

+43 1 531 20-0
Minoritenplatz 5, 1010 Wien

Herrn
Präsidenten des Nationalrates
Mag. Wolfgang Sobotka
Parlament
1017 Wien

Geschäftszahl: 2024-0.444.722

Die schriftliche parlamentarische Anfrage Nr. 18862/J-NR/2024 betreffend Wie steht es um die Datensicherheit des Bundes?, die die Abgeordneten zum Nationalrat Christian Hafenecker, MA, Kolleginnen und Kollegen am 13. Juni 2024 an mich richteten, darf ich anhand der mir vorliegenden Informationen wie folgt beantworten:

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)?*

Dazu wird auf die Beantwortung der Parlamentarischen Anfrage Nr. 18816/J-NR/2024 vom 12. Juni 2024 verwiesen.

Zu 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 des Bundesministeriums für Bildung, Wissenschaft und Forschung ist die Abteilung PräS/14 für die Erkennung und Behandlung von Cyberangriffen zuständig. Etwaige Informationen über Angriffe fließen via Meldung an die NIS-Behörde in das durch den gemäß Netz- und Informationssystemsicherheitsgesetz (NISG), BGBl. I Nr. 111/2018, eingerichteten IKDOK (Innerer Kreis der Operativen Koordinierung), welcher das gesamtstaatliche Lagebild erstellt.

Zu 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 für Bildung, Wissenschaft und Forschung vorrangig des Bundesrechenzentrums (BRZ GmbH) und BBG gelisteter Produkte und Dienstleistungen. Darüber hinaus erforderliche Leistungen werden gemäß Bundesvergabegesetz und unter Einhaltung der entsprechenden gesetzlichen Rahmenbedingungen (wie z.B. DSGVO) beschafft.

Von einer detaillierten Auflistung der Maßnahmen oder der Auflistung einzelner im Einsatz befindlicher Produkte muss im Hinblick auf die Sicherung der Effektivität der Schutzmaßnahmen Abstand genommen werden.

Zu den Fragen 5 bis 7:

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

Das Bundesministerium für Bildung, Wissenschaft und Forschung 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.

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

Zu 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 govCERT, die Cyber Sicherheit Steuerungsgruppe (CSS) sowie der Austrian Trust Circle Government (ATC-Gov) genannt.

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 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 Bildung, Wissenschaft und Forschung betreibt keinen wichtigen Dienst gemäß NISG, hat aber Maßnahmensetzungen in Anlehnung an die Vorgaben des NISG betreffend Einrichtungen der öffentlichen Verwaltung umgesetzt.

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.

Mit der Bundesrechenzentrum GmbH wurde ein gesetzlicher Dienstleister eingerichtet, welcher im 100%-igem Eigentum des Bundes steht. Als solcher ist er zentraler IT Dienstleister des Bundes.

Zu Frage 14:

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

Die Einhaltung der Vorschriften der DSGVO durch Verantwortliche, die gemäß Art. 2 und 3 DSGVO der DSGVO unterliegen, obliegt dem für die jeweilige Datenverarbeitung Verantwortlichen (vgl. Art. 24 DSGVO). Dies gilt auch im Falle eines Drittlandbezugs (etwa im Zusammenhang mit der Nutzung von Clouds).

Im Hinblick auf Datenübermittlungen an Drittländer ist auf die Vorschriften von Kapitel V DSGVO hinzuweisen, insbesondere auf Art. 48 DSGVO, demzufolge „[j]ediges Urteil eines Gerichts eines Drittlands und jegliche Entscheidung einer Verwaltungsbehörde eines Drittlands, mit denen von einem Verantwortlichen oder einem Auftragsverarbeiter die Übermittlung oder Offenlegung personenbezogener Daten verlangt wird, [...] unbeschadet anderer Gründe für die Übermittlung gemäß diesem Kapitel jedenfalls nur dann anerkannt oder vollstreckbar werden [dürfen], wenn sie auf eine in Kraft befindliche internationale Übereinkunft wie etwa ein Rechtshilfeabkommen zwischen dem ersuchenden Drittland und der Union oder einem Mitgliedstaat gestützt sind.“

Wien, 13. August 2024

Ao. Univ.-Prof. Dr. Martin Polaschek

