563/J
vom 26.02.2025 (XXVIII. GP)

ANFRAGE

des Abgeordneten Schnedlitz
an den Bundesminister für europäische und internationale Angelegenheiten
betreffend **Cyberangriffe auf österreichische Ministerien**

„Angriffe auf Websites von Ministerien, Verwaltungsbehörden, Energieversorgern und öffentlichen Verkehrssystemen in Österreich registrierte man im BMI seit Mitte September, hieß es weiter. Aufgrund der Häufigkeit solcher Attacken verfügen viele Websites über entsprechende Schutzmaßnahmen, weshalb der Schaden gering ausfalle“, so liest man auf orf.at am 24.09.2024.[1]

In der heutigen digitalen Welt sind Cyberangriffe eine wachsende Bedrohung für staatliche Institutionen, insbesondere für Ministerien, die mit sensiblen Daten und kritischen Informationen arbeiten. Diese Angriffe können nicht nur zu erheblichen Datenverlusten führen, sondern auch das Vertrauen der Öffentlichkeit in die Sicherheit und Integrität unserer Regierungsinstitutionen gefährden. Die Gefahr von Cyberangriffen reicht von Identitätsdiebstahl über Erpressung bis hin zu gezielten Attacken auf die Infrastruktur, die im schlimmsten Fall die Funktionsfähigkeit des Staates beeinträchtigen können. Angesichts dieser drohenden Gefahr und alarmierenden Entwicklungen liegt es nahe, dass Ministerien ausreichende Maßnahmen ergreifen, um sich gegen solche Bedrohungen zu wappnen und die Sicherheit der digitalen Systeme sowie vertraulichen und sensiblen Daten zu gewährleisten.

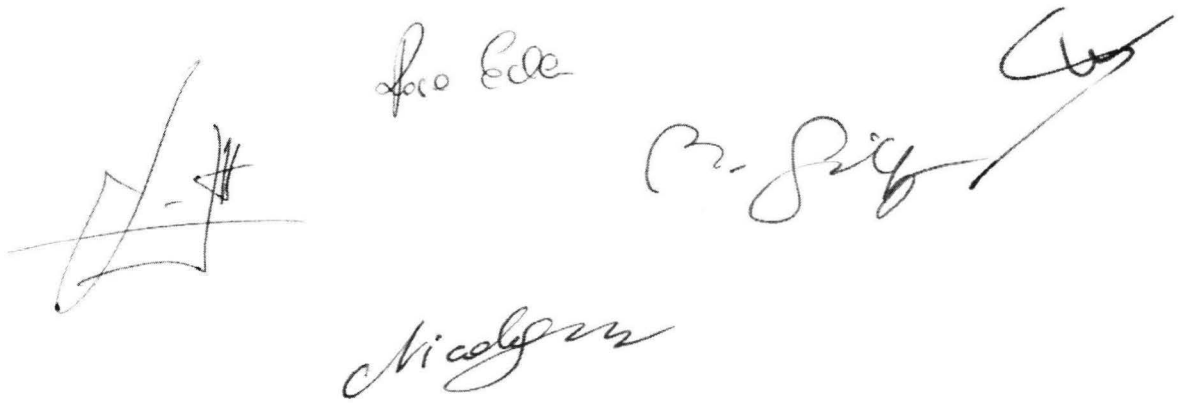
In diesem Zusammenhang stellt der unterfertigte Abgeordnete an den Bundesminister für europäische und internationale Angelegenheiten folgende

Anfrage

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“.
2. Gibt es konkrete Pläne, sich für den Ernstfall eines potenziellen Cyberangriffs zu schützen?
3. Welche Rolle und welche konkreten Aufgaben fallen Ihrem Ressort in der gesamtstaatlichen Bekämpfung von Cyberkriminalität zu?
4. Welche konkreten Maßnahmen werden aktiv von Ihrem Ministerium ergriffen, um sich präventiv gegen Cyberattacken und gegen Cyberkriminalität zu schützen?
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?
6. Gab es in Ihrem Ressort eigene Risikoanalysen?
    a. Falls ja, welche?
    b. Falls nein, warum nicht?

[1] https://orf.at/stories/3370777/

7. Welche konkreten Maßnahmen setzen Sie, um den spezifischen Risiken Ihres Ministeriums gerecht zu werden?
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?
9. Welche Maßnahmen wurden ergriffen, um alle Mitarbeitenden in Ihrem Ministerium gegen die drohende Gefahr von Cyberangriffen zu sensibilisieren?
10. Welche Maßnahmen werden in Zukunft ergriffen bzw. sind geplant, um alle Mitarbeitenden in Ihrem Ministerium gegen die drohende Gefahr von Cyberangriffen zu sensibilisieren?



	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2025-02-26T18:28:22+01:00
Prüfinformation	Dieses Dokument wurde elektronisch besiegelt. Informationen zur Prüfung des elektronischen Siegels und des Ausdrucks finden Sie unter: https://www.parlament.gv.at/siegel	