18861/J
vom 13.06.2024 (XXVII. GP)

ANFRAGE

des Abgeordneten Christian Hafenecker, MA
an den Bundesminister für Finanzen
betreffend **Wie steht es um die Datensicherheit des Bundes?**

Datensicherheit und der Schutz kritischer IT-Infrastruktur sind längst zum Rückgrat einer funktionierenden Bundesverwaltung und in weiterer Folge auch der Republik avanciert. Gerade deshalb lässt ein jüngst publizierter Prüfbericht des Rechnungshofes die Alarmglocken schrillen. [1] Darin werden erhebliche Sicherheitsmängel im IT-Bereich in zumindest drei Ministerien konstatiert.

Verbesserungsbedarf sieht der Rechnungshof jeweils bei den IT-Sicherheitsstrategien des Finanz-, Klimaschutz,- und Landwirtschaftsministeriums. Zudem sei im Bundesministeriengesetz zwar die Kompetenz für die Koordination, aber nicht für die Sicherheit der IT explizit erwähnt. Angesichts von rapide zunehmenden Cyberangriffen auf die öffentliche Verwaltung – der RH spricht allein im ersten Quartal 2023 von über 50 Sicherheitsvorfällen – ist davon auszugehen, dass auch andere Ministerien und Behörden in der Verantwortung des Bundes mit derartigen Gefahren konfrontiert sind und vermutlich nicht adäquat auf diese reagieren können. Und diese Gefahren betreffen nicht nur digitale, sondern auch physische Angriffe, etwa auf kritische Infrastrukturen.

Spätestens seit der Sabotage mehrerer Unterseekabel im Roten Meer im Februar dieses Jahres, bei der weltweite Internetverbindungen massiv gestört wurden, dürfte klar ersichtlich sein, dass die globale Vernetzung im Hardwarebereich äußert fragil ist.[2] Nicht auszuschließen ist, dass durch derartige Anschläge auch administrative Dienstleistungen oder gar militärische Infrastruktur betroffen werden. Zwischenfälle dürften aus österreichischer Sicht nicht zu vermeiden sein, besonders wenn sich wichtige IT-Infrastrukturen und -Lösungen im Ausland befinden, wovon mangels transparenter Informationen seitens der Ministerien und Vergleichswerten aus anderen europäischen Staaten ausgegangen werden muss.

Das betrifft auch den digitalen Bereich, etwa was Daten-Backups, Cloud-Storagelösungen und Datenzentren umfasst. Wenn Ministerien und Behörden hochsensible Daten generieren, speichern, verarbeiten, archivieren und/oder löschen, ist vielfach unklar, ob die dafür in Anspruch genommenen digitalen wie physischen Infrastrukturen (Software, Server), etwa über Clouds, in Österreich oder im Ausland befindlich sind. Bekannt ist lediglich, dass durch das Bundesrechenzentrum (BRZ) Cloudlösungen („GovCloud", „BRZ GoverDrive") angeboten werden, nicht aber, wo diese Daten letztendlich gespeichert werden.[3]

Daher ist das Ausmaß von Vernetzung, Arbeitsteilung bis hin zum kompletten Archivieren der Daten im Stammland des jeweiligen IT-Anbieters oftmals nur ungenügend bekannt. Das wirft weitere Fragen über Zugriffsmöglichkeiten, Sicherheit

[1] https://www.rechnungshof.gv.at/rh/home/news/Meldungen_2024/IT_Sicherheit_in_Ministerien.html
[2] https://www.handelsblatt.com/technik/it-internet/seekabel-im-roten-meer-durchtrennt-bedrohung-fuer-das-internet-in-europa-waechst-01/100020900.html
[3] https://www.brz.gv.at/was-wir-tun/geschaeftsfelder/cloud-solutions.html

und Autonomie im Bereich der IT-Sicherheit auf. Kommt es etwa zu breitangelegten Cyberangriffen auf Verwaltungs-IT-Infrastrukturen, bestünde durchaus auch die realistische Gefahr des Verlustes von hochsensiblen sozialen Daten, was in weiterer Folge etwa eine Auszahlung von Sozialleistungen verunmöglicht (Arbeitslosengeld, Pensionen usw.).

Der sogenannte „Cloud Act" der USA verpflichtet beispielsweise amerikanische Internet-Firmen und IT-Dienstleister, den US-Behörden auch dann Zugriff auf gespeicherte Daten zu gewährleisten, wenn die Speicherung nicht in den USA erfolgt. Sofern das Unternehmen seinen Sitz in den USA hat bzw. dem US-amerikanischen Recht unterliegt, haben Behörden Zugriff auf sämtliche Unternehmens- und Kundendaten von Cloud- und Kommunikationsanbietern. Der „Cloud Act" steht damit im krassen Gegensatz zur Europäischen Datenschutzgrundverordnung (DSGVO), die dem personenbezogenen Datenschutz höchste Priorität beimisst. Für Unternehmen, besonders aber auch Behörden, die ihre Cloud über Anbieter mit Sitz in den USA beziehen, stellt dies ein enormes Sicherheitsrisiko dar. Ähnliche Gefahren dürften bei IT-Anbietern existieren, die aus anderen außereuropäischen Staaten operieren, etwa aus China.

Strategisch aktive Nationen wie Großbritannien schützen ihre administrativen Daten zumindest soweit, als sie etwa US-Techfirmen ausschließlich auf eigenem Territorium Daten zur Verarbeitung überlassen.[4] Auch Israel handhabt dies im Bereich Cloud und Rechenzentren so.[5] Wiederum ist hier die Situation in Österreich unklar.

In diesem Zusammenhang stellt der unterfertigte Abgeordnete an den Bundesminister für Finanzen folgende

Anfrage

1. 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)?
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?
3. 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)?

[4] https://www.theguardian.com/uk-news/2021/oct/26/amazon-web-services-aws-contract-data-mi5-mi6-gchq
[5] https://www.reuters.com/technology/amazon-invest-72-bln-israel-launches-aws-cloud-region-2023-08-01/

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?
5. 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?
6. 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)?
7. Welche konkreten Maßnahmen und Sicherheitsstrategien verfolgt Ihr Ressort, um möglichen Missbrauch mit Daten durch Dritte zu verhindern?
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?
9. Wie ist der Stand der NIS-Richtlinien-Umsetzung in Ihrem Ministerium?
10. 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?
11. Gibt es Anstrengungen, Vorhaben oder Überlegungen, die Datenverarbeitung seitens der Bundesverwaltung in Österreich zu bewerkstelligen?
12. Welche Datenarchive im Wirkungsbereich des Bundes liegen im Ausland (Bitte um Auflistung)?
13. 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?
14. Welche Position nimmt die Bundesregierung zum US-„Cloud Act“ in Hinblick auf die DSGVO ein?

Sollten einzelne Antworten einer Vertraulichkeit bzw. Geheimhaltung unterliegen, wird ersucht, diese unter Einhaltung des Informationsordnungsgesetzes klassifiziert zu beantworten.

	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2024-06-13T15:44:38+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	