

**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: 2025-0.244.086

Ihr Zeichen: BKA - PDion  
(PDion)868/J-NR/2025

Wien, 27. Mai 2025

Sehr geehrter Herr Präsident,

die Abgeordneten zum Nationalrat Rosa Ecker, Kolleginnen und Kollegen haben am 27. März 2025 unter der Nr. 868/J an mich eine schriftliche parlamentarische Anfrage betreffend „Mögliche Hackerangriffe auf Ihr Ministerium“ gerichtet.

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

**Zur Frage 1:**

- Besteht aktuell die Gefahr, dass Hackerangriffe gegen Ihr Ministerium vorgenommen werden und gelingen könnten?
  - a. Wenn ja, wie sind Sie aktuell auf so einen Fall vorbereitet?

Angriffsversuche und Angriffe selbst können nie ausgeschlossen werden. Das Bundesministerium für Land- und Forstwirtschaft, Klima- und Umweltschutz, Regionen und Wasserwirtschaft (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 vorbereitet.

**Zur Frage 2:**

- Gab es im Jahr 2024 sogenannte „Überlastungsangriffe“ oder andere abgewehrte Angriffe?
  - a. Wenn ja, wann?
  - b. Wenn ja, in welchem Umfang?

Auch im Jahr 2024 gab es eine Vielzahl von Überlastungsangriffen (DDoS), deren Auswirkungen durch eine Kombination von automatischer Mitigierung und manuellem Eingriff minimiert werden konnten. Allgemein wird festgehalten, dass DDoS Angriffe, die eine Dauer von einigen Minuten bis Stunden aufweisen, als alltäglich angesehen werden müssen und Teil jeder Standardrisikobewertung sind.

**Zur Frage 3:**

- Wie wird seitens Ihres Ministeriums aktuell für die Datensicherheit gesorgt?
  - a. Wer kann auf die von Ihnen verarbeiteten Daten zugreifen?

Im BMLUK wird sowohl technisch als auch organisatorisch für Datensicherheit gesorgt. IKT-Sicherheit (und damit auch Datensicherheit) wird als fortlaufender und umfassender Prozess verstanden. Dementsprechend werden im risikobasierten Ansatz kontinuierlich Anpassungen an der IKT-Sicherheitsstruktur und der dahinterliegenden Prozesse vorgenommen. Erkenntnisse aus dem gesamtstaatlichen Lagebildprozess werden in Zusammenarbeit mit den Technikerinnen und Technikern des BMLUK zeitnah umgesetzt. Zugriffsberechtigungen erfolgen nach dem Bedarfsprinzip unter Berücksichtigung der Sensibilität der Daten.

**Zur Frage 4:**

- Konnten zuletzt durch Ihr Ministerium Datenlecks festgestellt werden?
  - a. Wenn ja, wie konnte es dazu kommen?
  - b. Wenn ja, welche Daten waren betroffen?

Seitens des BMLUK konnten zuletzt keine Datenlecks festgestellt werden.

**Zu den Fragen 5 bis 7:**

- Welche internen/externen Sicherheitssysteme überwachen derzeit die vorhandenen Daten, Betriebssysteme und elektronischen Einheiten?
  - a. Welche Kosten entstehen für diese Systeme jährlich? (Einkauf, Installation, Wartung, Betreuung, Ausbau etc)
  - b. Welche Kosten sind 2023 und 2024 entstanden?

- In welchem zeitlichen Abstand werden diese Sicherheitssysteme auf die neuesten Entwicklungen und Bedrohungen angepasst und adaptiert?
- Wie ist die vorgeschriebene Vorgehensweise, wenn so ein Hackingangriff erfolgreich ist und Maßnahmen ergriffen werden müssen?
  - a. Ist diese Vorgehensweise in allen Ministerien einheitlich?
  - b. Wie oft werden derartige Szenarien durchgespielt und Vorkehrungen getroffen?

Im BMLUK werden basierend auf erfolgten Risikobewertungen und Bedrohungsanalysen unterschiedliche Sicherheitssysteme zum Einsatz gebracht. Neben technischen Maßnahmen zum Update und Upgrade bestehender Systeme erfolgt zyklisch eine risikobasierte Beurteilung auf zum Einsatz zu bringende Sicherheitssysteme hin. Für den Fall erfolgreicher Angriffe wird das organisationsspezifische Vorgehen von den Bundesministerien aufgrund der grundsätzlichen Vorgaben des Netz- und Informationssystemsicherheitsgesetzes (NISG), BGBl. I Nr. 111/2018, im eigenen Verantwortungsbereich geregelt. Im BMLUK wird das Vorgehen im Falle von Cyberangriffen durch Notfallpläne festgelegt.

Im Hinblick auf die Sicherung der Effektivität der Schutzmaßnahmen muss von einer detaillierten Bekanntgabe Abstand genommen werden.

Mag. Norbert Totschnig, MSc

