Deutscher Bundestag **Drucksache 19/29783**

19. Wahlperiode 19.05.2021

Antrag

der Abgeordneten Joana Cotar, Uwe Schulz, Dr. Michael Espendiller, Peter Felser, Jörn König, Ulrich Oehme, Dr. Dirk Spaniel und der Fraktion der AfD

Anreizprogramme für IT-Sicherheit bei der Bundeswehr ausbauen

Der Bundestag wolle beschließen:

I. Der Deutsche Bundestag stellt fest:

Die immer weiter voranschreitende Digitalisierung der Bundeswehr betrifft die gesamten Organisationsstrukturen über alle Einheiten hinweg, wobei sich die Relevanz der Digitalisierung für die Bundeswehr vor allem in dem 2017 gegründeten Organisationsbereich Cyber- und Informationsraum (CIR) und der Abteilung Cyber/Informationstechnik im BMVg widerspiegelt. Diese Einheiten verstehen sich als „Treiber der Digitalisierung“, in dem die „digitale Transformation angestoßen wird“ (www.bmvg.de/resource/blob/143248/7add8013a0617d0c6a8f4ff969dc0184/20190925-download-erster-bericht-digitale-transformation-data.pdf). Für die Streitkräfte ist die Digitalisierung der Schlüssel zur Informations-, Führungs- und Wirkungsüberlegenheit, wie auch zur Verbesserung der Durchsetzungs- und Reaktionsfähigkeit (www.bmvg.de/resource/blob/143248/7add8013a0617d0c6a8f4ff969dc0184/20190925-download-erster-bericht-digitale-transformation-data.pdf, S. 3, Punkt 2). Wie bei anderen Streitkräften und Organisationen stellt die Komplexität der IT-Infrastruktur hinsichtlich eines sicheren Betriebs der zum Einsatz kommenden Technologien auch die Bundeswehr vor besondere Herausforderungen. Als Streitkraft einer der größten Industrienationen mit weltweitem Einsatzgebiet ist die Bundesehr nicht vor Hacker-Angriffen gefeit (www.faz.net/aktuell/wirtschaft/digitec/solarwinds-hack-massiver-cyberangriff-gefaehrdet-deutsche-behoerden-17134477.html). Die Hintergründe und Zwecke solcher Angriffe können nicht immer genau rekonstruiert werden, dienen aber der häufig der Spionage, Verschleierung oder der Sabotage (The Modern Ninja, Thomas Wilhelm, Jason Andress, in Ninja Hacking, 2011).

Um diesen Bedrohungen entgegenzuwirken, betreibt die Bundeswehr seit Oktober 2020 ein Bug-Bounty-Programm namens Vulnerability Disclosure Policy (VDPBw); www.bundeswehr.de/de/security-policy) (VDPBw). Hierbei überprüfen sogenannte White Hat Hacker die IT-Infrastruktur auf sicherheitsrelevante Schwachstellen (www.wiwo.de/technologie/digitale-welt/cybersecurity-die-bundeswehr-bittet-hacker-um-hilfe-und-speist-sie-mit-einem-fleisskaertchen-ab/26591646.html). White Hat Hacker sind IT-Sicherheitsexperten, welche im Rahmen eines Vertrages Sicherheitsevaluierungen (Ethics and Hacking, Thomas Wilhelm, in Professional Penetration Testing (Second Edition), 2013) durchführen. Im Falle der Bundeswehr ist ein White Hat Hacker an das Bug-Bounty-Programm VDPBw der Bundeswehr gebunden (www.bundeswehr.de/de/security-policy). Das VDPBw steht prinzipiell jedem White Hat Hacker

offen, der sich an die darin genannten Vorgaben hält und entsprechend mit der Bundeswehr in Kontakt tritt.

Die Angriffe auf die Infrastruktur der Bundeswehr sind enorm. Laut Staatssekretär Peter Tauber sind bis November 2020 im Rahmen des Bug-Bounty Programms der Bundeswehr VDPBw 40 sicherheitsrelevante Meldungen zu Systemen der Bundeswehr oder zu von Dritten für die Bundeswehr betriebenen Systemen eingegangen“ (Bundestagsdrucksache 19/24511, S. 49, Antwort auf die Schriftliche Frage 66.). Bereits 2017 hat die damalige Verteidigungsstaatssekretärin Katrin Suder „etwa 3500 substanzielle Angriffe auf Rechner, Netze und die Infrastruktur der deutschen Streitkräfte“ feststellen müssen (www.stuttgarter-nachrichten.de/inhalt.deutschland-baut-cyber-armee-auf-taeglich-3500-angriffe-auf-die-bundeswehr.9e64d548-97f2-45d3-9f54-89851c5e338f.html). Insgesamt gab es nach Angaben der Bundeswehr 2017 etwa zwei Millionen unautorisierte Zugriffsversuche auf ihre Systeme, darunter 8000 hochrangige, bei denen das Eindringen in die IT-Systeme der Armee nur nicht gelang, weil Abwehrmaßnahmen wie Firewalls funktionierten (www.dw.com/de/bundeswehr-gut-ger%C3%BCstet-f%C3%BCr-den-cyberkrieg/a-44984233). Der Direktor des technischen Forschungsinstituts Code an der Universität der Bundeswehr, Professor Udo Helmbrecht, konstatiert, „dass alles das, was an Technologien im Computerzeitalter zur Verfügung steht, weiterentwickelt wird, natürlich auch von Kriminellen oder von Staaten und Institutionen für Spionage beispielsweise missbraucht wird“ (www.deutschlandfunk.de/fehlende-it-sicherheitsstrategie-cyberangriffe-auf-daten.684.de.html?dram:article_id=489628). Auf Basis dieser Angaben gehen die Antragsteller davon aus, dass die Methoden und Umfang der Bedrohungen in Zukunft noch weiter steigen werden.

Länder wie die Vereinigten Staaten von Amerika haben mit White Hat Hackern bereits sehr gute Erfahrungen gemacht und die Zusammenarbeit professionalisiert (https://news.clearancejobs.com/2020/04/19/how-white-hat-hackers-keep-military-systems-safe/). Beispielsweise wurde bei der vierten „Hack the Air Force Challenge“ in 2019, durchgeführt von einer Organisation von White Hat Hackern und dem Department of Defence, das United States Air Force Virtual Data Center (virtuelle Datencenter) gehackt, ohne dass ein tatsächlicher Schaden entstanden ist (ebd.). Über die Erkenntnis, welche Systeme für Hacker anfällig sind, bietet die Zusammenarbeit mit White Hat Hackern darüber hinaus die Möglichkeit der Dokumentation und des Wissenstransfers. Auf Grund der Tatsache, dass White Hat Hackers in der Regel bei einer auf BugBounty Programme spezialisierten Organisation angestellt sind, stehen ihnen dort Trainingsbudgets und die neusten Hacker-Technologien zur Erprobung zur Verfügung (Ethics and Hacking, Thomas Wilhelm, in Professional Penetration Testing (Second Edition), 2013). Nach der Durchführung eines solchen Bug-Bounty-Programms können die gewonnenen Erkenntnisse der White Hat Hacker genutzt werden um diese bundewehrintern weiterzugeben und die Sicherheit der IT-Infrastruktur insgesamt zu verbessern.

Momentan ist das Bug-Bounty Programm der Bundewehr leider für White Hat Hacker weitestgehend unattraktiv. Während Unternehmen wie Apple und Google bereit sind, teils Millionenbeträge für gefundene IT-Schwachstellen an White Hat Hacker zu zahlen und das US-Verteidigungsministerium zwar keine absoluten Budgetzahlen nennt, aber im Herbst 2018 75.000 US-Dollar an die schnellsten Finder ausgezahlt hat, bietet die Bundeswehr lediglich eine Danksagung auf ihrer Webseite an (www.wiwo.de/technologie/digitale-welt/cybersecurity-die-bundeswehr-bittet-hacker-um-hilfe-und-speist-sie-mit-einem-fleisskaertchen-ab/26591646.html; www.bundeswehr.de/de/security-policy/danksagung). Hier besteht nach Ansicht der Antragsteller deutlicher Anpassungsbedarf auf Seiten der Bundeswehr.

II. Der Deutsche Bundestag fordert die Bundesregierung daher auf,

1. unter Federführung des Organisationsbereichs Cyber- und Informationsraum (CIR) und der Abteilung Cyber/Informationstechnik im BMVg eine Auswahl an international agierenden Bug-Bounty-Organisationen als mögliche Kooperationspartner der Bundeswehr zusammenzustellen,
2. die Anwendung des Bug-Bounty-Programms auf zuvor festgelegte Themengebiete zu priorisieren und später auf alle Bereiche auszuweiten. Besonderer Fokus ist auf Netzwerke, Internet-of-Things, Künstliche Intelligenz und Verwaltung zu legen,
3. die Vergütungen und Anreize zu einer Teilnahme an dem Bug-Bounty-Programm internationalen Standards anzugleichen,
4. einen systematischen und nachhaltigen Erkenntnis-Transfer der Bug-Bounty-Operationen in sämtliche relevanten Organisationseinheiten zu gewährleisten,
5. Bug-Bounty-Programme mindestens alle ein bis zwei Jahre durchzuführen und diese somit zu einem institutionalisierten Bestandteil der digitalen Verteidigung werden zu lassen.

Berlin, den 7. Mai 2021

Dr. Alice Weidel, Dr. Alexander Gauland und Fraktion

Begründung

Die Bundeswehr ist im Begriff, sich digital neu aufzustellen und neue Herausforderungen anzugehen. Um die Sicherheit der Soldaten und der IT-Infrastruktur bestmöglich zu gewährleisten, müssen neue Wege in den unterstützenden Maßnahmen gegangen werden. Länder wie die Vereinigten Staaten von Amerika sind hier bereits in der Vorreiterrolle und setzen unter anderem auf Bug Bounty-Programme, um mögliche digitale Angriffspunkte frühzeitig zu erkennen und zu beheben.

Gesamtherstellung: H. Heenemann GmbH & Co. KG, Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.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