4946/AB
vom 28.05.2026 zu 5492/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: 2026-0.278.416

Ihr Zeichen: BKA - PDion (PDion)5492/J-NR/2026

Wien, am 27. Mai 2026

Sehr geehrter Herr Präsident,

die Abgeordneten zum Nationalrat Süleyman Zorba und weitere haben am 27.03.2026 unter der **Nr. 5492/J** an mich eine schriftliche parlamentarische Anfrage betreffend **Cybersicherheitsvorfälle und -maßnahmen in den Bundesministerien** gerichtet.

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

Zur Frage 1

- *Gab es in Ihrem Ressort im Jahr 2025 Cyberangriffe oder Cybersicherheits-Vorfälle?*
    - *Falls ja, um wie viele Angriffe/Vorfälle hat es sich gehandelt?*
    - *Bei wie vielen Angriffen konnten die Täter ermittelt werden? Um welche Täter handelte es sich?*

Im Jahr 2025 wurden vier erwähnenswerte Informationssicherheitsvorfälle im Bundesministerium für Wirtschaft, Energie und Tourismus (BMWET) registriert. Sämtliche Vorfälle konnten erfolgreich abgewendet werden. Die Verursacher konnten eingegrenzt werden. Aus Gründen der Ressortsicherheit wird von einer Nennung der Gruppierungen Abstand genommen.

Zur Frage 2

- *Welche Präventionsmaßnahmen wurden von Ihrem Ministerium im vergangenen Jahr ergriffen, um sich vor Cyberangriffen und -kriminalität zu schützen?*
    - *Arbeiten Sie mit externen Expertinnen und Experten im Bereich Cybersicherheit zur Verhinderung von Cyberangriffen zusammen?*
    - *Wenn ja, um welche Experten handelte es sich im Jahr 2025?*
    - *Wie erfolgte die Auswahl?*
    - *Arbeiten Sie mit externen Unternehmen im Bereich Cybersicherheit zur Verhinderung von Cyberangriffen zusammen? Wenn ja, mit welchen?*

Das BMWET betreibt ein Informationssicherheitsmanagement-System (ISMS), welches auf Basis von Risikokategorien alle Informationssicherheitsrisiken behandelt. Daraus leitet sich eine Vielzahl technischer und organisatorischer Sicherheitsmaßnahmen ab. Das Krisenhandbuch des Ressorts sowie auch das Incident Response Management stellen einige dieser konkreten Pläne für die Bewältigung von Cyberangriffen dar.

Darüber hinaus tauscht sich das BMWET laufend mit Sicherheitsexpertinnen und -experten im Bund und der Privatwirtschaft aus, um Best Practices, neue Angriffsmuster, aber auch neue Lösungen aufzugreifen.

Sofern etwaige Beschaffungen dahingehend erforderlich sind, werden diese vorrangig über passende Lose der Bundesbeschaffung GmbH abgerufen.

Zur Frage 3

- *Gab es in Ihrem Ressort Risikoanalysen im Hinblick auf Cyberbedrohungen im Jahr 2025 und welche Ergebnisse brachten diese Analysen?*

Jedes IKT-Verfahren wird einer grundlegenden Informationssicherheitsrisikoanalyse unterzogen. Stellt sich dabei ein erhöhter Schutzbedarf heraus, wird eine erweiterte Informationssicherheitsanalyse durchgeführt und werden alle Komponenten im Detail geprüft. Darüber hinaus werden laufend externe Bedrohungsszenarien geprüft und entsprechende Maßnahmen gesetzt.

Zur Frage 4

- *Gibt es in Ihrem Ministerium Cybersicherheitsbeauftragte?*
    - *Welche Abteilungen oder Teams waren im Jahr 2025 innerhalb Ihres Ministeriums dafür zuständig?*

- *Wie viele Personen waren in Ihrem Ministerium im Jahr 2025 im Bereich Cyber- und IT-Sicherheit tätig?*
- *Welche konkreten Aufgaben nahmen diese Personen wahr?*

Derzeit befassen sich drei Personen, darunter auch der Chief Information Security Officer (CISO) und der IKT-Sicherheitsbeauftragte, hauptsächlich mit dem Themenkomplex Cyber- und IKT-Sicherheit in einem eigenen Referat in der IKT-Abteilung des BMWET.

Das Team verantwortet gesamthaft die Informations- & IKT-Sicherheit mit allen erforderlichen Tätigkeiten, unter anderem:

- Entwicklung und Umsetzung von Sicherheitsrichtlinien und -standards
- Implementierung technischer Sicherheitsmaßnahmen (Endpoint Detection & Response-Konfigurationen, Firewallregeln, Verschlüsselungsmechanismen, Zugriffskontrollen, Netzwerksegmentierung, Patchmanagement etc.)
- Planung und Umsetzung regelmäßiger Sicherheitsaudits und Schwachstellenanalysen
- Sicherstellung des Security-by-Design-Ansatzes
- Monitoring von Netzwerk- und Systemparametern
- Erkennung, Analyse und Koordination von Sicherheitsvorfällen
- Sicherstellung des Informationssicherheitsrisikomanagements
- Dokumentation und Reporting an Management und Aufsichtsbehörden
- Durchführung von Awareness-Schulungen und Sensibilisierungsmaßnahmen
- Implementierung weiterer organisatorischer Sicherheitsmaßnahmen

Zur Frage 5

- *Wie hoch war das Budget Ihres Hauses für IT- und Cybersicherheit im Jahr 2025?*

Dazu ist auf die Beantwortung der parlamentarischen Anfrage Nr. 3136/J zu verweisen.

Zur Frage 6

- *Gab es im Jahr 2025 konkrete verpflichtende Schulungsangebote in Fragen der IT- und Cybersicherheit für Mitarbeiter:innen Ihres Hauses sowie nachgeordneter Dienststellen?*
  - *Wenn ja, um welche Schulungsangebote handelte es sich?*
  - *Wie hoch waren die Kosten für dies Schulungen?*

Alle Schulungen wurden ressortintern ausgearbeitet und durchgeführt. Eine der zahlreichen awareness-bildenden Maßnahmen wurde mit einem externen Unternehmen durchgeführt und hat Kosten von € 8.586,86 verursacht.

Ergänzend ist auf die Beantwortung der parlamentarischen Anfrage Nr. 3136/J zu verweisen.

Dr. Wolfgang Hattmannsdorfer

Elektronisch gefertigt

REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR WIRTSCHAFT, ENERGIE UND TOURISMUS @ AMTSSIGNATUR	Unterzeichner	Bundesministerium für Wirtschaft, Energie und Tourismus
	Datum/Zeit	2026-05-27T16:47:41+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	2026-05-28T07:38:47+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	