Bundesministerium
Wohnen, Kunst, Kultur,
Medien und Sport

bmwkms.gv.at

**Andreas Babler, MSc**
Vizekanzler
Bundesminister für Wohnen, Kunst, Kultur,
Medien und Sport

Herrn
Präsidenten des Nationalrates
Dr. Walter Rosenkranz
Parlament
1017 Wien

Geschäftszahl: 2026-0.279.978

Wien, 27. Mai 2026

Sehr geehrter Herr Präsident,

die Abgeordneten zum Nationalrat Süleyman Zorba und weitere Abgeordnete haben am 27. März 2026 unter der **Nr. 5493/J** an mich eine schriftliche parlamentarische Anfrage betreffend „Cybersicherheitsvorfälle und -maßnahmen in den Bundesministerien“ gerichtet.

Diese Anfrage beantworte ich nach den mir vorliegenden Informationen wie folgt:

**Zu Frage 1:**

- *Gab es in Ihrem Ressort im Jahr 2025 Cyberangriffe oder Cybersicherheits-Vorfälle?*
    a. *Falls ja, um wie viele Angriff/Vorfälle hat es sich gehandelt?*
    b. *Bei wie vielen Angriffen konnten die Täter ermittelt werden? Um welche Täter handelte es sich?*

Das Bundesministerium für Wohnen, Kunst, Kultur, Medien und Sport (BMWKMS) sieht sich – wie auch andere Ministerien, Unternehmen und Einrichtungen – kontinuierlichen Angriffsversuchen im Cyberraum ausgesetzt. Im Jahr 2025 erfolgten mehrere Überlastungsangriffe auf IT-Verfahren, sogenannte Distributed Denial of Service (DDoS) – Angriffe, in der Dauer von wenigen Minuten bis mehrere Stunden. Die Angriffe konnten

aufgrund der getroffenen technischen und organisatorischen Maßnahmen erfolgreich abgewehrt werden. Das BMWKMS meldet Cyberangriffe den zuständigen Strafverfolgungsbehörden. Die Strafverfolgung von Cyberkriminalität fällt jedoch nicht in den Zuständigkeitsbereich des BMWKMS. In Bezug auf Ermittlungsergebnisse darf daher auf das dafür zuständige Bundesministerium verwiesen werden.

**Zu den Fragen 2 und 3:**

- *Welche Präventionsmaßnahmen wurden von Ihrem Ministerium im vergangenen Jahr ergriffen, um sich vor Cyberangriffen und -kriminalität zu schützen?*
    a. *Arbeiten Sie mit externen Expertinnen und Experten im Bereich Cybersicherheit zur Verhinderung von Cyberangriffen zusammen?*
    b. *Wenn ja, um welche Experten handelte es sich im Jahr 2025?*
    c. *Wie erfolgte die Auswahl?*
    d. *Arbeiten Sie mit externen Unternehmen im Bereich Cybersicherheit zur Verhinderung von Cyberangriffen zusammen? Wenn ja, mit welchen?*
- *Gab es in Ihrem Ressort Risikoanalysen im Hinblick auf Cyberbedrohungen im Jahr 2025 und welche Ergebnisse brachten diese Analysen?*

Der Schutz der verarbeiteten Daten sowie der eingesetzten IT-Services und IKT-Infrastrukturkomponenten stellt einen wesentlichen Bestandteil der organisatorischen und technischen Sicherheitsvorkehrungen im Ressort dar.

In diesem Zusammenhang wurde im BMWKMS im dritten Quartal 2025 eine GAP-Analyse auf Basis des Security Framework Bund 2 (SFB 2) durchgeführt. Um die seitens des Rechnungshofs empfohlene Überprüfung unter Einbeziehung von externem Fachwissen sicherstellen zu können, wurde die TÜV TRUST IT TÜV AUSTRIA GMBH beauftragt. Die Beauftragung erfolgte im Rahmen eines Abrufs über die Bundesbeschaffung GmbH (BBG). Auf Grundlage der Ergebnisse dieser Analyse wurde in weiterer Folge ein Projekt zur Weiterentwicklung der IT-Sicherheit initiiert.

Darauf aufbauend wurde das interne Managementsystem weiterentwickelt, um den aktuellen Anforderungen gemäß Netz- und Informationssystemsicherheitsgesetzes 2026 (NISG 2026) sowie den einschlägigen ISO-Standards gerecht zu werden. Das auf dieser Basis entwickelte Informationssicherheits-Managementsystem (ISMS) orientiert sich nach den internationalen Standards ISO/IEC 27001 und berücksichtigt die geltenden rechtlichen Rahmenbedingungen.

Das ISMS dient insbesondere der strukturierten Identifikation und Bewertung bestehender Risiken sowie der Umsetzung geeigneter technischer und organisatorischer Maßnahmen unter Berücksichtigung des jeweiligen Stands der Technik in den Bereichen Prävention, Erkennung und Reaktion. Ergänzend dazu wird, entsprechend den Vorgaben des ISMS sowie im Hinblick auf die Anforderungen des NISG, ein strukturiertes Risikomanagementsystem aufgebaut, das der systematischen Durchführung von Risikoanalysen sowie der frühzeitigen Identifikation und Behandlung sicherheitsrelevanter Bedrohungen dient. Dementsprechend werden laufend Risikoanalysen im BMWKMS durchgeführt.

Im Rahmen des Projekts wurde darüber hinaus eine Vielzahl weiterer Maßnahmen zur präventiven Stärkung der Informationssicherheit umgesetzt. So wurde eine Informationssicherheitsorganisation eingerichtet, bestehend aus Expert:innen insbesondere in den Bereichen Schutz klassifizierter Informationen, Datenschutz sowie allgemeine Sicherheitsangelegenheiten. Dieses Gremium tagt regelmäßig und berät die oberste Leitung in Fragen der Informationssicherheit.

Im Bereich der Cybersicherheit fungiert die BRZ GmbH als zentrale Ansprechpartnerin für Sicherheitsvorfälle und unterstützt bei der Eindämmung möglicher Bedrohungen bzw. Angriffe. Darüber hinaus ist vorgesehen, die Wirksamkeit der gesetzten Maßnahmen regelmäßig sowie anlassbezogen zu überprüfen und zu evaluieren.

**Zu Frage 4:**

- *Gibt es in Ihrem Ministerium Cybersicherheitsbeauftragte?*
    a. *Welche Abteilungen oder Teams waren im Jahr 2025 innerhalb Ihres Ministeriums dafür zuständig?*
    b. *Wie viele Personen waren in Ihrem Ministerium im Jahr 2025 im Bereich Cyber- und IT-Sicherheit tätig?*
    c. *Welche konkreten Aufgaben nahmen diese Personen wahr?*

Im BMWKMS wird diese Rolle durch den Chief Information Security Officer (CISO) wahrgenommen. Für das Management der Informationssicherheit – darunter fallen auch die IT- und Cybersicherheit – waren im Jahr 2025 die Abteilung I/A/8 sowie das Referat I/A/8/b – IT zuständig. Es darf in diesem Zusammenhang auf die für diesen Zeitraum gültige Geschäfts- und Personaleinteilung des BMWKMS verwiesen werden. Der Aufgabenbereich umfasst im Wesentlichen die Organisation, die kontinuierliche Evaluierung und die Weiterentwicklung der informationssicherheitsrelevanten Prozesse und Regelungen des Ressorts, die Überprüfung der Normkonformität iZm dem

Sicherheitsstandard ISO 27001 sowie den Betrieb und die Weiterentwicklung des ISMS des BMWKMS.

**Zu Frage 5:**

- *Wie hoch war das Budget Ihres Hauses für IT- und Cybersicherheit im Jahr 2025?*

Da IT- und Cybersicherheit eine Querschnittsmaterie darstellen, sind die damit verbundenen Aufwände und Kosten nicht eindeutig zuordenbar.

**Zu Frage 6:**

- *Gab es im Jahr 2025 konkrete verpflichtende Schulungsangebote in Fragen der IT- und Cybersicherheit für Mitarbeiter:innen Ihres Hauses sowie nachgeordneter Dienststellen?*
    a. *Wenn ja, um welche Schulungsangebote handelte es sich?*
    b. *Wie hoch waren die Kosten für diese Schulungen?*

Im BMWKMS erfolgt die Schulung hinsichtlich der geltenden Regelungen im Zusammenhang mit der Informationssicherheit und dem Datenschutz sowie die Sensibilisierung im Zusammenhang mit relevanten Cyberrisiken sowohl in Präsenz als auch online über unterschiedliche Kanäle, insbesondere über das Intranet sowie per E-Mail. Im Rahmen des Bildungsprogramms der Verwaltungsakademie des Bundes werden umfassende Aus-, Fort- und Weiterbildungsmaßnahmen für diesen Bereich angeboten. Das Intranet wird genutzt, um über laufende Kampagnen zu informieren, auf neue Schulungsangebote hinzuweisen und durch konkrete Handlungsempfehlungen, etwa zum sicheren Umgang mit Smartphones, weiter zu sensibilisieren.

Andreas Babler, MSc

| | | |
|---|---|---|
| REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR WOHNEN, KUNST, KULTUR, MEDIEN UND SPORT @ AMTSSIGNATUR | Unterzeichner | Bundesministerium für Wohnen, Kunst, Kultur, Medien und Sport |
| | Datum/Zeit | 2026-05-27T10:50:58+02:00 |
| | Aussteller-Zertifikat | CN=a-sign-corporate-07,OU=a-sign-corporate-07,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT |
| | Serien-Nr. | 479679199 |
| | Hinweis | Dieses Dokument wurde amtssigniert. |
| | Prüfinformation | Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: http://www.signaturpruefung.gv.at |

| | | |
|---|---|---|
| | **Unterzeichner** | Parlamentsdirektion |
| | **Datum/Zeit-UTC** | 2026-05-27T10:55:37+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 | |