Deutscher Bundestag **Drucksache 18/10682**

18. Wahlperiode 12.12.2016

Kleine Anfrage

der Abgeordneten Jan Korte, Frank Tempel, Dr. André Hahn, Ulla Jelpke, Katrin Kunert, Dr. Petra Sitte und der Fraktion DIE LINKE.

Cyber-Sicherheitsstrategie der Bundesregierung

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.

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.

Wir fragen die Bundesregierung:

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)?
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)?
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?
   b) Mit welchen Immatrikulationszahlen rechnet die Bundesregierung aufgrund entsprechender Bedarfsanmeldungen aus dem Geschäftsbereich des Bundesministeriums der Verteidigung?
   c) Für wie viele Studentinnen und Studenten insgesamt soll der geplante Studiengang offen stehen?
   d) Wie weit ist die Konzeption dieses Studiengangs fortgeschritten, und was werden wesentliche Lerninhalte sein?
   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?
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?
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?
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?
7. Was ist konkret gemeint, wenn in der Cyber-Sicherheitsstrategie von der Durchführung von „Netzwerkoperationen“ (S. 11) durch staatliche Stellen die Rede ist?

8. Was sind in diesem Zusammenhang die von der Bundesregierung oder nachgeordneten Stellen zugrunde gelegten Szenarien von „schwerwiegenden Cyber-Angriffen“?
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?
10. Soll die Bundeswehr auch in solchen Amtshilfevorgängen auf Leistungen ziviler Unternehmen zurückgreifen, und wenn ja, wozu ist dann noch das Amtshilfekonstrukt notwendig?
11. Wie weit ist der Aufbau einer „Cyber-Reserve“ bei der Bundeswehr bereits vorangeschritten?
    a) Wie ist sie in die Aufbauorganisation der Bundeswehr eingegliedert?
    b) Wie viele Reservisten sind für diese Cyber-Reserve gemeldet und mit welchen Vorläufen einziehbar?
    c) Was sind die rechtlichen Voraussetzungen zum Einsatz einer solchen Reservisteneinheit?
    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.?
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)?
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?
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?
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?
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?
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)?

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

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?

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?

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)?

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?

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?

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?

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

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?

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)?

Berlin, den 12. Dezember 2016

Dr. Sahra Wagenknecht, Dr. Dietmar Bartsch und Fraktion

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