Deutscher Bundestag **Drucksache 18/9334**

18. Wahlperiode 03.08.2016

Kleine Anfrage

der Abgeordneten Jan Korte, Frank Tempel, Annette Groth, Dr. André Hahn, Andrej Hunko, Ulla Jelpke, Katrin Kunert, Dr. Alexander S. Neu, Martina Renner, Kersten Steinke, Halina Wawzyniak und der Fraktion DIE LINKE.

Pläne der Bundesregierung für eine neue Cybersicherheitsstrategie

Nach Medienberichten von „ZEIT ONLINE“ und dem Deutschlandfunk vom 7. Juli 2016 plant die Bundesregierung die Verabschiedung einer neuen „Cybersicherheitsstrategie für Deutschland 2016“. Ein Referentenentwurf werde gegenwärtig zwischen den zuständigen Bundesministerien abgestimmt und soll im Herbst 2016 vom Kabinett verabschiedet werden. Entstehen soll demnach eine größere und fast militärische Sicherheitsarchitektur für den digitalen Raum, bestehend aus verschiedenen Behörden, die nicht nur beraten, sondern auch schnell handeln können soll. Der Strategie zufolge sollen gleich drei mobile Eingreiftruppen, sogenannte „Quick Reaction Forces“ zum Zweck der Strafverfolgung und der zivilen Gefahrenabwehr aufgebaut werden. Daneben sollen verschiedene Gremien und Behörden, darunter das Bundesamt für Sicherheit in der Informationstechnik (BSI) und das Cyber-Abwehrzentrum (Cyber-AZ) des Bundes in Bonn, stark ausgebaut, Polizei, Bundeswehr, Regierung und Wirtschaft stärker miteinander vernetzt werden. Laut den Medienberichten soll außerdem mit einem nationalen Computer Emergency Response Team (CERT) eine weitere Institution gegründet werden, um sofort auf eventuelle Angriffe reagieren zu können. Ferner prüfe die Bundesregierung, ob Hersteller haftbar gemacht werden können, wenn sie Sicherheitsmängel in ihrer Software und ihrer Hardware nicht beheben (vgl. ZEIT ONLINE vom 7. Juli 2016). Außerdem erklärte der Bundesminister des Innern, Dr. Thomas de Maizière, gegenüber dem ZDF-Morgenmagazin: „Wir wollen dass die Provider selbst eine Haftung und Verantwortung dafür übernehmen, wenn Straftaten in ihrem Netz stattfinden“ (ZDF-Morgenmagazin vom 21. Juli 2016).

Wir fragen die Bundesregierung:

1. Treffen die Pressemeldungen über Pläne der Bundesregierung für eine neue „Cybersicherheitsstrategie für Deutschland 2016“ zu, und wann soll diese verabschiedet werden bzw. in Kraft treten?
2. In welcher Weise soll die Strategie parlamentarisch beraten werden?
3. Welche Pläne existieren für einen Ausbau des BSI?
4. Welche Pläne existieren für einen Ausbau des Cyber-AZ des Bundes in Bonn, welche Behörden sollen daran in welchem Umfang beteiligt werden, und wer wird nach diesen Plänen zukünftig die Federführung innehaben?

5. Inwieweit wird bei den Plänen der Bundesregierung die grundsätzliche Kritik des Bundesrechnungshofs am Cyber-AZ, wonach dessen Einrichtung nicht gerechtfertigt und sein Nutzen „fraglich“ sei, da die jetzige Konzeption „nicht geeignet [sei], die über die Behördenlandschaft verteilten Zuständigkeiten und Fähigkeiten bei der Abwehr von Angriffen aus dem Cyberraum zu bündeln“ (Süddeutsche Zeitung vom 7. Juni 2014), berücksichtigt?
6. Soll das Cyber-AZ nach Plänen der Bundesregierung wesentlich umstrukturiert werden, um sinnvoller zu arbeiten?

   Wenn ja, in welcher Form soll das im Detail geschehen?
7. Hat die Bundesregierung selbst eine Evaluation des Cyber-AZ durchführen lassen, und wenn ja, mit welchem Ergebnis?

   Wenn nein, warum nicht?
8. Wie weit wurden die Planungen des Bundesministeriums des Inneren (BMI) zur Einrichtung von zwei Unterabteilungen „IT- und Cybersicherheit, sichere Informationstechnik“ und „Cybersicherheit im Bereich der Polizeien und des Verfassungsschutzes“ (heise.de, „Innenministerium: zwei neue Stäbe für die Cybersicherheit“, 13. Juni 2014) umgesetzt, was sind ihre Aufgaben, wie viel Personal wurde dorthin aus welchen anderen Abteilungen versetzt, und wie viel neu gewonnen?
9. Ist es nach Einschätzung der Bundesregierung mit Hilfe der Cyber-Abwehrabteilung im BMI besser als mit dem Cyber-AZ gelungen, die über die Behördenlandschaft verteilten Zuständigkeiten und Fähigkeiten bei der Abwehr von Angriffen aus dem Cyberraum zu bündeln?
10. Wie soll die zivil-militärische Zusammenarbeit zwischen Cyber-AZ und Bundeswehr im Detail neu konzipiert werden?
11. Treffen die Medienberichte zur Einrichtung des CERT zu, und wenn ja,

    a) handelt es sich dabei um eine tatsächlich neue Einrichtung oder die seit dem 1. September 2001 beim BSI bestehende „CERT-Bund“;

    b) was soll sich nach den bisherigen Planungen organisatorisch, personell und bei den Zuständigkeiten für das CERT bzw. CERT-Bund ändern;

    c) welche genaue Rolle ist ihm innerhalb der Cybersicherheitsstrategie zugedacht;

    d) mit welchen Kosten für Personal und Technik rechnet die Bundesregierung (bitte entsprechend aufschlüsseln)?
12. Inwieweit sind Cyber-AZ und CERT in den Ausbau der für offensive Cyber-Einsätze trainierenden CNO-Einheit (CNO – Computer Networks Operation) der Bundeswehr eingebunden?
13. Trifft es zu, dass der BND die „Lagebildaufklärung“ in fremden Netzen übernimmt oder übernehmen soll und seine Ressourcen im Konfliktfall den CNO-Kräften der Bundeswehr zur Verfügung stellt?
14. Wie viele öffentliche und nicht öffentliche Einrichtungen betreiben in der Bundesrepublik Deutschland ein CERT (bitte so weit wie möglich nach Verwaltung, Wirtschaft und Universitäten/Forschungseinrichtungen differenzieren), die im Deutschen CERT-Verbund zusammengeschlossen sind?
15. Existiert mittlerweile der „Verbund Deutscher Verwaltungs-CERT“, was sind seine Aufgaben und Tätigkeitsfelder, und wer hat die Geschäftsführung inne?

16. Welche externen Beraterinnen und Berater waren und sind bei der Ausarbeitung der „Cybersicherheitsstrategie für Deutschland 2016“ in welcher Form und Funktion tätig, und welche Kosten entstehen dadurch jeweils (bitte entsprechend nach den genannten Kategorien auflisten)?

17. Trifft es zu, dass im BMI Pläne existieren, wonach künftig mit dem Bundesamt für Verfassungsschutz (BfV), dem Bundeskriminalamt (BKA) und dem BSI gleich drei Behörden jeweils eine digitale Eingreiftruppe (Quick Reaction Force) aufbauen, die jederzeit ausrücken kann?

    Wenn ja, wie sehen diese Pläne konkret aus?

    a) Wann soll das „Cyber-Team“ des BfV einsatzbereit sein, aus wie vielen Personen soll es bestehen, mit welchen Ressourcen soll es ausgestattet werden, und welche Aufgaben soll es auf welcher Rechtsgrundlage übernehmen?

    b) Wann soll die Quick Reaction Force des BKA einsatzbereit sein, aus wie vielen Personen soll sie bestehen, mit welchen Ressourcen soll sie ausgestattet werden, und welche Aufgaben soll sie auf welcher Rechtsgrundlage übernehmen?

    c) Wann soll das Mobile Incident Response Team (MIRT) des BSI einsatzbereit sein, aus wie vielen Personen soll es bestehen, mit welchen Ressourcen soll es ausgestattet werden, und welche Aufgaben soll es auf welcher Rechtsgrundlage übernehmen?

    d) Sollen die Mitglieder der genannten neuen Einheiten durch Neustrukturierungen und Umsetzungen oder durch Neugewinnung von Personal gewonnen werden, und wie hoch schätzt die Bundesregierung den entstehenden Personalbedarf?

18. Wie und auf welcher Rechtsgrundlage soll die jeweilige Zuständigkeit der Quick Reaction Forces geregelt und sollen mögliche Kompetenzprobleme vermieden werden?

19. Wie soll verhindert werden, dass das Trennungsgebot zwischen Polizei und Nachrichtendiensten verletzt wird und sich Zuständigkeiten überschneiden?

20. Trifft es zu, dass im BMI Pläne existieren, wonach das BMI zusammen mit den Providern die „Sensorik im Netz ausbauen“ will, um Cyberangriffe und Infektionen besser erkennen zu können und laufende Angriffe abzuschwächen?

    Wenn ja:

    a) Was ist konkret mit „Sensorik“ gemeint?

    b) Auf welcher jeweiligen Rechtsgrundlage soll dies ggf. erfolgen?

    c) Welche entsprechenden Einrichtungen (honey pots etc.) werden dazu bereits von den Netzbetreibern in der Bundesrepublik Deutschland betrieben, und welche Defizite hat die Bundesregierung hierbei erkannt?

    d) Fällt darunter auch eine sogenannte „Deep Packet Inspection“?

21. Soll künftig der komplette Netzwerkverkehr automatisiert überwacht werden, und wenn ja, von wem soll dies auf welche Weise und auf welcher Rechtsgrundlage erfolgen?

    Wenn nein, in welchem Umfang und auf welche Weise soll dann die Überwachung auf welcher konkreten Rechtsgrundlage erfolgen?

22. Existieren in der Bundesregierung oder einzelnen Geschäftsbereichen Planungen mit dem Ziel, den Straftatenkatalog in § 100a der Strafprozessordnung (StPO) zu erweitern, und wenn ja, welche Straftatbestände oder kriminologischen Phänomenbereiche kommen hierfür in Betracht?

23. Um welche Straftaten handelt es sich nach Auffassung der Bundesregierung konkret, „die online und konspirativ verübt werden“ und demnach in den Straftatenkatalog des § 100a StPO aufgenommen werden müssten?

24. Plant die Bundesregierung eine „Anpassung“ der Mitwirkungspflichten von Unternehmen, etwa bei der Identifizierung von Nutzern, und wenn ja, wie soll diese Anpassung im Detail aussehen?

25. Wie können und sollen nach Auffassung der Bundesregierung eine Haftung und Verantwortung der Provider konkret geregelt werden, wenn Straftaten in deren Netzen stattfinden, und wie kann sichergestellt werden, dass Provider ihre Netze auf kriminelle Handlungen und Inhalte hin überprüfen, ohne dass sie dabei ihrerseits eine gesetzwidrige Überwachungsinfrastruktur aufbauen?

26. Kann die Bundesregierung ausschließen, dass darunter Pflichten auch für deutsche Anbieter von anonymen Internetdiensten sein werden?

27. Ist es korrekt, dass Pläne existieren, der Staat müsse sich stärker für private Sicherheitsdienstleister öffnen, weil es nach Auffassung der Bundesregierung in den Sicherheitsbehörden an Fachkräften mangele?

    Wenn ja:

    a) In welchen Bereichen und für welche Aufgaben will das BMI mehr private Sicherheitsfirmen einsetzen?

    b) Inwieweit soll die Bundeswehr künftig bei der Cyberabwehr Unterstützung durch zivile Akteure erhalten?

    c) Wie kann oder soll nach Auffassung der Bundesregierung die Datensicherheit bei der Beauftragung privater Unternehmen z. B. bei der Datenweitergabe etc. gewährleistet werden?

    d) Sieht die Bundesregierung insbesondere bei der Beauftragung nichtdeutscher privater Unternehmen Sicherheitsrisiken, und wenn ja, welche sind dies?

28. Ist es zutreffend, dass Pläne bestehen, wonach im BMI außerdem eine zentrale Stelle entstehen soll, die „Cyberwaffen“ (Hard- und Software zur Infiltration und zum aktiven Eindringen in fremde Computersysteme) beschafft und entwickelt, und wenn ja, aus welchen Gründen wird dies für nötig erachtet, und auf welcher jeweiligen Rechtsgrundlage soll dies passieren?

29. Was muss als Aufgabe dieser neuen Stabsstelle im BMI unter der Formulierung „technische Unterstützung für nationale Sicherheitsbehörden im Hinblick auf deren operative Cyberfähigkeiten“ im Detail verstanden werden (bitte ausführen)?

30. Ist es zutreffend, dass die Bundesregierung derzeit prüft, ob Hersteller haftbar gemacht werden können, wenn sie Sicherheitsmängel in ihrer Software und ihrer Hardware nicht beheben, und wenn ja,

    a) welche Ergebnisse hat diese Prüfung bereits erbracht;

    b) plant die Bundesregierung eine entsprechende Überarbeitung des IT-Sicherheitsgesetzes?

Berlin, den 3. August 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