MAG. KLAUDIA TANNER
BUNDESMINISTERIN FÜR LANDESVERTEIDIGUNG

S91143/38-PMVD/2024 27. Mai 2024

Herrn
Präsidenten des Nationalrates

Parlament
1017 Wien

Die Abgeordneten zum Nationalrat Dr. Brandstätter, Kolleginnen und Kollegen haben am 27. März 2024 unter der Nr. 18235/J an mich eine schriftliche parlamentarische Anfrage betreffend „Frequenz von Cyberattacken und Gegenmaßnahmen“ gerichtet. Diese Anfrage beantworte ich wie folgt:

Zu 1 bis 4a:

Diese Fragen betreffen durchwegs Angelegenheiten, die im Interesse der Staatssicherheit und im besonderen Sicherheitsinteresse des Bundesministeriums für Landesverteidigung (BMLV) liegen und somit gemäß Art. 20 Abs. 3 aus Gründen der Umfassenden Landesverteidigung nicht geeignet sind, im Rahmen einer parlamentarischen Anfragebeantwortung öffentlich erörtert zu werden. Ich ersuche daher um Verständnis, dass eine Beantwortung nicht möglich ist und verweise auf die Zuständigkeit des Ständigen Unterausschusses des Landesverteidigungsausschusses des Nationalrats zur Überprüfung von nachrichtendienstlichen Maßnahmen.

Zu 5:

Das BMLV verfügt über eine Vielzahl an technischen und organisatorischen Kontrollmechanismen und Sicherheitssystemen, die dem hohen Schutzbedarf des Ressorts entsprechen. Darüber hinaus wurden konkrete Prozesse implementiert, um Sicherheitsvorfälle effizient und effektiv abwehren zu können. Allfällige und weitere Maßnahmen des BMLV im Sinne der Fragestellung sind im Interesse der Umfassenden Landesverteidigung aus Gründen der Amtsverschwiegenheit (Art. 20 Abs. 3 B-VG) nicht geeignet, im Rahmen einer parlamentarischen Anfragebeantwortung öffentlich erörtert zu werden.

Zu 6:

Mit der Einführung des Gehaltsschemas RIVIT, speziell für IT-Fachexperten und -expertinnen, wurde ein positiver Schritt für die Attraktivierung des Arbeitsgebers Bund und eine angemessene Entlohnung gesetzt.

Zu 7 und 7a:

Da Cybersicherheit eine gesamtstaatliche Querschnittsmaterie ist, sind wirksame Koordinierungsstrukturen und gesamtstaatliche kooperative Modelle notwendig. Diese ergeben sich aus den gesetzlichen Grundlagen und Zuständigkeitsbereichen sowie etablierten sektor- und ressortübergreifenden Gremien, Plattformen und Koordinierungsstrukturen und sind in der Österreichischen Strategie für Cybersicherheit 2021 geregelt. Die strategische Koordination im Bereich Cybersicherheit obliegt dem Bundeskanzleramt (BKA) und wird beispielsweise im Rahmen der Cyber-Sicherheit-Steuerungsgruppe (CSS), bei der u.a. alle Sicherheitsressorts (BKA, BMI, BMEIA, BMLV) vertreten sind, wahrgenommen. Darüber hinaus erfolgt ein wöchentlicher Austausch der Sicherheitsressorts auf technisch-operativer Ebene im Inneren Kreis der Operativen Koordinierungsstruktur (IKDOK); federführend ist dabei das BMI.

Zu 8, 8a und 8b:

Aufbauend auf dem Strategischen Kompass wurde im Mai 2023 die Cyber Defence Policy der EU beschlossen, die festhält, welche Cyber-Fähigkeiten der EU sowie der EU-Mitgliedstaaten im Bereich der Cyber-Sicherheit und -Verteidigung durch Kapazitätenaufbau und neuen Kooperationsmechanismen gestärkt werden sollen. Zur Umsetzung der Cyber Defence Policy wurde im Juli 2023 der Implementierungsplan veröffentlicht, der 46 Maßnahmen beinhaltet und sich derzeit in der Umsetzungsphase befindet. Für die Koordinierung der Umsetzung im Rahmen der österreichischen Landesverteidigung liegt die Zuständigkeit beim BMLV. Aktive Beteiligung durch das BMLV an derzeitigen Projekten zur Umsetzung der Cyber Defence Policy beinhalten den Aufbau eines EU-Cyber-Lagezentrums, die Implementierung von Cyber Rapid Response Teams (CRRT) auf EU-Ebene und die Vernetzung von militärischen CERTs aller EU-Mitgliedstaaten. Darüber hinaus ist die Schaffung gemeinschaftlicher Standards und Zertifizierungen sowie ein Investment in Forschung, Entwicklung und Aufbau von Fähigkeiten der Union zum Schutz des EU-Cyber-Raums wichtiger Schwerpunkt. Jegliche Stärkung der Cybersicherheit der EU bedeutet auch eine Stärkung der österreichischen Cybersicherheit, weshalb alle Maßnahmen im Rahmen der Umsetzung der Europäischen Cybersicherheitsstrategie zu unterstützen sind.

Zu 9:

Eine Ermittlung der Budgetmittel für den spezifischen Bereich der Cyberdefense über die angefragten Zeiträume würde einen außergewöhnlich hohen, nicht zu rechtfertigenden

Verwaltungsaufwand erfordern. Aus diesem Grund ersuche ich um Verständnis, dass eine Beantwortung dieser Fragen nicht möglich ist.

Mag. Klaudia Tanner

REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR LANDESVERTEIDIGUNG @ AMTSSIGNATUR	**Unterzeichner**	Bundesministerium für Landesverteidigung
	Datum/Zeit-UTC	2024-05-27T06:50:22+02:00
	Prüfinformation	Informationen zur Prüfung der elektronischen Signatur bzw. des Ausdrucks finden Sie unter: http://www.bmlv.gv.at/amtssignatur
Hinweis	Dieses Dokument wurde amtssigniert. Auch ein Ausdruck dieses Dokuments hat gemäß § 20 E-Government-Gesetz die Beweiskraft einer öffentlichen Urkunde.	

	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2024-05-27T06:55:04+02:00
Prüfinformation	Dieses Dokument wurde elektronisch besiegelt. Informationen zur Prüfung des elektronischen Siegels und des Ausdrucks finden Sie unter: https://www.parlament.gv.at/siegel	