2664/AB
vom 10.10.2025 zu 3124/J (XXVIII. GP)

Bundesministerium
Inneres

Mag. Gerhard Karner
Bundesminister

Herrn
Präsidenten des Nationalrates
Dr. Walter Rosenkranz
Parlament
1017 Wien

Geschäftszahl: 2025-0.750.123

Wien, am 9. Oktober 2025

Sehr geehrter Herr Präsident!

Der Abgeordnete zum Nationalrat Süleyman Zorba, Freundinnen und Freunde haben am 12. August 2025 unter der Nr. **3124/J** an mich eine schriftliche parlamentarische Anfrage betreffend „IT- und Cybersicherheit im Bundesministerium für Inneres sowie bei Mitarbeiter:innen in Schlüsselpositionen“ gerichtet.

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

Zur Frage 1:

- *Welche verbindlichen Richtlinien bestehen derzeit in Ihrem Haus zur sicheren Nutzung dienstlicher IT Geräte (Smartphones, Laptops, Tablets) durch Mitarbeiter: innen?*

Die Handhabung der IKT-Ausstattung ist für alle Bediensteten des Bundes in der IKT Nutzungsverordnung geregelt. Überdies bestehen im BMI weitergehende Regelungen und Erlässe wie „Technische Vorgaben zur Verwendung der IT im Bundesministerium für Inneres 2024“, Erlass für mobile Polizeikommunikation und im Erlass „Organisatorische Vorgaben zur Verwendung der IT im Bundesministerium für Inneres“.

Darüber hinaus findet auch ein regulärer und anlassbezogener Informationsaustausch zwischen den Ministerien und obersten Organen statt.

Zu den Fragen 2 bis 5 und 9 bis 11:

- *Gibt es gesonderte Vorgaben für den Umgang mit vertraulichen Informationen auf mobilen Geräten, insbesondere hinsichtlich Verschlüsselung, Zwei Faktor Authentifizierung und Speicherung sensibler Daten?*
- *In welchen zeitlichen Abständen werden Sicherheitsüberprüfungen oder Audits der dienstlichen IT Geräte durchgeführt, sowohl im Inland als auch bei im Ausland tätigen Mitarbeiter:innen?*
  a. *Wie oft finden diese Audits im Durchschnitt pro Jahr statt?*
  b. *Welche internen oder externen Stellen führen diese Audits durch?*
- *Werden Diensthandys oder andere mobile Geräte auf Reisen in Länder mit erhöhtem Spionagerisiko durch „Burner Phones" oder andere Einweggeräte ersetzt?*
  a. *Wenn ja, seit wann gilt diese Praxis und für welche Destinationen?*
- *Welche Maßnahmen bestehen, um das Risiko der Nutzung unsicherer öffentlicher Netzwerke (z.B. Hotel WLANs) durch Mitarbeiter:innen zu minimieren?*
- *Gibt es eine regelmäßige Evaluierung der vorhandenen Sicherheitsstandards unter Einbeziehung externer Sicherheits- und Datenschutzexperten? Wenn ja, wann fand die letzte Evaluierung statt und welche Ergebnisse wurden daraus abgeleitet?*
- *Wurden nach Bekanntwerden des eingangs erwähnten Sicherheitsvorfalls im Jahr 2025 konkrete Maßnahmen gesetzt, um ähnliche Fälle künftig zu verhindern?*
  a. *Wenn ja, welche?*
- *Inwieweit arbeitet Ihr Haus mit nationalen und internationalen Stellen (z. B. DSN, CERT, EU Partner) zusammen, um sich über aktuelle Bedrohungen und Best Practices auszutauschen?*

Für das BMI hat der Schutz der verarbeiteten Daten und der dafür eingesetzten IT-Verfahren und IKT-Infrastrukturkomponenten eine hohe Priorität. Für den Umgang mit vertraulichen Daten darf auf die Geheimschutzordnung des Bundes sowie das Informationssicherheitsgesetz hingewiesen werden. Das BMI verfügt über entsprechende Informationssicherheits- und Datenschutz-Managementsysteme, welche sich an internationalen Sicherheitsstandards orientieren.

Diese Systeme sorgen unter anderem dafür, dass die diesbezüglich geltenden Rechtsvorschriften eingehalten und bestehende Risiken systematisch identifiziert, beurteilt und mittels geeigneter technischer und organisatorischer Maßnahmen unter Berücksichtigung des Stands der Technik in den Bereichen Prävention, Erkennung und Reaktion reduziert werden. Es sieht darüber hinaus vor, dass die Aktualität der geltenden Regelungen sowie die Wirksamkeit der getroffenen Maßnahmen sowohl regelmäßig als

auch im Anlassfall überprüft, bewertet und evaluiert wird. Dabei wird auch die Expertise externer und interministerieller Stellen genutzt.

Die Evaluierung und Aktualisierung der diesbezüglichen Erlässe erfolgen laufend. Die öffentlich verfügbaren Sicherheitsstandards spezifizieren dafür umfassende Anforderungs- bzw. Maßnahmenkataloge.

Gemäß BMEIA und BMI/DSN Länderbewertungen werden für Dienstreisen individuelle Schutzmaßnahmen entsprechend den aktuellen Sicherheitsstandards und Good Practices, wie beispielsweise den Handlungsempfehlungen der Direktion Staatsschutz und Nachrichtendienst gesetzt.

Im Hinblick auf die Sicherung der Effektivität der getroffenen Schutzmaßnahmen muss jedoch von einer detaillierten Bekanntgabe Abstand genommen werden.

Zur Frage 6:

- *Wie werden die Mitarbeiter:innen in Fragen der IT Sicherheit geschult?*
  a. *Gibt es verpflichtende Schulungen für alle Beschäftigten?*
  b. *In welchen zeitlichen Abständen werden diese Schulungen angeboten?*
  c. *Werden Sondertrainings für besonders exponierte Funktionen oder Mitarbeiter:innen in Schlüsselpositionen durchgeführt?*

Es werden laufend verpflichtende online eLearning Module auf dem eCampus der SIAK angeboten und abgehalten. Das Schulungsprogramm wird auf die unterschiedlichen Bedürfnisse der jeweiligen Personengruppen angepasst. Im Rahmen des Bildungsprogramms der Verwaltungsakademie des Bundes werden überdies umfassende Aus-, Fort- und Weiterbildungsmaßnahmen für diesen Bereich angeboten.

Zur Frage 7:

- *Welche Abteilungen oder Teams sind innerhalb Ihres Hauses für IT Sicherheit und Cyberabwehr zuständig?*
  a. *Wie viele Planstellen sind aktuell für diesen Bereich vorgesehen?*
  b. *Wie viele davon sind mit qualifiziertem Personal besetzt?*

Für die angesprochenen Bereiche sind im Bundesministerium für Inneres die Gruppe IV/DDS – Direktion Digitale Services (DDS) und die Direktion Staatsschutz und Nachrichtendienst (DSN) zuständig.

Da die Mitarbeiter im Bereich der Informationssicherheit in einem sensiblen Bereich tätig sind, muss aus Gründen der Informationssicherheit und des Datenschutzes von einer Nennung weiterer Details Abstand genommen werden.

Zur Frage 8:

- *Wie hoch war das jährliche Budget Ihres Ressorts für IT- und Cybersicherheit in den letzten fünf Jahren (bitte nach Jahren aufschlüsseln)?*

Da IT- und Cybersicherheit eine Querschnittsmaterie darstellen, sind die damit verbundenen Aufwände und Kosten nicht eindeutig zuordenbar.

Zur Frage 12:

- *Gibt es Meldewege oder Whistleblower Plattformen für Mitarbeiter: innen, um Sicherheitslücken oder ungewöhnliche Vorfälle anonym zu melden?*
  a. *Wenn ja, wie wird sichergestellt, dass diese Hinweise unverzüglich bearbeitet werden?*

Mitarbeiterinnen und Mitarbeiter des Bundesministeriums für Inneres können sich an die Meldestelle nach dem HinweisgeberInnenschutzgesetz (HSchG) wenden, von welcher eingehende Hinweise im Einklang mit den gesetzlichen Bestimmungen bearbeitet werden.

Es darf auf die im BAK eingerichteten Meldestellen verwiesen werden, diese finden sich auf der Homepage des BAK unter https://www.bak.gv.at/701/start.aspx

Darüber hinaus wird auf die Meldepflicht gemäß § 53 Abs. 1 Beamten-Dienstrechtsgesetz 1979 (für Vertragsbedienstete iVm § 5 Abs. 1 Vertragsbedienstetengesetz 1948) hingewiesen. Wird demnach dem Bundesbediensteten in Ausübung des Dienstes der begründete Verdacht einer von Amts wegen zu verfolgenden gerichtlich strafbaren Handlung bekannt, die den Wirkungsbereich der Dienststelle betrifft, der er angehört, so ist dies unverzüglich dem Leiter der Dienststelle zu melden.

Gerhard Karner

	Datum/Zeit	2025-10-10T14:45:08+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.	2052038352
Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at. Eine Verifizierung des Ausdruckes kann bei der ausstellenden Behörde/Dienststelle erfolgen.	
Hinweis	Dieses Dokument wurde amtssigniert.	

	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2025-10-10T14:49:37+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	