806/AB
vom 27.05.2025 zu 859/J (XXVIII. GP)

Bundeskanzleramt

bundeskanzleramt.gv.at

Dr. Christian Stocker
Bundeskanzler

Herrn
Dr. Walter Rosenkranz
Präsident des Nationalrats
Parlament
1017 Wien

Geschäftszahl: 2025-0.240.634

Wien, am 27. Mai 2025

Sehr geehrter Herr Präsident,

die Abgeordneten zum Nationalrat Ecker, MBA, Kolleginnen und Kollegen haben am 27. März 2025 unter der Nr. **859/J** eine schriftliche parlamentarische Anfrage betreffend „Mögliche Hackerangriffe auf Ihr Ministerium“ an mich gerichtet.

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

Zu Frage 1:

1. *Besteht aktuell die Gefahr, dass Hackerangriffe gegen das Bundeskanzleramt vorgenommen werden und gelingen könnten?*
   a. *Wenn ja, wie sind Sie aktuell auf so einen Fall vorbereitet?*

Angriffsversuche und Angriffe auf IT-Systeme können nie vollständig ausgeschlossen werden. Das Bundeskanzleramt ist daher durch technische und organisatorische Sicherheitsmaßnahmen nach dem aktuellen Stand der Technik in den Bereichen Prävention, Absicherung, Erkennung und Incident-Response vorbereitet.

Zu Frage 2:

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

Im Jahr 2024 gab es eine Vielzahl von Überlastungsangriffen (DDoS), deren Auswirkungen durch eine Kombination von automatischer Mitigierung und manuellen Eingriffen 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.

Zu Frage 3:

3. *Wie wird Ihrerseits aktuell für die Datensicherheit gesorgt?*
   a. *Wer kann auf die von Ihnen verarbeiteten Daten zugreifen?*

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

Zu Frage 4:

4. *Konnten zuletzt durch das Bundeskanzleramt Datenlecks festgestellt werden?*
   a. *Wenn ja, wie konnte es dazu kommen?*
   b. *Wenn ja, welche Daten waren betroffen?*

Seitens des Bundeskanzleramtes konnten zuletzt keine Datenlecks festgestellt werden.

Zu Frage 5:

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 Bundeskanzleramt werden – basierend auf erfolgten 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.

Zu Frage 6:

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

Neben technischen Maßnahmen für Updates und Upgrades bestehender Systeme erfolgt zyklisch eine risikobasierte Beurteilung in Bezug auf zum Einsatz zu bringende Sicherheitssysteme. Im Hinblick auf die Sicherung der Effektivität der Schutzmaßnahmen muss von einer detaillierten Auflistung Abstand genommen werden.

Zu Frage 7:

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 Netz- und Informationssystemsicherheitsgesetz regelt das grundsätzliche Handeln und die Ministerien regeln das organisationsspezifische Vorgehen im eigenen Verantwortungsbereich. Im Bundeskanzleramt 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.

Dr. Christian Stocker

REPUBLIK ÖSTERREICH BUNDESKANZLERAMT AMTSSIGNATUR	Unterzeichner	serialNumber=734173660,CN=Bundeskanzleramt,C=AT
	Datum/Zeit	2025-05-27T10:53:41+02:00
	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at Informationen zur Prüfung des Ausdrucks finden Sie unter: https://www.bundeskanzleramt.gv.at/verifizierung
	Hinweis	Dieses Dokument wurde amtssigniert.

	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2025-05-27T12:23:35+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	