Deutscher Bundestag **Drucksache 19/5790**

19. Wahlperiode 15.11.2018

Kleine Anfrage

der Abgeordneten Alexander Müller, Alexander Graf Lambsdorff, Grigorios Aggelidis, Renata Alt, Jens Beeck, Nicola Beer, Dr. Jens Brandenburg (Rhein-Neckar), Britta Katharina Dassler, Bijan Djir-Sarai, Dr. Marcus Faber, Daniel Föst, Thomas Hacker, Markus Herbrand, Katja Hessel, Manuel Höferlin, Dr. Christoph Hoffmann, Reinhard Houben, Olaf in der Beek, Thomas L. Kemmerich, Pascal Kober, Ulrich Lechte, Oliver Luksic, Till Mansmann, Christian Sauter, Dr. Wieland Schinnenburg, Matthias Seestern-Pauly, Judith Skudelny, Bettina Stark-Watzinger, Dr. Marie-Agnes Strack-Zimmermann, Benjamin Strasser, Katja Suding, Linda Teuteberg, Michael Theurer, Nicole Westig und der Fraktion der FDP

Härtung der Sicherheit von IT-Systemen und -Netzen in Bundeswehrnutzung

Die Bundeswehr sieht sich zahlreichen Angriffen auf ihre IT-Systeme und -Netze mit zum Teil hohem Schadenspotenzial ausgesetzt (Antwort der Bundesregierung vom 15. Juni 2018 auf die Schriftliche Frage 87 des Abgeordneten Alexander Graf Lambsdorff auf Bundestagsdrucksache 19/2922). Die Sicherheit von IT-Systemen und -Netzen, die von der Bundeswehr genutzt werden, muss aus Sicht der Fragesteller dringend und kontinuierlich gestärkt werden, um die Resilienz unserer Streitkräfte im digitalen Raum zu erhöhen.

Die Streitkräfte verfügen zwar über eigene Fähigkeiten, die von der Bundeswehr verwendeten IT-Systeme und -Netze auf Schwachstellen zu prüfen und einem Penetration-Testing zu unterziehen. Allerdings gibt es nach Kenntnis der Fragesteller verschiedene Einschränkungen, die einer umfassenden und fortdauernden Stärkung der Cyber-Resilienz der Bundeswehr entgegentreten und gegebenenfalls Schwachstellen unerkannt bleiben lassen, was die Systeme der Bundeswehr potenziell anfällig für Cyber-Angriffe macht, und im schlimmsten Fall zur Gefährdung von Leib und Leben unserer Soldatinnen und Soldaten führen kann. Ferner stellt sich die Frage nach der personellen Ausstattung der für Cybersicherheit zuständigen Organisationseinheiten.

Wir fragen die Bundesregierung:

1. Was unternimmt die Bundesregierung, um systematisch und planvoll alle IT-Systeme und -Netze der Bundeswehr resilient gegen Cyber-Angriffe zu machen?

2. Wie sind die Durchführung von Schwachstellenanalysen und das Penetration-Testing in IT-Systemen und -Netzen der Bundeswehr geregelt, und welche Vorgaben gelten für sie?

   a) Werden grundsätzlich alle IT-Systeme und -Netze der Bundeswehr Schwachstellenanalysen bzw. Penetration-Testings unterzogen?

      Wenn nein, warum nicht?

   b) Falls nicht alle IT-Systeme und -Netze der Bundeswehr systematisch überprüft werden können, sieht die Bundesregierung darin ein Risikopotenzial, und teilt sie die Einschätzung der Fragesteller, dass die Möglichkeit einer hausinternen Überprüfung auf Schwachstellen uneingeschränkt gelten soll?

3. Wie und auf Grund welcher Kriterien erfolgt die Auswahl, welche IT-Systeme und -Netze der Bundeswehr einer Schwachstellenanalyse bzw. einem Penetration-Testing unterzogen werden?

4. Falls diese Analysen bislang nur auf Anforderung der jeweiligen Nutzereinheiten der IT-Systeme stattfinden, teilt die Bundesregierung die Ansicht der Fragesteller, dass eine planvolle und systematische Analyse der Systeme besser von zentralen für Cyber-Sicherheit zuständigen Einrichtungen (wie z. B. dem Chief Information Security Officer, CISO-Bw, oder der Abteilung Cyber des Bundesministeriums der Verteidigung) veranlasst werden sollten?

5. Wie viele vollständig personell und materiell ausgerüstete Einsatzteams besitzt die Bundeswehr für die Suche nach und die Analyse von Schwachstellen und Eindringmöglichkeiten in eigene Systeme und Netze (bitte nach Dezernaten aufschlüsseln)?

6. a) Ist es üblich, dass Unterstützung durch externe Berater eingekauft werden muss, um die nötigen Aufgaben im Bereich Absicherung und Härtung eigener IT-Systeme und -Netze der Bundeswehr durchführen zu können?

   b) Wenn ja, in welchem finanziellen Volumen wurden seit dem Jahr 2014 externe Unterstützungsleistungen eingekauft (bitte nach Jahr und Projekt aufschlüsseln), und welche Unterstützungsleistungen sind für das Haushaltsjahr 2019 vorgesehen (bitte die vorgesehenen Haushaltsmittel mit angeben)?

7. a) Ist die Bundesregierung der Ansicht, dass die personelle Ausstattung für diese Aufgaben mittel- und langfristig ausreichend ist?

   b) Ist ein personeller und/oder materieller Aufwuchs geplant?

      Wenn ja, bitte die Details nennen und nach Dezernaten sowie Jahr aufschlüsseln?

8. Schränken Nutzungsverträge des Bundesamts für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw) die hausinterne Analyse von IT-Systemen und -Netzen der Bundeswehr ein?

9. Kam es in der Vergangenheit schon vor, dass potenziell unsichere oder ungehärtete Systeme nicht untersucht oder abgesichert wurden, weil Nutzungsverträge des BAAINBw diese Analysen verhinderten?

   Wenn ja, bitte die Fälle auflisten?

10. a) Behält sich das BAAINBw vertraglich grundsätzlich mit der Beschaffung jeglicher IT-Systeme vor, deren Schwachstellen hausintern analysieren zu dürfen?

    Falls nein, warum nicht?

    b) Wenn die Analyseergebnisse verbindlich als geheim eingestuft werden, was spricht dann dagegen, diese Bedingung als „conditio sine qua non“ für die Beschaffung festzulegen?

11. Besitzt die Bundeswehr derzeit Waffensysteme mit integrierten IT-Systemen, die gravierende Sicherheitslücken besitzen und dadurch vorübergehend oder dauerhaft aus der Nutzung genommen werden mussten (wenn ja, bitte auflisten)?

Berlin, den 7. November 2018

Christian Lindner 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