5627/AB
vom 31.07.2026 zu 6216/J (XXVIII. GP)

Bundesministerium Finanzen

bmf.gv.at

Dr. Markus Marterbauer
Bundesminister für Finanzen

Johannesgasse 5, 1010 Wien

Herrn Präsidenten
des Nationalrates
Dr. Walter Rosenkranz
Parlament
1017 Wien

Geschäftszahl: 2026-0.467.696

Wien, 31. Juli 2026

Sehr geehrter Herr Präsident!

Auf die schriftliche parlamentarische Anfrage Nr. 6216/J vom 1. Juni 2026 der Abgeordneten Rosa Ecker, MBA, Kolleginnen und Kollegen beehre ich mich Folgendes mitzuteilen:

Zu Frage 1, 2, 4 und 5

1. Wie beurteilen Sie die aktuelle Gefahr, dass Hackerangriffe gegen Ihr Ressort vorgenommen werden und gelingen könnten?

2. Inwieweit ist Ihr Ressort auf mögliche Hackerangriffe vorbereitet?

4. Wie wird seitens Ihres Ressorts aktuell für die Datensicherheit gesorgt?

5. Wer kann wie auf die von Ihnen verarbeiteten Daten aktuell zugreifen?

Cyberangriffe auf IT-Verfahren und IKT-Infrastrukturkomponenten können nie generell ausgeschlossen werden. Für das Bundesministerium für Finanzen (BMF) hat der Schutz der verarbeiteten Daten und der dafür eingesetzten IT-Verfahren und IKT-Infrastrukturkomponenten eine hohe Priorität. Das BMF verfügt daher über ein

kombiniertes Informationssicherheits- und Datenschutz-Managementsystem, welches regelmäßig nach den internationalen Sicherheitsstandards ISO/IEC 27001 und ISO/IEC 27701 überprüft wird.

Das Managementsystem sorgt unter anderem dafür, dass die diesbezüglich geltenden Rechtsvorschriften eingehalten und bestehende Risiken systematisch identifiziert, beurteilt und mittels geeigneten technischen und organisatorischen Maßnahmen nach dem Stand der Technik in den Bereichen Prävention, Erkennung und Reaktion reduziert werden. Es sieht darüber hinaus vor, dass die Wirksamkeit der Maßnahmen sowohl regelmäßig als auch im Anlassfall überprüft, bewertet und evaluiert wird. Zugriffsberechtigungen erfolgen nach dem Bedarfsprinzip unter Berücksichtigung der Sensibilität der Daten.

Die öffentlich verfügbaren Sicherheitsstandards ISO/IEC 27001 (Informationssicherheits-Management) und ISO/IEC 27701 (Datenschutz-Management) spezifizieren dafür umfassende Anforderungs- bzw. Maßnahmenkataloge. Im Hinblick auf die Sicherung der Effektivität der Schutzmaßnahmen muss jedoch von einer detaillierten Bekanntgabe Abstand genommen werden.

Zu Frage 3

Gab es im Jahr 2025 sogenannte „Überlastungsangriffe" oder andere abgewehrte Angriffe?

a. Wenn ja, wann?

b. Wenn ja, in welchem Umfang?

c. Wenn ja, kennen Sie den Ursprung dieser Hacking-Angriffe?

Im Jahr 2025 erfolgten mehrere sogenannte Distributed Denial of Service (DDoS) Angriffe auf IT-Verfahren und IKT-Infrastrukturkomponenten des BMF in der Dauer von wenigen Minuten bis mehreren Stunden. Aufgrund der getroffenen technischen und organisatorischen Maßnahmen konnten die Angriffe erfolgreich abgewehrt werden. Das BMF meldet Cyberangriffe den zuständigen Strafverfolgungsbehörden. Die Strafverfolgung von Cyberkriminalität fällt jedoch nicht in den Zuständigkeitsbereich des BMF.

Zu Frage 6

Konnten im Jahr 2025 durch Ihr Ressort Datenlecks festgestellt werden?

a. Wenn ja, wie konnte es dazu kommen?

b. Wenn ja, welche Daten waren betroffen?

Seitens des BMF konnten zuletzt keine Datenlecks festgestellt werden.

Zu Frage 7 bis 9

7. Welche internen/externen Sicherheitssysteme überwachen derzeit die vorhandenen Daten, Betriebssysteme und elektronischen Einheiten?

a. Wie hoch sind die aktuellen jährlichen Kosten hierfür (Einkauf, Installation, Wartung, Betreuung, Ausbau etc.)?

b. Welche Kosten sind 2025 entstanden?

8. In welchem zeitlichen Abstand werden diese Sicherheitssysteme auf die neuesten Entwicklungen und Bedrohungen angepasst und adaptiert?

9. Wer ist mit der Instandhaltung der ministeriellen Sicherheitssysteme beauftragt?

Im BMF werden basierend auf erfolgten Risikobewertungen und Bedrohungsanalysen unterschiedliche Sicherheitssysteme zum Einsatz gebracht. Der Betrieb dieser Systeme erfolgt durch die Bundesrechenzentrum GmbH. Da IT- und Cybersicherheit eine Querschnittsmaterie darstellen, sind die damit verbundenen Aufwände und Kosten nicht eindeutig zuordenbar. Neben technischen Maßnahmen zum Update und Upgrade bestehender Systeme erfolgt zyklisch eine risikobasierte Beurteilung auf zum Einsatz zu bringende Sicherheitssysteme hin. Im Hinblick auf die Sicherung der Effektivität der Schutzmaßnahmen muss jedoch von einer detaillierten Bekanntgabe Abstand genommen werden.

Zu Frage 10

10. Wie ist die derzeitige Vorgabe im Umgang mit Hacking-Angriffen?

a. Ist diese Vorgehensweise in allen Resorts einheitlich?

b. Wie oft werden derartige Szenarien durchgespielt und Vorkehrungen getroffen?

Das Netz- und Informationssystemsicherheitsgesetz (NISG) regelt Grundsätzliches, die Ministerien regeln das organisationsspezifische Vorgehen im eigenen Verantwortungsbereich. Das BMF verfügt über einen Notfallplan, der die einzuleitenden Maßnahmen und Zuständigkeiten bei auftretenden Vorfällen im Zusammenhang mit wesentlichen Cyberbedrohungen regelt und führt regelmäßige Notfallübungen in Form von Simulationen, Planspielen, Workshops und dergleichen durch. Im Hinblick auf die Sicherung der Effektivität der Schutzmaßnahmen muss jedoch von einer detaillierten Bekanntgabe Abstand genommen werden.

Der Bundesminister:
Dr. Markus Marterbauer

Elektronisch gefertigt

Bundesministerium Finanzen	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at Informationen zur Prüfung des Ausdrucks finden Sie unter: https://www.bmf.gv.at/verifizierung
	Datum/Zeit	2026-07-31T15:43:05+02:00
Unterzeichner	Bundesministerium für Finanzen	
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.	874736968	
Dokumentenhinweis	Dieses Dokument wurde amtssigniert.	

	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2026-07-31T15:55:26+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	