3131/J
vom 12.08.2025 (XXVIII. GP)

Anfrage

der Abgeordneten Süleyman Zorba, Freundinnen und Freunde

an die Bundesministerin für Landesverteidigung

betreffend IT- und Cybersicherheit im Bundesministerium für Landesverteidigung sowie bei Mitarbeiter:innen in Schlüsselpositionen

BEGRÜNDUNG

In den vergangenen Jahren haben sich vermehrt Hinweise auf Cyberangriffe gegen staatliche Einrichtungen und deren Bedienstete ergeben. Auch im diplomatischen Bereich sind Fälle bekannt geworden, bei denen Dienstgeräte kompromittiert und vertrauliche Informationen unbefugt erlangt wurden. Um solchen Vorfällen vorzubeugen, bedarf es klarer Richtlinien zur Nutzung von dienstlichen Geräten, regelmäßiger Sicherheitsüberprüfungen sowie ausreichender personeller und finanzieller Ressourcen.

Die Abwehrfähigkeit gegenüber Cyberangriffen ist essenziell, um staatliche Souveränität und das Vertrauen in die Institutionen zu wahren. Ministerien und deren Mitarbeiter:innen verfügen über sensible Informationen, die bei unzureichender Absicherung erhebliche sicherheits- und außenpolitische Folgen nach sich ziehen können.

Insbesondere im Lichte eines medial bekannt gewordenen Vorfalls aus dem Jahr 2025, bei dem Kommunikationsdaten eines österreichischen Diplomaten abgeflossen sind[1], besteht ein öffentliches Interesse an der Klärung der bestehenden Sicherheitsmechanismen und Vorsorgemaßnahmen in den Ministerien.

Die unterfertigenden Abgeordneten stellen daher folgende

ANFRAGE

1. Welche verbindlichen Richtlinien bestehen derzeit in Ihrem Haus zur sicheren Nutzung dienstlicher IT Geräte (Smartphones, Laptops, Tablets) durch Mitarbeiter:innen?

[1] https://www.derstandard.at/story/3000000282225/diensthandy-des-eu-botschafters-in-bruessel-wurde-ausgespaeht

2. Gibt es gesonderte Vorgaben für den Umgang mit vertraulichen Informationen auf mobilen Geräten, insbesondere hinsichtlich Verschlüsselung, Zwei Faktor Authentifizierung und Speicherung sensibler Daten?

3. In welchen zeitlichen Abständen werden Sicherheitsüberprüfungen oder Audits der dienstlichen IT Geräte durchgeführt, sowohl im Inland als auch bei im Ausland tätigen Mitarbeiter:innen?

a) Wie oft finden diese Audits im Durchschnitt pro Jahr statt?

b) Welche internen oder externen Stellen führen diese Audits durch?

4. Werden Diensthandys oder andere mobile Geräte auf Reisen in Länder mit erhöhtem Spionagerisiko durch „Burner Phones" oder andere Einweggeräte ersetzt?

a) Wenn ja, seit wann gilt diese Praxis und für welche Destinationen?

5. Welche Maßnahmen bestehen, um das Risiko der Nutzung unsicherer öffentlicher Netzwerke (z. B. Hotel WLANs) durch Mitarbeiter:innen zu minimieren?

6. Wie werden die Mitarbeiter:innen in Fragen der IT Sicherheit geschult?

a) Gibt es verpflichtende Schulungen für alle Beschäftigten?

b) In welchen zeitlichen Abständen werden diese Schulungen angeboten?

c) Werden Sondertrainings für besonders exponierte Funktionen oder Mitarbeiter:innen in Schlüsselpositionen durchgeführt?

7. Welche Abteilungen oder Teams sind innerhalb Ihres Hauses für IT Sicherheit und Cyberabwehr zuständig?

a) Wie viele Planstellen sind aktuell für diesen Bereich vorgesehen?

b) Wie viele davon sind mit qualifiziertem Personal besetzt?

8. Wie hoch war das jährliche Budget Ihres Ressorts für IT- und Cybersicherheit in den letzten fünf Jahren (bitte nach Jahren aufschlüsseln)?

9. Gibt es eine regelmäßige Evaluierung der vorhandenen Sicherheitsstandards unter Einbeziehung externer Sicherheits- und Datenschutzexperten? Wenn ja, wann fand die letzte Evaluierung statt und welche Ergebnisse wurden daraus abgeleitet?

10. Wurden nach Bekanntwerden des eingangs erwähnten Sicherheitsvorfalls im Jahr 2025 konkrete Maßnahmen gesetzt, um ähnliche Fälle künftig zu verhindern?

a) Wenn ja, welche?

11. Inwieweit arbeitet Ihr Haus mit nationalen und internationalen Stellen (z. B. DSN, Abwehramt und HNA, CERT, EU Partner) zusammen, um sich über aktuelle Bedrohungen und Best Practices auszutauschen?

12. Gibt es Meldewege oder Whistleblower Plattformen für Mitarbeiter:innen, um Sicherheitslücken oder ungewöhnliche Vorfälle anonym zu melden?

a) Wenn ja, wie wird sichergestellt, dass diese Hinweise unverzüglich bearbeitet werden?

	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2025-09-07T14:22:42+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	