Bundesministerium
Land- und Forstwirtschaft,
Klima- und Umweltschutz,
Regionen und Wasserwirtschaft

bmluk.gv.at

Mag. Norbert Totschnig, MSc
Bundesminister für Land- und Forstwirtschaft,
Klima- und Umweltschutz,
Regionen und Wasserwirtschaft

Herrn
Dr. Walter Rosenkranz
Präsident des Nationalrats
Parlament
1017 Wien

Geschäftszahl: 2026-0.472.753

Ihr Zeichen: 6211/J-NR/2026

Wien, 31. Juli 2026

Sehr geehrter Herr Präsident,

die Abgeordneten zum Nationalrat Rosa Ecker, MBA, Kolleginnen und Kollegen haben am 1. Juni 2026 unter der Nr. **6211/J** an mich eine schriftliche parlamentarische Anfrage betreffend „Hacking-Angriffe auf Ministerien – Daten 2025“ gerichtet.

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

Zu den Fragen 1 und 2:

- Wie beurteilen Sie die aktuelle Gefahr, dass Hackerangriffe gegen Ihr Ressort vorgenommen werden und gelingen könnten?
- Inwieweit ist Ihr Ressort auf mögliche Hackerangriffe vorbereitet?

Im Bundesministerium für Land- und Forstwirtschaft, Klima- und Umweltschutz, Regionen und Wasserwirtschaft (BMLUK) werden laufend organisatorische und technische Maßnahmen gesetzt, um die Cybersicherheit zu erhöhen und einen angemessenen Schutz vor Cyberangriffen und Cyberkriminalität sicherzustellen. Dabei arbeitet das BMLUK auch mit externen Fachleuten zusammen. Zudem fließen Erkenntnisse aus dem gesamtstaatlichen Cyber-Lagebildprozess in die Sicherheitsmaßnahmen ein und werden in enger Zusammenarbeit mit dem technischen Personal des BMLUK zeitnah bewertet und

umgesetzt. Das BMLUK ist zur Abwehr solcher Versuche durch technische und organisatorische Sicherheitsmaßnahmen auf dem Stand der Technik in den Bereichen Prävention, Absicherung, Erkennung und Incident Response auf bekannte Angriffsmuster bestmöglich vorbereitet.

Zur 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?

Auch im Jahr 2025 kam es zu einer Vielzahl von Überlastungsangriffen [Distributed Denial of Service – DDoS]. Die Auswirkungen dieser Angriffe konnten durch eine Kombination aus automatisierten Schutzmaßnahmen (Mitigierung) und manuellen Eingriffen des technischen Personals minimiert werden. Allgemein wird festgehalten, dass DDoS-Angriffe mit einer Dauer von wenigen Minuten bis zu mehreren Stunden als alltägliche Bedrohungslage anzusehen sind und im Rahmen der Standardrisikobewertung berücksichtigt werden.

Die eindeutige Zuordnung des Ursprungs von DDoS-Angriffen ist aufgrund verwendeter technischer Verschleierungsmaßnahmen nicht möglich, weshalb keine gesicherten Angaben über den tatsächlichen Ursprung gemacht werden können.

Zu den Fragen 4 und 5:

- Wie wird seitens Ihres Ressorts aktuell für die Datensicherheit gesorgt?
- Wer kann wie auf die von Ihnen verarbeiteten Daten aktuell zugreifen?

Im BMLUK wird sowohl durch technische als auch durch organisatorische Maßnahmen für ein hohes Maß an Datensicherheit gesorgt. Informations- und Datensicherheit werden dabei als fortlaufender und ganzheitlicher Prozess verstanden. Auf Basis eines risikoorientierten Ansatzes werden die IKT-Sicherheitsmaßnahmen sowie die zugrundeliegenden Prozesse laufend überprüft und an aktuelle Bedrohungslagen angepasst. Darüber hinaus werden Erkenntnisse aus dem gesamtstaatlichen Cyber-Lagebildprozess laufend bewertet und in enger Zusammenarbeit mit den zuständigen Technikerinnen und Technikern des BMLUK zeitnah umgesetzt. Zugriffsberechtigungen auf Systeme und Daten erfolgen nach dem Bedarfsprinzip unter

Berücksichtigung der jeweiligen Schutzbedarfe und der Sensibilität der verarbeiteten Informationen.

Zur 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 BMLUK konnten im Jahr 2025 keine Datenlecks festgestellt werden.

Zu den Fragen 7, 8 und 10:

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

Im BMLUK werden auf Basis von Risikobewertungen, Bedrohungsanalysen und geltenden Sicherheitsvorgaben unterschiedliche technische und organisatorische Sicherheitsmaßnahmen sowie Sicherheitssysteme zum Schutz von Daten, Betriebssystemen und sonstigen informationstechnischen Komponenten eingesetzt. Neben technischen Maßnahmen zum Update und Upgrade bestehender Systeme erfolgt zyklisch eine risikobasierte Beurteilung hinsichtlich zum Einsatz zu bringender Sicherheitssysteme. Das Netz- und Informationssicherheitsgesetz 2026, BGBl. I Nr. 94/2025, regelt Grundsätzliches, die Bundesministerien regeln das organisationsspezifische Vorgehen im eigenen Verantwortungsbereich. Folglich bestehen im BMLUK Notfallpläne, die im Falle von Cyberangriffen zur Anwendung kommen.

Eine detaillierte Darstellung der eingesetzten Sicherheitssysteme, ihrer Architektur, ihres Umfangs sowie der damit verbundenen Kosten würde Rückschlüsse auf die Sicherheitsstruktur des Ressorts ermöglichen und könnte dadurch die Wirksamkeit der getroffenen Schutzmaßnahmen beeinträchtigen. Aus Gründen der Informationssicherheit

wird daher von einer näheren Bekanntgabe der eingesetzten Systeme sowie der damit verbundenen Kosten Abstand genommen.

Zur Frage 9:

- Wer ist mit der Instandhaltung der ministeriellen Sicherheitssysteme beauftragt?

Die Instandhaltung der ministeriellen Sicherheitssysteme wird von der im BMLUK zuständigen Fachabteilung sowie von autorisierten und vertraglich gebundenen Fachkräften bzw. Dienstleisterinnen und Dienstleistern wahrgenommen.

Mag. Norbert Totschnig, MSc

Bundesministerium Land- und Forstwirtschaft, Klima- und Umweltschutz, Regionen und Wasserwirtschaft	Unterzeichner	Bundesministerium für Land- und Forstwirtschaft, Klima- und Umweltschutz, Regionen und Wasserwirtschaft
	Datum/Zeit	2026-07-31T11:23:06+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.	1197990292
Hinweis	Dieses Dokument wurde amtssigniert.	
Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur und des Ausdrucks finden Sie unter: https://www.bmluk.gv.at/amtssignatur	

	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2026-07-31T11:28:02+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	