - Verbundprojekt: Kontext- und strukturbasierte Abwehr zielgerichteter Angriffe - **APT-Sweeper** -	01.08.2014	31.07.2017
Verbundprojekt: Systemic Security for Critical Infrastructures - **SURF** -	01.09.2014	31.12.2016
Verbundprojekt: Intelligente Intrusion-Detection-Systeme für Industrienetze - **INDI** -	01.11.2014	31.10.2017
Verbundprojekt: Security Indicators for Critical Infrastructure Analysis - **SICIA** -	01.11.2014	31.10.2017
Verbundprojekt: „Security Management as a Service“ für Betreiber kritischer Infrastrukturen der Verwaltung - **SECMaaS** -	01.04.2015	31.10.2017
Verbundprojekt: Schutz von Verkehrs-, Tunnel- und ÖPNV-Leitzentralen vor Cyber-Angriffen - **Cyber-Safe** -	01.02.2015	31.01.2018
Verbundprojekt: Modellbasierte Sicherheitsanalyse von IKT-basierten Kritischen Infrastrukturen - **MoSaIK** -	01.01.2015	31.12.2017
Verbundprojekt: Framework zum präventiven Krisen- und Risiko-Management für Rechenzentren systemrelevanter Banken - **PREVENT** -	01.01.2015	31.12.2017

Thema	Laufzeit	
Verbundprojekt: Labor für IT-Sicherheit bei Wasserversorgern - **AQUA-IT-Lab** -	01.01.2015	30.06.2017
Verbundprojekt: IT-Security Awareness Penetration Testing - **ITS.APT** -	01.01.2015	31.12.2017
Verbundprojekt: Vernetzte IT-Sicherheit Kritischer Infrastrukturen - **VeSiKi** -	01.01.2015	30.06.2018
KMU-innovativ - Verbundprojekt: Smartcard-basierte Sicherheitsanker für Android - **SmaSA** -	01.04.2015	31.03.2017
Verbundprojekt: Sichere Informationsnetze bei kleinen und mittleren Energieversorgern - **SIDATE** -	01.08.2015	31.07.2018
Verbundprojekt: Risiken industrieller IT: Metriken, Messung, Visualisierung - **RiskViz** -	01.04.2015	31.03.2018
KMU-innovativ - Verbundprojekt: Netzsicherheit in Unternehmen und Behörden basierend auf Software Defined Networking- **SarDiNe** -	01.03.2015	28.02.2018
Sicheres Cloud-Computing: Rechtliche Herausforderungen und Lösungsmöglichkeiten - Wissenschaftliche Begleitforschung zu den Projekten des BMBF	01.04.2015	31.03.2018
Verbundprojekt: Rechtssichere Verifikation elektronischer Identitäten in betreibersicheren Cloud-Systemen - **Verifi-eID** -	01.07.2015	30.06.2017
Verbundprojekt: Nationales Referenzprojekt zur IT-Sicherheit in Industrie 4.0 - **IUNO** -	01.07.2015	30.06.2018
KMU-innovativ - Verbundprojekt: Profilbasierte Anomalieerkennung für SIEM-Systeme - **PA-SIEM** -	01.10.2015	30.09.2017
Modellierung des Privacy Paradoxons aus technischer und psychologischer Sicht - **MoPPa**	01.11.2015	31.10.2017
Verbundprojekt: Selbstdatenschutz durch statische und dynamische Analyse zur Validierung von Android-Apps - **AndProtect** -	01.11.2015	31.10.2017
Verbundprojekt: Transparente Informationen zur individuellen Nutzung von Cloud-Services - **TRINICS** -	01.01.2016	30.06.2018
Verbundprojekt: Vertrauenswürdige Verteilung von Verschlüsselungsschlüsseln - **VVV** -	01.01.2016	31.12.2017
Verbundprojekt: Einfach Nutzbare Ende-Zu-Ende Verschlüsselung von E-Mail zur Alltagskommunikation – **enzevalos** -	01.01.2016	31.12.2017
Verbundprojekt: PeRsOnal MedIcal SafE - **PROMISE_DS** -	01.01.2016	31.12.2018
Verbundprojekt: Anonymität Online der nächsten Generation - **AN.ON-Next** -	01.01.2016	31.12.2018
Verbundprojekt: Starker Datenschutz für Bonus- und Zahlungssysteme - **Goodcoin** -	01.01.2016	31.12.2018
Verbundprojekt: Smart Privacy in Mobile Apps - **SmartPriv** -	01.01.2016	31.12.2018
Verbundprojekt: Datenschutzfreundliche Smartphone-Anwendungen ohne Kompromisse - **AppPETs** -	01.02.2016	31.01.2019
Verbundprojekt: PGuard App und Webportal - **PGuard** -	01.01.2016	30.06.2018
Verbundprojekt: Supporting the security community - **SECUNITY** -	01.01.2016	31.12.2018
Verbundprojekt: Sicheres Arbeiten im Web 2.0 - vollsynchrones Editieren verschlüsselter Dokumente - **SyncEnc** -	01.02.2016	31.07.2018

Thema	Laufzeit	
Verbundprojekt: Privacy-enhancing and Reliable Anti-Doping Integrated Service Environment - **PARADISE** -	01.01.2016	31.12.2017
KMU-innovativ - Verbundprojekt: Drahtlose, robuste, adaptive, industrielle Systeme - **DRAISE** -	01.02.2016	31.01.2019
Verbundprojekt: Selbstdatenschutz im vernetzten Fahrzeug - **SeDaFa** -	01.01.2016	31.12.2017
KMU-innovativ: Verbundprojekt: Sichere mobile Business Apps für Kunden und Nutzer von Serviceprovidern - **SimoBA** -	01.02.2016	31.01.2018
Verbundprojekt: Selbstbestimmte Verwertung personenbezogener Daten mit inhärentem Privatsphäre- und Datenschutz - **myneData** -	01.06.2016	31.05.2019
EUREKA-Verbundprojekt: SEcure Networking for DAta Transport in Europe - TAilored Network for Data cEnters in the Metro (Celtic-Plus Project ID: C2015/3-1) - **SENDATE-TANDEM** -	01.04.2016	31.03.2019
EUREKA-Verbundprojekt SEcure Networking for a DATa Center Cloud in Europe - ProgrammabLe Architecture for distributed NETwork functions and Security (Celtic-Plus Project ID: C2015/3-1) - **SENDATE-PLANETS** -	01.04.2016	31.03.2019
EUREKA-Verbundprojekt: SENDATE - Sichere und flexible Datenzentrums-Interkonnektivität (Celtic-Plus Project ID: C2015/3-1)- **SENDATE-Secure-DCI** -	01.06.2016	31.05.2019
EUREKA-Verbundprojekt SEcure Networking for a DATa Center Cloud in Europe - Flexible Infrastruktur für Datenzentrenkommunikation mit einzigartiger Sicherheit (Celtic-Plus Project ID: C2015/3-1) - **SENDATE-FICUS** -	01.05.2016	30.04.2019
Privacy and Digital Health Technologies	01.03.2016	28.02.2018
Verbundprojekt: Erkennung, Nachweis und Bekämpfung verdeckter Propaganda-Angriffe über neue Online-Medien - **PropStop** -	01.06.2016	31.05.2019
Verbundprojekt: DetektIon maliziöser Systemzustände, VisualisieruNG, ForEnsik, Meldung von SicherheiTsvorfällen - **DINGFEST** -	01.06.2016	31.05.2019
Verbundprojekt: Anomalie-Erkennung zur Verhinderung von Angriffen auf gesichtsbildbasierte Authentifikationssysteme - **ANANAS** -	01.06.2016	31.05.2019
Verbundprojekt: Selbstdatenschutz im Online-Commerce - **SIOC** -	01.04.2016	31.03.2019
Verbundprojekt: Explicit Privacy-Preserving Host Intrusion Detection System - **EXPLOIDS** -	01.07.2016	30.06.2019
Verbundprojekt: Erkennung von IT-Sicherheitsvorfällen an Internet-Knotenpunkten - **X-CHECK** -	01.05.2016	30.04.2019
Verbundprojekt: Verhaltensbasierte Analyse und Erkennung von modernem Schadcode - **VAMOS** -	01.08.2016	31.07.2019
Verbundprojekt: DECentralized Anomaly DEtection - **DecADe** -	01.06.2016	31.05.2019
Verbundprojekt: Datenschutz-respektierende Erkennung von Innentätern - **DREI** -	01.07.2016	31.01.2019
Eine Entwicklungsumgebung zur intelligenten Dienstfindung und -komposition - **ISCO** -	01.06.2016	31.05.2018
Innovative Strukturen für Digitales Vergessen -**InStruct**-	01.08.2016	31.07.2020
KMU-innovativ - Verbundprojekt: IT-Risikomanagement in der Hafentelematik auf Basis der Software-Architektur - **PortSec**-	01.09.2016	31.08.2018

Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333