Deutscher Bundestag **Drucksache 19/24518**

19. Wahlperiode 20.11.2020

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Dr. Marcus Faber, Alexander Graf Lambsdorff, Jens Beeck, weiterer Abgeordneter und der Fraktion der FDP
– Drucksache 19/23032 –

Cyber-Sicherheit von maritimen Navigationssystemen der Marine

Vorbemerkung der Fragesteller

Mit dem Fortschreiten der Digitalisierung der Kampfschiffe der Deutschen Marine wachsen neben den Chancen auch kontinuierlich die Gefahren durch eben diese Digitalisierung. Die Dimension Cyber- und Informationsraum ist nicht mehr nur eine Unterstützungsebene, sondern wird in heutigen Konflikten ein elementarer Teil der Wirkebene sein. Mit der Digitalisierung, Automatisierung und Vernetzung der Systeme auf den Kampfschiffen müssen diese Systeme auch robuster werden, um unter geänderten geopolitischen Bedingungen gegen neue hybride Bedrohungen und Cyber-Angriffe von Staaten und Organisationen gewappnet zu sein.

Aktuell warnt das Bundesamt für Verfassungsschutz (BfV) vor Gefährdungen wie Spionage und Sabotage hinsichtlich umfassender Navigationssysteme, sogenannter ECDIS (Electronic Chart Display and Information System) auf Schiffen (https://www.maritimes-cluster.de/news/aktuelles/sicherheitshinweis-des-bundesamtes-fuer-verfassungsschutz/). In solchen Navigationssystemen können die GPS-Navigation (GPS = Global Positioning System), das Radar, das Automatische Identifikationssystem, elektronische Seekarten etc. integriert werden. Damit sind diese Systeme unabdingbar für eine uneingeschränkte, sichere sowie zeitgemäße Navigation und damit auch für die Einsatzbereitschaft der Kampfschiffe der Deutschen Marine. Insbesondere global agierende Hersteller von modernen maritimen Navigationssystemen, so befürchtet das BfV, können in den jeweiligen „Herkunftsländern weitreichender Einflussnahme der dortigen Nachrichtendienste ausgesetzt (…)“ sein. Damit besteht auch die Gefahr, dass bei solchen kritischen Anwendungen für die Marine bereits bei der Programmierung, aber auch bei späteren Updates der Software ein Risiko zur Kompromittierung besteht.

In Krisensituationen bestünde damit die Möglichkeit, dass die Position sowie die Fahrt und der Kurs von Kriegsschiffen feindlichen Kräften zur Verfügung steht. Dies bedeutet eine unmittelbare Gefahr für die Besatzung und wäre eine Einschränkung der Einsatzfähigkeit. Ein derartiges Einfallstor in das Netzwerk eines Kampfschiffes kann auch auf andere Systeme ausstrahlen. So besteht die Gefahr, dass ein möglicher feindlicher Zugriff auf die Navigationssysteme aufgrund der Vernetzung an Bord dazu führt, dass Zugang zu Sensoren, Effektoren und Steuerungssystemen erhalten werden kann (https://esut.de/

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums der Verteidigung vom 19. November 2020 übermittelt.

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

2019/08/fachbeitraege/streitkraefte-fachbeitraege/14134/herausforderungen-der-cyber-sicherheit-in-der-deutschen-marine/). Die Cyber-Sicherheit von Navigationssystemen der Marine ist damit von besonderer und kritischer Bedeutung für die Einsatzbereitschaft.

Vorbemerkung der Bundesregierung

Das verfassungsrechtlich verbürgte Frage- und Informationsrecht des Deutschen Bundestages gegenüber der Bundesregierung wird durch gleichfalls Verfassungsrang genießende schutzwürdige Interessen wie das Staatswohl begrenzt.

Das Bundesministerium der Verteidigung (BMVg) ist nach sorgfältiger Abwägung des parlamentarischen Informationsanspruchs des Deutschen Bundestages mit dem Staatswohl zu der Auffassung gelangt, dass die Beantwortung der Fragen in Teilen nicht in offener Form erfolgen kann.

Deshalb wurden gemäß der Allgemeinen Verwaltungsvorschrift zum materiellen Geheimschutz des Bundesministeriums des Innern, für Bau und Heimat (BMI) die Antwort auf die Frage 21 als „VS – Nur für den Dienstgebrauch“ und die Antworten auf die Fragen 1 bis 10, 13, 14 und 16 bis 20 als „VS – Geheim“ eingestuft.*

1. Sind bei Navigationssystemen der Deutschen Marine Firmen (inklusive Tochterfirmen) beteiligt, die Standorte in Ländern haben, die auf der Staatenliste im Sinne von § 13 Absatz 1 Nummer 17 des Sicherheitsüberprüfungsgesetzes (SÜG) stehen?

   Wenn ja, welche Firmen in welchen Ländern?

2. Sieht die Bundesregierung ein Risiko, dass auch die Marine von der in der Vorbemerkung der Fragesteller genannten Warnung des BfV betroffen ist?

3. Welche Maßnahmen hat die Marine getroffen, um den Sicherheitshinweisen des BfV zu folgen?

4. Findet die Programmierung dieser Navigationssysteme von Firmen (inklusive Tochterfirmen) in Ländern statt, die auf der Staatenliste im Sinne von § 13 Absatz 1 Nummer 17 SÜG stehen, und wenn ja, welche Firmen in welchen Ländern?

5. Werden diese Navigationssysteme gezielt und regelmäßig nach Schadsoftware und ungewollten Funktionen überprüft?

6. Wurden die genannten Systeme von den zuständigen Stellen der Bundeswehr (z. B. Zentrum für Cybersicherheit, Zentrum für Softwarekompetenz, Zentrum für Cyber Operations) einmal auf mögliche Angreifbarkeit („Penetration“) getestet, bezüglich selbständiger Kontaktaufnahmen der Systeme nach außen geprüft oder einer Code-Analyse unterzogen?

7. Wurde geprüft, ob diese Systeme die IT-Sicherheitsanforderungen der Bundeswehr einhalten?

   a) Wenn ja, wann, von wem, und mit welchem Ergebnis?

   b) Wenn nein, warum nicht, und existieren Hinderungsgründe?

* Das Bundesministerium der Verteidigung hat Teile der Antwort als „VS – Vertraulich“ und „VS – Geheim“ eingestuft. Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

8. Wurden Prüfungen der genannten Systeme von Dienststellen der Bundeswehr verhindert, z. B. aufgrund rechtlicher Bedenken, und wenn ja, mit welcher Begründung?

9. Wann wurden letztmalig die Implementierungs- und Wartungsverfahren dieser Systeme kritisch evaluiert?

10. Gab es in der Vergangenheit anlassbezogene Prüfungen der Navigationssysteme, und wenn ja, wann, und auf welchen Schiffen?

Die Fragen 1 bis 10 werden zusammen beantwortet.

Auf die als GEHEIM eingestufte Anlage wird verwiesen.

Die Bundesregierung ist nach sorgfältiger Abwägung des parlamentarischen Informationsanspruchs des Deutschen Bundestages mit dem Wohl des Bundes (Staatswohl), das durch Bekanntwerden geheimhaltungsbedürftiger Informationen gefährdet werden könnte, der Auffassung, dass eine Beantwortung der Fragen 1 bis 10 in offener Form nicht erfolgen kann.

Die erbetenen Auskünfte sind geheimhaltungsbedürftig, weil sie sicherheitsrelevante Angaben enthalten, deren Bekanntwerden die Sicherheit der Bundesrepublik Deutschland gefährden oder ihren Interessen schweren Schaden zufügen kann. Heutige, moderne Navigationssysteme von Kriegsschiffen sind unabdingbar für eine uneingeschränkte, sichere sowie zeitgemäße Navigation. Im Zeitalter der Digitalisierung und Vernetzung kommt der Cybersicherheit von Navigationssystemen der Marine in besonders hohem Maße eine kritische Bedeutung für die Einsatzbereitschaft und Sicherheit der Besatzungen der Kampfschiffe der Deutschen Marine zu. In der Auseinandersetzung mit den vorliegenden Fragestellungen, insbesondere den Fragen nach den Herkunftsländern, der Programmierung der Navigationssysteme und deren Resilienz, werden – die Cybersicherheit und Produktinformationen betreffend – detaillierte Antworten zur Kenntnis gebracht, die einem hohen Schutzbedürfnis unterliegen, insofern sie Rückschlüsse auf Fähigkeiten zulassen.

11. Werden die bereits bei der Marine verbauten Navigationssysteme durch Firmen (inklusive Tochterfirmen) in Ländern ferngewartet, die auf der Staatenliste im Sinne von § 13 Absatz 1 Nummer 17 SÜG stehen?

Nein, für die Fernwartung gelten gemäß der im Geschäftsbereich des BMVg geltenden Zentralen Dienstvorschrift (ZDv) A-960/1 „Informationssicherheit“ sehr strenge Auflagen. Im Projekt „Radarnavigation, Electronic Chart Display Information System (ECDIS), Automatic Information System (AIS)“ (RadEA) ist eine Fernwartung nicht gefordert und es findet auch keine Fernwartung statt.

12. Können diese Navigationssysteme grundsätzlich durch Firmen (inklusive Tochterfirmen) aus Ländern ferngewartet werden, die auf der Staatenliste im Sinne von § 13 Absatz 1 Nummer 17 SÜG stehen?

Auf die Antwort auf die Frage 11 wird verwiesen.

13. Hat die Bundeswehr uneingeschränkten Zugriff auf den Quellcode dieser Navigationssysteme?

14. Existieren sogenannte Blackboxes in diesen Navigationssystemen?

Die Fragen 13 und 14 werden zusammen beantwortet.

Auf die als GEHEIM eingestufte Anlage wird verwiesen.

Die Bundesregierung ist nach sorgfältiger Abwägung des parlamentarischen Informationsanspruchs des Deutschen Bundestages mit dem Wohl des Bundes (Staatswohl), das durch Bekanntwerden geheimhaltungsbedürftiger Informationen gefährdet werden könnte, der Auffassung, dass eine Beantwortung der Fragen 13 und 14 in offener Form nicht erfolgen kann. Die erbetenen Auskünfte zu Quellcodes und Blackboxes in Navigationssystemen für die Deutsche Marine sind geheimhaltungsbedürftig, weil sie Rückschlüsse auf die technische Leistungsfähigkeit enthalten, deren Bekanntwerden für die Sicherheit der Schiffe im Einsatz nachteilig sein und die Sicherheit der Bundesrepublik Deutschland gefährden oder ihren Interessen schweren Schaden zufügen kann.

15. Wie werden die zuständigen IT-Offiziere der Marine ausgebildet und nach welchen Auswahlverfahren für das einzelne Kampfschiff ernannt?

Die Ausbildung der IT-Offiziere der Marine umfasst drei Ausbildungsabschnitte. Aufbauend auf einer Basisqualifikation (Fachschulausbildung/Studium) in Abhängigkeit der Laufbahn (Offiziere des militärfachlichen Dienstes und Offiziere des Truppendienstes) erfolgt eine streitkräftegemeinsame erste Dienstposten-Qualifikation durch den Lehrgang IT-Manager der Bundeswehr. Dieser hat zum Ziel, streitkräftegemeinsame Kenntnisse und Grundfertigkeiten zu erwerben, um die Elemente des IT-Systems Bundeswehr/Führungsunterstützung der Bundeswehr zu planen, zu steuern und zu überwachen. Anschließend folgt die weitere Dienstposten-Qualifikation im Rahmen von Spezialisierungen durch die Wahrnehmung weiterer lehrgangsgebundener Ausbildung.

16. Inwiefern werden Geheimhaltungsbereiche auf den Kampfschiffen der Deutschen Marine gesichert und kontrolliert?

Auf die als GEHEIM eingestufte Anlage wird verwiesen.

Die Bundesregierung ist nach sorgfältiger Abwägung des parlamentarischen Informationsanspruchs des Deutschen Bundestages mit dem Wohl des Bundes (Staatswohl), das durch Bekanntwerden geheimhaltungsbedürftiger Informationen gefährdet werden könnte, der Auffassung, dass eine Beantwortung der Frage 16 in offener Form nicht erfolgen kann. Die erbetenen Auskünfte sind geheimhaltungsbedürftig, weil die Geheimhaltungsbereiche auf den Kampfschiffen der Deutschen Marine Rückschlüsse auf eigene militärische Handlungs- und Verteidigungsfähigkeiten erlauben. Sie enthalten sicherheitsrelevante Angaben, deren Bekanntwerden für die Sicherheit der Schiffe im Einsatz nachteilig sein und die Sicherheit der Bundesrepublik Deutschland gefährden oder ihren Interessen schweren Schaden zufügen kann.

17. Sind bei der Marine aktuell Navigationssysteme von Firmen (inklusive Tochterfirmen) verbaut, die vom Militärischen Abschirmdienst (MAD) oder vom Bundesamt für Verfassungsschutz als Prüf- oder Verdachtsfall geführt werden?

18. Laufen derzeit Ausschreibungen für neue ECDIS-Navigationssysteme für die Marine, und wie ist der Stand der Ausschreibung bzw. Vergabe, und wenn ja, für welche Kampfschiffe der Marine läuft die Ausschreibung?

19. Wurde die Warnung der Behörden vor möglichen Zugriffsmöglichkeiten auf die ECDIS-Systeme oder möglicher Sabotage dieser Systeme bei der Ausschreibung berücksichtigt, und welche Maßnahmen wurden getroffen, um solche Zugriffe von Beginn an auszuschließen?

20. Hat der MAD oder das BfV wegen der laufenden Ausschreibung eine oder mehrere Prüfungen von möglichen oder tatsächlichen Anbietern eingeleitet?

Die Fragen 17 bis 20 werden zusammen beantwortet.

Auf die als GEHEIM eingestufte Anlage wird verwiesen.

Die Bundesregierung ist nach sorgfältiger Abwägung des parlamentarischen Informationsanspruchs des Deutschen Bundestages mit dem Wohl des Bundes (Staatswohl), das durch Bekanntwerden geheimhaltungsbedürftiger Informationen gefährdet werden könnte, der Auffassung, dass eine Beantwortung der Fragen 17 bis 20 in offener Form nicht erfolgen kann. Die erbetenen Auskünfte sind geheimhaltungsbedürftig, weil nachrichtendienstliche Erkenntnisse der Einstufung unterliegen, deren Bekanntwerden die Sicherheit der Bundesrepublik Deutschland gefährden oder ihren Interessen schweren Schaden zufügen kann.

21. Handelt es sich bei ECDIS-Navigationssystemen um sogenannte nationale verteidigungsindustrielle Schlüsseltechnologie?

Auf die als „VS – Nur für den Dienstgebrauch“ eingestufte Anlage wird verwiesen.*

Die erbetenen Auskünfte sind geheimhaltungsbedürftig, weil sie deutliche Rückschlüsse zu eigenen militärischen Handlungs- und Verteidigungsfähigkeiten erlauben. Sie enthalten sicherheitsrelevante Angaben, deren Bekanntwerden für die Interessen der Bundesrepublik Deutschland nachteilig sein können. Bei offener Beantwortung wäre eine freie Einsicht in die Kapazitäten und Fähigkeiten der deutschen Hersteller zu befürchten. Die Handlungsfähigkeit zumindest von Teilen der Bundesregierung könnte damit empfindlich verringert werden.

* 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.

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