



Mag. Gerhard Karner
Bundesminister

Herrn
Präsidenten des Nationalrates
Mag. Wolfgang Sobotka
Parlament
1017 Wien

Geschäftszahl: 2024-0.532.657

Wien, am 13. August 2024

Sehr geehrter Herr Präsident!

Der Abgeordnete zum Nationalrat Christian Hafenecker, MA hat am 13. Juni 2024 unter der Nr. **18893/J** an mich eine schriftliche parlamentarische Anfrage betreffend „Wie steht es um die Datensicherheit des Bundes?“ gerichtet.

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

Zu den Fragen 1 und 3:

- *Wie viele Cyberangriffe verzeichnete Ihr Ressort in der laufenden Legislaturperiode?*
 - a. *Wie viele dieser Cyberangriffe waren erfolgreich, konnten also Schaden anrichten (Datendiebstahl, Lahmlegung, DDos etc.)?*
 - b. *Sofern bekannt, aus welchen Ländern/Regionen stammten diese Cyberangriffe (bitte um Auflistung)?*
- *Wie viele Cyberangriffe verzeichneten nachgeordnete Dienststellen Ihres Ressorts in der laufenden Legislaturperiode?*
 - a. *Welche nachgeordneten Dienststellen waren betroffen?*
 - b. *Wie viele dieser Cyberangriffe waren erfolgreich, konnten also Schaden anrichten (Datendiebstahl, Lahmlegung, DDos etc.)?*

- c. *Sofern bekannt, aus welchen Ländern/Regionen stammten diese Cyberangriffe (bitte um Auflistung)?*

Es darf auf die Beantwortung zu PA 18815/J vom 12.06.2024 (XXVII. GP) verwiesen werden.

Zur Frage 2:

- *Gibt es eine zentrale Stelle innerhalb Ihres Ressorts oder innerhalb der Bundesverwaltung, an die derartige Vorfälle gemeldet werden bzw. gemeldet werden müssen (Stichwort Lagebild)?*
 - a. *Wer führt ein solches Lagebild?*

Innerhalb der Bundesverwaltung ist das GovCERT für die Entgegennahme von Meldungen über Sicherheitsvorfälle gemäß § 22 Abs. 2 und Abs.3 NISG zuständig. Diese Informationen fließen in das durch den gemäß NISG eingerichteten IKDOK (Innerer Kreis der Operativen Koordinierung), welcher das gesamtstaatliche Lagebild erstellt.

Zur Frage 4:

- *Mit welchen ausländischen IT-Konzernen arbeitet Ihr Ressort derzeit in welchen Bereichen zusammen (Bitte um Auflistung nach Name und Land)?*
 - a. *Welche Verträge bestehen mit welchen ausländischen IT-Konzernen?*
 - b. *Welche konkreten Dienstleistungen werden in Anspruch genommen?*
 - c. *Zu welchen Dienstleistungen gab es Ausschreibungen?*

Bei der Beschaffung von IT-Leistungen bedient sich das Bundesministerium vorrangig des Bundesrechenzentrums (BRZ) und BBG gelisteter Produkte und Dienstleistungen. Nicht derartig beschaffbare Leistungen werden gemäß Bundesvergabegesetz und unter Einhaltung der entsprechenden gesetzlichen Rahmenbedingungen (wie z.B. DSGVO) beschafft.

Darüber hinaus muss von der detaillierten Auflistung der Maßnahmen zur Erhöhung bzw. dem Erhalt eines hohen IKT- Sicherheitsniveaus gemäß des Netz- und Informationssystemsicherheitsgesetz, BGBl. I Nr. 111/2018, oder aber auch der Auflistung einzelner im Einsatz befindlicher Produkte im Hinblick auf die Sicherung der Effektivität der Schutzmaßnahmen Abstand genommen werden.

Zu den Fragen 5 und 6:

- *Wo und wie werden digital generierte Daten (personenbezogene wie nichtpersonenbezogene) durch Ihr Ressort konkret gesichert?*
 - a. *Sofern Cloud-Lösungen in Anspruch genommen werden, welche und in welchen Staaten liegen die dazugehörigen Server?*
 - b. *Welche externen Dienstleister haben Zugriff auf welche Daten in Ihrem Ressort?*
- *Wo werden Daten-Backups Ihres Ressorts konkret gesichert?*
 - a. *Sofern Cloud-Lösungen in Anspruch genommen werden, welche und in welchen Staaten liegen die dazugehörigen Server?*
 - b. *Wer hat Zugriff auf diese Backups?*
 - c. *Hat Ihr Ressort jederzeit Zugriff auf diese Backups?*
 - d. *Haben externe Dienstleister oder Dritte Zugriff auf diese Backups (Bitte um Auflistung)?*

Das Bundesministerium für Inneres verfolgt bei der Verarbeitung von Daten einen risikobasierten Ansatz. Abhängig von der Schutzwürdigkeit der Daten, werden diese gegebenenfalls unter Einsatz starker Verschlüsselung und georedundant gespeichert. Je nach Kritikalität der Daten ist der Zugriff auf bestimmte Personengruppen eingeschränkt.

Zur Frage 7:

- *Welche konkreten Maßnahmen und Sicherheitsstrategien verfolgt Ihr Ressort, um möglichen Missbrauch mit Daten durch Dritte zu verhindern?*

Daten werden im Bundesministerium für Inneres im risikobasierten Ansatz geschützt. Das Bundesministerium für Inneres verfolgt darüber hinaus einen gesamtheitlichen Ansatz, welcher Maßnahmen nach Stand der Technik sowie organisatorisch entsprechend umsetzt.

Zur Frage 8:

- *Gibt es zwischen den ressortübergreifenden Abstimmungen, gemeinsame Arbeitsgruppen, Organisationseinheiten oder ähnliches im Bereich IT-Sicherheit und Cybersecurity hinsichtlich Synergien, Wissen, Effizienz, Lagebewusstsein, Gefährdungspotenzial und ähnlichem?*

Im Bereich der IT-Sicherheit und Cybersecurity gibt es sowohl auf strategischer, operativer als auch technischer Ebene interministerielle Arbeits- und Austauschgruppen. Als Beispiel seien hier genannt die Cyber Sicherheit Steuerungsgruppe (CSS), der Innere Kreis der Operativen Koordinierungsstruktur (IKDOK) bzw. die Operativen Koordinierungsstruktur

(OpKoord), sowie der Austrian Trust Circle Government (ATC-Gov). Das durch den IKDOK erstellte Cyberlagebild wird allen Ministerien zur Verfügung gestellt.

Zu den Fragen 9 und 10:

- *Wie ist der Stand der NIS-Richtlinien-Umsetzung in Ihrem Ministerium?*
- *Wurden die aktuellen Umsetzungen der NIS-Richtlinien evaluiert?*
 - a. *Wenn ja, mit welchen Ergebnissen?*
 - b. *Wenn nein, warum nicht bzw. ist eine Evaluierung geplant? Wann?*

Das Netz- und Informationssystemsicherheitsgesetz (NISG) legt Maßnahmen fest, mit denen ein hohes Sicherheitsniveau von Netz- und Informationssystemen von Betreibern wesentlicher Dienste, Anbietern digitaler Dienste sowie Einrichtungen der öffentlichen Verwaltung erreicht werden soll. Das Bundesministerium für Inneres evaluiert und implementiert laufend technische und organisatorische Maßnahmen, um den Vorgaben der NIS-Richtlinie zu entsprechen. Die Bewertung der Eignung der Sicherheitsmaßnahmen erfolgt auf kontinuierlicher Basis unter Abstützung auf den Risikoeinschätzungen und technischen Empfehlungen des IKDOK.

Zu den Fragen 11 bis 13:

- *Gibt es Anstrengungen, Vorhaben oder Überlegungen, die Datenverarbeitung seitens der Bundesverwaltung in Österreich zu bewerkstelligen?*
- *Welche Datenarchive im Wirkungsbereich des Bundes liegen im Ausland (Bitte um Auflistung)?*
- *Welche Anstrengungen unternimmt die Bundesregierung, um sämtliche Datenarchive auf österreichisches Staatsgebiet zu holen und somit gerade in Krisenzeiten ein Mindestmaß an digitaler Autonomie und Sicherheit zu gewährleisten?*

Die Datenverarbeitung in den Ministerien erfolgt nach Analyse hinsichtlich der Klassifizierung, Kritikalität, Verfügbarkeitsanforderungen und Datenschutzerfordernissen abgestuft lokal, auf ministerieller Infrastruktur, auf Bundesinfrastruktur oder auf Infrastruktur von Drittanbietern. Wo eine Datenverarbeitung durch Dritte wahrgenommen wird, erfolgt dies nach erfolgter Risikobewertung und unterliegt den strengen Regelungen der DSGVO. Zusätzlich existieren unterschiedliche Projekte um die Abhängigkeit von Dritten zu reduzieren. Hinsichtlich der Bundesinfrastruktur darf darauf hingewiesen werden, dass mit der Bundesrechenzentrum GmbH schon seit Langem ein gesetzlicher Dienstleister eingerichtet wurde, welcher im 100%igem Eigentum des Bundes steht. Als solcher ist er zentraler IT-Dienstleister des Bundes und auf österreichischem Staatsgebiet tätig. Hinsichtlich meines Ressorts ist zusätzlich festzuhalten, dass ein eigenes

Rechenzentrum betrieben wird, dieses keine Datenarchive in Unions- oder Drittstaaten unterhält. Vielmehr betreibt das Bundesministerium für Inneres sämtliche Datenarchive innerhalb dieses eigenen Rechenzentrums, auf eigenen Systemen unter eigener zentraler Verwaltung.

Zur Frage 14:

- *Welche Position nimmt die Bundesregierung zum US-„Cloud Act“ in Hinblick auf die DSGVO ein?*

Die Festlegung der Position der Bundesregierung fällt nicht in den Vollzugsbereich des Bundesministeriums für Inneres bzw. unterliegen Meinungen und Einschätzungen nicht dem parlamentarischen Interpellationsrecht.

Gerhard Karner

