

Mag. Norbert Totschnig, MSc
Bundesminister für Land- und Forstwirtschaft,
Regionen und Wasserwirtschaft

Herrn
Mag. Wolfgang Sobotka
Präsident des Nationalrats
Parlament
1017 Wien

Geschäftszahl: 2024-0.445.296

Ihr Zeichen: BKA - PDion
(PDion)18863/J-NR/2024

Wien, 13. August 2024

Sehr geehrter Herr Präsident,

die Abgeordneten zum Nationalrat Christian Hafenecker, MA, Kolleginnen und Kollegen haben am 13. Juni 2024 unter der Nr. **18863/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)?

In Beantwortung der gestellten Fragen darf auf die Beantwortung der parlamentarischen Anfrage Nr. 18801/J vom 12. Juni 2024 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?

Im Falle eines erheblichen Sicherheitsvorfalles wird von den IKT-Verantwortlichen des Bundesministeriums für Land- und Forstwirtschaft, Regionen und Wasserwirtschaft eine Meldung an „nis.govcert.gv.at“ abgesetzt.

Diese Informationen fließen in das durch den gemäß Netz- und Informationssystemsicherheitsgesetz, BGBl. I Nr. 111/2018, eingerichteten „Inneren Kreis der Operativen Koordinierung“ (IKDOK) ein, 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 für Land- und Forstwirtschaft, Regionen und Wasserwirtschaft vorrangig der Bundesrechenzentrum GmbH, der Land-, forst- und wasserwirtschaftlichen Rechenzentrum GmbH und der in der Bundesbeschaffung GmbH gelisteten Produkte und Dienstleistungen. Nicht derartig beschaffbare Leistungen werden gemäß Bundesvergabegesetz 2018, BGBl. I Nr. 65/2018 idgF, und unter Einhaltung der entsprechenden gesetzlichen Rahmenbedingungen [wie z. B. der Datenschutz-Grundverordnung (DSGVO)] beschafft.

Darüber hinaus muss von der detaillierten Auflistung der Maßnahmen zur Erhöhung bzw. dem Erhalt eines hohen IKT-Sicherheitsniveaus gemäß des Netz- und Informationssystemsicherheitsgesetzes, BGBl. I Nr. 111/2018, und 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 nicht-personenbezogene) 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 Land- und Forstwirtschaft, Regionen und Wasserwirtschaft verfolgt bei der Verarbeitung von Daten einen risikobasierten Ansatz. Abhängig von der Schutzwürdigkeit werden die Daten gegebenenfalls unter Einsatz geeigneter 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 Land- und Forstwirtschaft, Regionen und Wasserwirtschaft gemäß risikobasiertem Ansatz geschützt. Das Bundesministerium für Land- und Forstwirtschaft, Regionen und Wasserwirtschaft verfolgt darüber hinaus einen gesamtheitlichen Ansatz, welcher Maßnahmen nach dem 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 und operativer als auch auf technischer Ebene interministerielle Arbeits- und Austauschgruppen. Als Beispiel seien hier die Cyber Sicherheit Steuerungsgruppe, der IKDOK bzw. die Operative Koordinierungsstruktur sowie der Austrian Trust Circle Government genannt.

Das durch den IKDOK erstellte Cyberlagebild wird allen Bundesministerien 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 Bundesministerium für Land- und Forstwirtschaft, Regionen und Wasserwirtschaft bereitet sich aktuell unter Berücksichtigung der sich aus dem Rechnungshofbericht „Management der IT-Sicherheit im Finanzministerium, Klimaschutzministerium und Landwirtschaftsministerium“ (Reihe Bund 2024/16) ergebenden Empfehlungen auf die Umsetzung des aufgrund der NIS-2-Richtlinie noch zu erlassenden nationalen Rechtsaktes vor.

Das Bundesministerium für Land- und Forstwirtschaft, Regionen und Wasserwirtschaft betreibt keine wichtigen Dienste im Sinne des Netz- und Informationssystemsicherheitsgesetzes, BGBl. I Nr. 111/2018, daher erfolgte diesbezüglich keine Umsetzung beziehungsweise Evaluierung.

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 Bundesministerien erfolgt nach Analyse hinsichtlich der Klassifizierung, Kritikalität, Verfügbarkeitsanforderungen und Datenschutzerfordernissen abgestuft lokal, auf ministerieller Infrastruktur, auf Bundesinfrastruktur oder auf Infrastruktur von Drittanbietenden. 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-prozentigen Eigentum des Bundes steht. Als solcher ist er zentraler IT-Dienstleister des Bundes und auf österreichischem Staatsgebiet tätig.

Darüber hinaus gibt es unterschiedliche Projekte, um die Abhängigkeit von Dritten zu reduzieren.

Zur 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 dieser gemäß Art. 2 und 3 DSGVO unterliegen, obliegt den für die jeweilige Datenverarbeitung Verantwortlichen (Art. 24 DSGVO). Dies gilt auch im Falle eines Drittlandbezugs – etwa im Zusammenhang mit der Nutzung von Clouds.

Mag. Norbert Totschnig, MSc

