728/AB
vom 27.05.2025 zu 864/J (XXVIII. GP)

Bundesministerium
Wirtschaft, Energie
und Tourismus

bmwet.gv.at

Dr. Wolfgang Hattmannsdorfer
Bundesminister

Stubenring 1, 1010 Wien

Herrn
Präsidenten des Nationalrates
Dr. Walter Rosenkranz
Parlament
1017 Wien

Geschäftszahl: 2025-0.252.289

Ihr Zeichen: BKA - PDion (PDion)864/J-NR/2025

Wien, am 27. Mai 2025

Sehr geehrter Herr Präsident,

die Abgeordneten zum Nationalrat Rosa Ecker, MBA und weitere haben am 27.03.2025 unter der **Nr. 864/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?*
    - *Wenn ja, wie sind Sie aktuell auf so einen Fall vorbereitet?*

Angriffsversuche und Angriffe selbst auf die IKT-Systeme des Bundesministeriums für Wirtschaft, Energie und Tourismus (BMWET) können nie ausgeschlossen werden. Das Ressort 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?*

- *Wenn ja, wann?*
- *Wenn ja, in welchem Umfang?*

Mit dem Internet verbundene IKT-Systeme sind grundsätzlich zahlreichen, meist automatisierten Angriffsversuchen ausgesetzt. Diese werden durch die IKT-Sicherheitssysteme, ebenso weitestgehend automatisiert, abgewehrt.

In Einzelfällen kommt es zu Angriffsversuchen, welche über diesem "Grundrauschen" liegen. Diesbezüglich ist auf die Beantwortung der parlamentarischen Anfrage Nr. 18865/J der XXVII. GP zu verweisen.

Zu den Fragen 3 und 6

- *Wie wird seitens Ihres Ministeriums aktuell für die Datensicherheit gesorgt?*
  - *Wer kann auf die von Ihnen verarbeiteten Daten zugreifen?*
- *In welchem zeitlichen Abstand werden diese Sicherheitssysteme auf die neuesten Entwicklungen und Bedrohungen angepasst und adaptiert?*

Neben technischen Update- und Upgrademaßnahmen bestehender Systeme erfolgt zyklisch eine risikobasierte Beurteilung auf zum Einsatz zu bringende Sicherheitssysteme hin. Im Hinblick auf die Sicherung der Effektivität der Schutzmaßnahmen muss von näheren Ausführungen Abstand genommen werden.

Zur Frage 4

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

Nein.

Zur Frage 5

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

Im BMWET werden basierend auf erfolgten Risikobewertungen und Bedrohungsanalysen unterschiedliche Sicherheitssysteme zum Einsatz gebracht. Um deren Effektivität gegen

Bedrohungsakteure nicht zu gefährden, muss von detaillierten Ausführungen Abstand genommen werden.

Zur Frage 7

- *Wie ist die vorgeschriebene Vorgehensweise, wenn so ein Hackingangriff erfolgreich ist und Maßnahmen ergriffen werden müssen?*
    - *Ist diese Vorgehensweise in allen Ministerien einheitlich?*
    - *Wie oft werden derartige Szenarien durchgespielt und Vorkehrungen getroffen?*

Im BMWET regeln Notfallpläne das Vorgehen im Fall von Cyberangriffen. Allgemein gilt, dass das Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen Grundsätzliches regelt und die Ministerien das organisationsspezifische Vorgehen im eigenen Verantwortungsbereich festlegen. Auch hier muss im Hinblick auf die Sicherung der vollen Effektivität der Schutzmaßnahmen von detaillierten Ausführungen Abstand genommen werden.

Dr. Wolfgang Hattmannsdorfer

Elektronisch gefertigt

REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR WIRTSCHAFT, ENERGIE UND TOURISMUS @ AMTSSIGNATUR	Unterzeichner	Bundesministerium für Wirtschaft, Energie und Tourismus
	Datum/Zeit	2025-05-27T08:30:21+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.	2082304761
	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	2025-05-27T09:04:01+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	