MAG. KLAUDIA TANNER
BUNDESMINISTERIN FÜR LANDESVERTEIDIGUNG

S91143/51-PMVD/2026 27. Mai 2026

Herrn
Präsidenten des Nationalrates

Parlament
1017 Wien

Die Abgeordneten zum Nationalrat Zorba, Freundinnen und Freunde haben am 27. März 2026 unter der Nr. 5491/J an mich eine schriftliche parlamentarische Anfrage betreffend „Cybersicherheitsvorfälle und -maßnahmen in den Bundesministerien“ gerichtet. Diese Anfrage beantworte ich wie folgt:

Zu 1 bis 1b:

Das Bundesministerium für Landesverteidigung (BMLV) ist durchgehend Ziel des gesamten Spektrums von Cyberangriffen, welche regelmäßig durch die Cybersicherheitsexperten und Sicherheitssysteme des Militärischen Cyberzentrums (MilCyZ) abgewehrt werden. Eine vollständige Aufzählung von Art und Umfang der Angriffe kann aus Gründen der militärischen Sicherheit hier nicht bereitgestellt werden. Hinsichtlich der Ermittlungsergebnisse und Strafverfolgungsmaßnahmen darf an das Bundesministerium für Inneres und das Bundesministerium für Justiz verwiesen werden.

Zu 2 und 2a:

Das Österreichische Bundesheer (ÖBH) muss aufgrund der Aufgaben der militärischen Landesverteidigung, insbesondere im Cyberraum, in der Lage sein, Angriffe selbstständig im gesamten Cyber-Bedrohungsspektrum abwehren zu können. Dafür ist es erforderlich, die eigenen Mitarbeiter bestmöglich auszubilden und über aktuelle Bedrohungen zu informieren. Darüber hinaus verfügt das MilCyZ über kompetente und verlässliche Milizexperten, welche meist selbst einen „Expertenstatus“ in der Privatwirtschaft genießen und im Bedarfsfall ebenfalls aktiviert werden können. Das Hinzuziehen von externen Experten erfolgt nur vereinzelt im Bedarfsfall. Weitere Zusammenarbeit mit externer Expertise ergeht im Zuge von Kooperationen mit Fachhochschulen und Universitäten und erfolgt im Regelfall im Zusammenhang mit Beratungsleistungen, Forschungsprojekten und der Entwicklung von Sicherheitslösungen.

Zu 2b bis 2d, 4b, 4c und 5:

Da eine detaillierte Erörterung von Sicherheitsmaßnahmen für verfassungsmäßige Einrichtungen im Rahmen einer parlamentarischen Anfrage dem Interesse der Staatssicherheit und der militärischen Landesverteidigung zuwiderlaufen würde, ersuche ich um Verständnis, dass eine Beantwortung dieser Fragen nicht möglich ist.

Zu 3:

Ja, in meinem Ressort gibt es regelmäßige Überprüfungen der Cyberbedrohungen. Diese werden durch Risikoanalysen für sämtliche klassifizierten Systeme sowie im Bedarfsfall auch für nicht-klassifizierte Systeme durchgeführt. Die daraus resultierenden Ergebnisse werden in regelmäßigen Abständen im Rahmen der Maßnahmenverfolgung überprüft und entsprechend behördlich geteilt.

Zu 4 und 4a:

Das MilCyZ bildet den Kern der Cyberverteidigungsfähigkeit (Cyber Defence) des ÖBH in den Bereichen IKT-Sicherheit und Cyber-Operations. Dem Bereich des MilCyZ kommen die Aufgaben für das Cyber Sicherheitsmanagement, die Cyber Sicherheitstechnik und Konzepte sowie Informationssicherheit zu. Zusätzlich verfügt dieses Zentrum über Einheiten für Elektronische Kampfführung sowie die Cyber- Sicherheitsoperationszentrale und bildet mit seinen Fähigkeiten das zentrale Cyber-Verteidigungselement des Ressorts. Die Funktion „Cybersicherheitsbeauftragter“ im Sinne der Fragestellung entspricht in etwa der Funktion des Chief Information Security Officer (CISO) des BMLV.

Zu 6, 6a und 6b:

Die Mitarbeiterinnen und Mitarbeiter des BMLV haben eine jährliche, laufend angepasste und aktualisierte IKT-Sicherheitsbelehrung zu absolvieren. Darüber hinaus werden anlassbezogen bezugnehmend auf Bedrohungen sowie Verhaltensempfehlungen zur Gefahrenvermeidung bzw. -abwehr Warn- und Informationsschreiben in Umlauf gebracht. Eine Benennung von Kosten für derartige Schulungen kann aufgrund der budgetären Strukturierung nicht vorgenommen werden. Eine Ermittlung der gewünschten Daten 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	2026-05-27T06:56:55+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.	

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2026-05-27T07:01:39+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	