Bundesministerium
Arbeit, Soziales, Gesundheit,
Pflege und Konsumentenschutz

sozialministerium.gv.at

Korinna Schumann
Bundesministerin

Herrn
Dr. Walter Rosenkranz
Präsident des Nationalrates
Parlament
1017 Wien

Geschäftszahl: 2025-0.267.545

Wien, 23.5.2025

Sehr geehrter Herr Präsident!

Ich beantworte die an mich gerichtete schriftliche parlamentarische **Anfrage Nr. 866/J der Abgeordneten Ecker betreffend Mögliche Hackerangriffe auf Ihr Ministerium** wie folgt:

Eingangs darf ich auch auf die Beantwortung der parlamentarischen Anfrage Nr. 565/J verweisen.

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 Arbeit, Soziales, Gesundheit, Pflege und Konsumentenschutz 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.

Frage 2: *Gab es im Jahr 2024 sogenannte „Überlastungsangriffe" oder andere abgewehrte Angriffe?*

a. Wenn ja, wann?

b. Wenn ja, in welchem Umfang?

Auch 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.

Frage 3: *Wie wird seitens Ihres Ministeriums aktuell für die Datensicherheit gesorgt?*

a. Wer kann auf die von Ihnen verarbeiteten Daten zugreifen?

Im Bundesministerium für Arbeit, Soziales, Gesundheit, Pflege und Konsumentenschutz 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 Ressorts zeitnahe umgesetzt. Zugriffsberechtigungen erfolgen nach dem Bedarfsprinzip unter Berücksichtigung der Sensibilität der Daten.

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?

Im Bundesministerium für Arbeit, Soziales, Gesundheit, Pflege und Konsumentenschutz wurden zuletzt keine Datenlecks festgestellt.

Frage 5: *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?

Im Bundesministerium für Arbeit, Soziales, Gesundheit, Pflege und Konsumentenschutz werden basierend auf regelmäßig stattfindenden Risikobewertungen und Bedrohungsanalysen unterschiedliche Sicherheitssysteme zum Einsatz gebracht. Im Hinblick auf die Sicherung der Effektivität dieser Schutzmaßnahmen muss von einer detaillierten Bekanntgabe Abstand genommen werden.

Frage 6: *In welchem zeitlichen Abstand werden diese Sicherheitssysteme auf die neuesten Entwicklungen und Bedrohungen angepasst und adaptiert?*

Neben technischen Maßnahmen zum Update und Upgrade 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 einer detaillierten Auflistung Abstand genommen werden.

Frage 7: *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?

Das NISG regelt Grundsätzliches, die Ministerien regeln das organisationsspezifische Vorgehen im eigenen Verantwortungsbereich. Im Bundesministerium für Arbeit, Soziales, Gesundheit, Pflege und Konsumentenschutz regeln Notfallpläne das Vorgehen im Falle von Cyberangriffen. Im Hinblick auf die Sicherung der Effektivität der Schutzmaßnahmen muss von einer detaillierten Bekanntgabe Abstand genommen werden.

Mit freundlichen Grüßen

Korinna Schumann

REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR ARBEIT, SOZIALES, GESUNDHEIT, PFLEGE UND KONSUMENTENSCHUTZ @ AMTSSIGNATUR	Unterzeichner	Bundesministerium für Arbeit, Soziales, Gesundheit, Pflege und Konsumentenschutz
	Datum/Zeit	2025-05-26T09:36:40+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.	1088205675
Hinweis	Dieses Dokument wurde amtssigniert.	
Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: http://www.signaturpruefung.gv.at Informationen zur Prüfung des Ausdrucks finden Sie unter: https://www.sozialministerium.at/site/Ministerium/Willkommen_im_Ministerium/Amtssignatur/Amtssignatur	

	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2025-05-26T10:08:13+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	