18194/AB
vom 12.08.2024 zu 18837/J (XXVII. GP)

MAG. KLAUDIA TANNER
BUNDESMINISTERIN FÜR LANDESVERTEIDIGUNG

S91143/77-PMVD/2024 12. August 2024

Herrn
Präsidenten des Nationalrates

Parlament

1017 Wien

Die Abgeordneten zum Nationalrat Ecker, MBA, Kolleginnen und Kollegen haben am 12. Juni 2024 unter der Nr. 18837/J an mich eine schriftliche parlamentarische Anfrage betreffend „Mögliche Hackerangriffe auf Ihr Ministerium" gerichtet. Diese Anfrage beantworte ich wie folgt:

Zu 1 und 1a:

Angriffe bzw. Angriffsversuche können nie ausgeschlossen werden. Im Fall eines erfolgreichen Angriffs ist jedoch das Bundesministerium für Landesverteidigung (BMLV) durch entsprechende Verfahren zur Erkennung und Reaktion auf verschiedene Szenarien vorbereitet, sodass Maßnahmen zur raschen Eindämmung und Bereinigung der betroffenen Systeme ergriffen werden können.

Zu 2, 2a und 2b:

Ja, es gab derartige Angriffe. Ich ersuche um Verständnis, dass eine weiterführende Beantwortung dieser Fragen aus Gründen der Amtsverschwiegenheit im Interesse der umfassenden Landesverteidigung gemäß Art. 20 Abs. 3 B-VG nicht möglich ist.

Zu 3:

Zur Sicherstellung der Datensicherheit gelangen als Grundschutz Maßnahmen nach Maßgabe von „best practices" und nach dem Stand der Technik zur Anwendung. In sensiblen Bereichen, wie dem Datenschutz bzw. Geheimschutz, werden in meinem Ressort auch darüber hinausgehende Maßnahmen ergriffen.

Zu 4, 4a und 4b:

Dazu verweise ich auf die Ausführungen in Beantwortung der parlamentarischen Anfragen Nr. 11856/J (Nr. 11519/AB) durch den Bundesminister für Inneres und Nr. 18802/J durch den Bundeskanzler.

Zu 5 und 6:

Das BMLV setzt mehrere Sicherheitssysteme ein, die im Rahmen von Analysen der aktuellen und absehbaren Bedrohungslagen laufend angepasst werden. Durch Re-evaluierungen und Überprüfungen geeigneter Technologien wird zudem sichergestellt, dass nicht mehr zeitgemäße Sicherheitssysteme gegen neue Anwendungen ausgetauscht werden.

Zu 7:

Für derartige Vorfälle ist ein Notfallprozess vorgesehen, der den Informationsfluss zwischen den Entscheidungsträgern und die Implementierung von Krisenstäben regelt. Konkret werden erfolgreiche Angriffe vom Militärischen Computer Emergency Readiness (MilCERT) Team behandelt.

Zu 8, 8a und 8b:

Zur Vorbereitung der Abwehr von Cyber-Angriffen finden verschiedene nationale und internationale Übungen in Abständen von einigen Wochen bis Monaten statt. Abhängig von der jeweiligen Übung liegt der Rahmen zwischen ein bis zwei Personentagen und Wochen. Es werden dabei sowohl technische Cyberübungen als auch Notkommunikationsübungen zur Aufrechterhaltung der Führungsfähigkeit des Österreichischen Bundesheeres (ÖBH) bei Ausfall sämtlicher Standardkommunikationsmittel (wie etwa im Fall eines Blackouts) durchgeführt. Diese Notkommunikationsübungen finden regional bzw. bundesweit mehrmals pro Jahr statt.

Zu 8c:

Entfällt.

Zu 9:

Die Einsatzfähigkeit des ÖBH ist durch Überbrückungsmaßnahmen bis zur Verfügbarkeit eines umfassenden Notkommunikationsnetzes sichergestellt.

Mag. Klaudia Tanner

	Unterzeichner	Bundesministerium für Landesverteidigung
	Datum/Zeit-UTC	2024-08-12T07:10:48+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	2024-08-12T07:14:12+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	