Deutscher Bundestag **Drucksache 19/6503**

19. Wahlperiode 13.12.2018

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Alexander Müller, Alexander Graf Lambsdorff, Grigorios Aggelidis, weiterer Abgeordneter und der Fraktion der FDP
– Drucksache 19/5790 –

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

Vorbemerkung der Fragesteller

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.

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

Das Bundesministerium der Verteidigung (BMVg) hat entlang den Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zentrale Regelungen erlassen, um die Sicherheit von IT im gesamten Lebenszyklus sicherzustellen.

In der Beschaffungsphase werden Schutzbedarfserhebungen und Bedrohungsanalysen durchgeführt und geeignete Maßnahmen zur Risikominimierung nach Maßgabe BSI-Grundschutz dokumentiert und implementiert. Vor Einführung eines

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums der Verteidigung vom 11. Dezember 2018 übermittelt.

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

neuen Systems in die Nutzung erfolgt eine Schwachstellenanalyse im Rahmen der Akkreditierung. Unter Akkreditierung wird ein Prüfungs- und Genehmigungsverfahren von IT durch die zuständige Stelle verstanden.

In der Nutzungsphase werden bis zur Aussonderung regelmäßig Schwachstellenanalysen bzw. Penetrationstests im Rahmen von Inspektionen durchgeführt. Weiterhin werden zur IT-sicherheitstechnischen Überwachung und Blockierung u. a. von Schadsoftware, Systeme zur Erkennung und zum Schutz an Netzübergängen in Fremdnetze, an den Grenzen von Netzsegmenten sowie an den Endgeräten bzw. Servern eingesetzt.

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?

Die Fragen 2 bis 2b werden zusammen beantwortet.

Es werden grundsätzlich und systematisch – zentral priorisiert durch den Chief Information Security Officer der Bundeswehr (CISOBw) – alle IT-Systeme und -Netze einer Schwachstellenanalyse bzw. einem Penetrationstest unterzogen.

In der Beschaffungsphase eines neuen Systems wird vor dessen Einführung in die Nutzung eine Schwachstellenanalyse im Rahmen der Akkreditierung durchgeführt.

Bestandssysteme und -Netze in der Nutzung werden im Rahmen der personellen und materiellen Kapazitäten durch den CISOBw priorisiert systematisch einer Schwachstellenanalyse bzw. einem Penetrationstest unterzogen.

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?

Die Priorisierung erfolgt anhand der Kriterien Angriffsfläche aus dem Internet, Wert der verarbeiteten Informationen und Wert der Verfügbarkeit des Systems oder Netzes für die Aufgaben der Bundeswehr.

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?

Auf die Antwort zu Frage 2 wird verwiesen.

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)?

Zur Beantwortung der Frage 5 wird auf die „VS – Nur für den Dienstgebrauch“ eingestufte Anlage* verwiesen. Die Einstufung erfolgt, da Kenntnisse zu den bestehenden Einsatzteams Rückschlüsse auf die Einsatzfähigkeit der Bundeswehr zuließen. Die Kenntnisnahme durch Unbefugte kann für die Interessen der Bundesrepublik Deutschland nachteilig sein.

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)?

Die Fragen 6a und 6b werden zusammen beantwortet.

Es ist nicht üblich, externe Berater bei der Schwachstellenanalyse bzw. Penetrationstests eigener IT-Systeme und -Netze der Bundeswehr einzubeziehen.

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?

Zur Beantwortung der Fragen 7a und 7b wird auf die „VS – Nur für den Dienstgebrauch“ eingestufte Anlage* verwiesen. Die Einstufung erfolgt, da Kenntnisse zu den bestehenden Einsatzteams Rückschlüsse auf die Einsatzfähigkeit der Bundeswehr zuließen. Die Kenntnisnahme durch Unbefugte kann für die Interessen der Bundesrepublik Deutschland nachteilig sein.

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

Nutzungsverträge des BAAINBw werden grundsätzlich so geschlossen, dass sie die Analyse von IT-Systemen und -Netzen durch Kräfte der Bundeswehr gestatten. In Einzelfällen können Gesetze (z. B. Medizingerätegesetz, Luftfahrtgesetz) Einschränkungen enthalten, die sich auf die Nutzungsverträge auswirken.

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?

Der Bundesregierung sind derartige Fälle nicht bekannt.

* Das Bundesministerium der Verteidigung 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.

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?

Ja.

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

Auf die Antwort zu Frage 10a wird verwiesen.

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)?

Der Bundesregierung sind keine Waffensysteme bekannt, die aufgrund von gravierenden Sicherheitslücken in den darin integrierten IT-Systemen vorübergehend oder dauerhaft aus der Nutzung genommen werden musst.

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