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: 2025-0.155.675

Ihr Zeichen: BKA - PDion
(PDion)568/J-NR/2025

Wien, 25. April 2025

Sehr geehrter Herr Präsident,

die Abgeordneten zum Nationalrat Michael Schnedlitz, Kolleginnen und Kollegen haben am 26. Februar 2025 unter der Nr. **568/J** an mich eine schriftliche parlamentarische Anfrage betreffend „Cyberangriffe auf österreichische Ministerien“ gerichtet.

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

Zur Frage 1:

- Gab es in Ihrem Ressort Cyberangriffe seit dem Jahr 2022?
  a. Falls ja, bitte um detaillierte Schilderung des Angriffs bzw. der Angriffe und der daraus resultierenden „Schäden".

Das Bundesministerium für Land- und Forstwirtschaft, Klima- und Umweltschutz, Regionen und Wasserwirtschaft (BMLUK) ist, so wie auch andere Bundesministerien und Unternehmen, kontinuierlichen Angriffsversuchen im Cyberraum ausgesetzt. Im BMLUK konnten bisher derartige Angriffsversuche sowie Schäden und Ausfälle erfolgreich von den eigenen Schutzsystemen abgewehrt werden. Aus Gründen der IT-Sicherheit des Ressorts können nähere Details nicht bekannt gegeben werden.

Zu den Fragen 2, 4 und 7:

- Gibt es konkrete Pläne, sich für den Ernstfall eines potenziellen Cyberangriffs zu schützen?
- Welche konkreten Maßnahmen werden aktiv von Ihrem Ministerium ergriffen, um sich präventiv gegen Cyberattacken und gegen Cyberkriminalität zu schützen?
- Welche konkreten Maßnahmen setzen Sie, um den spezifischen Risiken Ihres Ministeriums gerecht zu werden?

Im BMLUK werden zur Erhöhung der Cybersicherheit Maßnahmen getroffen, um sich angemessen vor Cyberattacken und Cyberkriminalität zu schützen. Das BMLUK arbeitet dafür auch mit externen Fachleuten zusammen. Weiters fließen die Erkenntnisse aus dem gesamtstaatlichen Lagebildprozess mit ein und werden gemeinsam mit dem technischen Personal des BMLUK zeitnahe umgesetzt. Aus Gründen der IT-Sicherheit können nähere Details nicht bekannt gegeben werden.

Zur Frage 3:

- Welche Rolle und welche konkreten Aufgaben fallen Ihrem Ressort in der gesamtstaatlichen Bekämpfung von Cyberkriminalität zu?

Die Aufgabenwahrnehmung zur Bekämpfung der Cyberkriminalität obliegt dem Bundesministerium für Inneres.

Zur Frage 5:

- Welche Rolle spielen externe Experten in der Vorbereitung und im Schutz gegen potenzielle Cyberangriffe?
  a. Welche Art von Experten wird hier beigezogen und warum?

Externe Fachleute können vorhandene Schwachstellen aufdecken, Sicherheitsmaßnahmen entwickeln und im Krisenfall beratend unterstützen. Ihre unabhängige Expertise ergänzt internes Wissen und ermöglicht eine objektive Sicherheitsbewertung nach internationalen Standards.

Anlassbezogen werden externe IT-Fachleute hinzugezogen, um gezielt Prävention, Schulung, Notfallmanagement und Krisenbewältigung zu gewährleisten.

Zur Frage 6:

- Gab es in Ihrem Ressort eigene Risikoanalysen?
  a. Falls ja, welche?

b. Falls nein, warum nicht?

Das BMLUK betreibt ein Informations-Sicherheits-Management-System nach „best practice“ und führt in diesem Umfang Risikoanalysen und zyklisch eine Schutzbedarfsanalyse durch.
Darüber hinaus darf auf die Beantwortung die Fragen 2, 4 und 7 verwiesen werden.

Zur Frage 8:

- Gibt es so etwas wie „Cybersicherheitsbeauftragte" in Ihrem Ministerium?
  a. Wenn ja, wie viele Personen sind zum Zeitpunkt der Beantwortung dafür vorgesehen?
  b. Wenn ja, über welche Expertise verfügt diese Person/ verfügen diese Personen?
  c. Wenn ja, was sind die konkreten Aufgaben dieser Person/Personen?
  d. Wenn nein, warum nicht?

Innerhalb des BMLUK werden diese Agenden vom Chief-Information-Security-Officer des BMLUK, in enger Zusammenarbeit und Abstimmung mit dem Abteilungsleiter der IKT-Abteilung und Chief-Information-Officer sowie dem Chief-Digital-Officer des Ressorts wahrgenommen. Aus Gründen der Aufrechterhaltung eines hohen Schutzniveaus innerhalb des BMLUK wird von einer näheren Beschreibung der Expertise Abstand genommen.

Zu den Fragen 9 und 10:

- Welche Maßnahmen wurden ergriffen, um alle Mitarbeitenden in Ihrem Ministerium gegen die drohende Gefahr von Cyberangriffen zu sensibilisieren?
- Welche Maßnahmen werden in Zukunft ergriffen bzw. sind geplant, um alle Mitarbeitenden in Ihrem Ministerium gegen die drohende Gefahr von Cyberangriffen zu sensibilisieren?

Im BMLUK werden für Mitarbeiterinnen und Mitarbeiter zyklisch Awareness-Schulungen durchgeführt, aber auch sonstige Bewusstseinsbildungsmaßnahmen (wie z. B. Online-Awareness-Trainings, gezielte Informationskampagnen, Erlass von Richtlinien) gesetzt. Darüber hinaus werden aktuelle Informationen anlassbezogen über das Intranet des BMLUK zum Thema Cybersicherheit bereitgestellt.

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	2025-04-25T10:22:49+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.bml.gv.at/amtssignatur	

	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2025-04-25T14:27:00+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	