18295/AB
vom 13.08.2024 zu 18891/J (XXVII. GP)

Bundesministerium
Klimaschutz, Umwelt,
Energie, Mobilität,
Innovation und Technologie

bmk.gv.at

Leonore Gewessler, BA
Bundesministerin

leonore.gewessler@bmk.gv.at
+43 1 711 62-658000
Radetzkystraße 2, 1030 Wien
Österreich

An den
Präsident des Nationalrates
Mag. Wolfgang Sobotka
Parlament
1017 W i e n

Geschäftszahl: 2024-0.444.809

. August 2024

Sehr geehrter Herr Präsident!

Die Abgeordneten zum Nationalrat Hafenecker, MA und weitere Abgeordnete haben am 13. Juni 2024 unter der **Nr. 18891/J** an mich eine schriftliche parlamentarische Anfrage betreffend Wie steht es um die Datensicherheit des Bundes? gerichtet.

Diese Anfrage beantworte ich 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)?*

Mit dem Internet verbundene IT-Systeme sind grundsätzlich zahlreichen, meist automatisierten Angriffsversuchen ausgesetzt. Diese werden durch die IKT-Sicherheitssysteme ebenso weitestgehend automatisiert abgewehrt.
Darüber hinaus ist uns kein erfolgreicher Angriff auf die im Ressort betriebenen Computersystem bekannt. Ein spezieller Cyberangriff auf das Ressort, der nennenswerten Schaden verursacht hätte, wurde nicht beobachtet.

Es darf darüber hinaus auf meine Beantwortung zu PA 18813/J Mögliche Hackerangriffe auf Ihr Ministerium vom 12.06.2024 (XXVII. GP) verwiesen werden.

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 Bundesministerium für Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie (BMK) ist die Abteilung Präsidium 4 – Informations- und Kommunikationstechnik für die Erkennung und Behandlung von Cyberangriffen verantwortlich. Diese Informationen fließen in das durch den gemäß NISG 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 BMK vorrangig des Bundesrechenzentrums (BRZ) und seitens der 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 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 BMK verfolgt bei der Verarbeitung von Daten einen risikobasierten Ansatz. Abhängig von der Schutzwürdigkeit der Daten werden diese gegebenenfalls unter Einsatz starker Verschlüs-

selung und georedundant gespeichert. Je nach Kritikalität der Daten ist der Zugriff auf bestimmte Personengruppen eingeschränkt.

Zu Frage 7:

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

Daten werden im Klimaschutzministerium im risikobasierten Ansatz geschützt. Das BMK 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 genannt die Cyber Sicherheit Steuerungsgruppe (CSS), der Innere Kreis der Operativen Koordinierungsstruktur (IKDOK) bzw. die Operative 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. Bei der Bewertung und Implementierung von Sicherheitsvorkehrungen sowie bei der Meldung von Sicherheitsvorfällen werden die unter NISG §22 genannten Punkte berücksichtigt.
Die Bewertung der Eignung der Sicherheitsmaßnahmen erfolgt auf kontinuierlicher Basis unter Abstützung auf die Risikoeinschätzungen und technischen Empfehlungen des IKDOK und GovCERT.

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 Datenschutzanforderungen 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 und auf österreichischem Staatsgebiet tätig.
Darüber hinaus gibt es unterschiedliche Projekte, um die Abhängigkeit von Dritten zu reduzieren.

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 „[…] jegliches 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." Der Abschluss derartiger Rechtshilfeabkommen obliegt den zuständigen Fachministerien.

Leonore Gewessler, BA

REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR KLIMASCHUTZ, UMWELT, ENERGIE, MOBILITÄT, INNOVATION UND TECHNOLOGIE @ AMTSSIGNATUR	Hinweis	Dieses Dokument wurde amtssigniert.
	Datum	2024-08-13T16:20:02+02:00
	Seriennummer	1871969199
	Aussteller-Zertifikat	CN=a-sign-corporate-05,OU=a-sign-corporate-05,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at/

	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2024-08-13T16:25:31+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	