



Parlamentarischer Vorstoss

Vorstoss-Nr.: 166-2023
Vorstossart: Interpellation
Richtlinienmotion: ☐
Geschäftsnummer: 2023.RRGR.232

Eingereicht am: 22.08.2023

Fraktionsvorstoss: Nein
Kommissionsvorstoss: Nein
Eingereicht von: Reinhard (Thun, FDP) (Sprecher/in)

Weitere Unterschriften: 0

Dringlichkeit verlangt: Ja
Dringlichkeit gewährt: Nein 12.09.2023

RRB-Nr.: vom
Direktion: Finanzdirektion
Klassifizierung: Nicht klassifiziert

Datensicherheit und Datenspeicherung

In der heutigen, zunehmend vernetzten Welt sind Datensicherheit und die Strategie zur Datenspeicherung zentrale Themen, die sowohl die öffentliche Verwaltung als auch die Wirtschaft betreffen.

Durch die täglichen medialen Meldungen von Hackerangriffen oder Datenlecks ist man verführt zu meinen, dass alle Probleme dadurch gelöst werden, alle Daten auf einem eigenen Server zu halten. Die Wahl zwischen der Speicherung von Daten auf einem eigenen Server oder in der Cloud ist aber viel mehr als eine technische Entscheidung; sie hat weitreichende Auswirkungen auf die Sicherheit, Compliance und Effizienz unserer digitalen Infrastruktur. Der Kanton Bern steht vor der Herausforderung, eine Strategie zu entwickeln, die sowohl den aktuellen Anforderungen als auch den zukünftigen Entwicklungen gerecht wird. Die heutige Speicherung von Daten bei der BEDAG und die sichere Übertragung zwischen Benutzer und Server sind nur ein Teil des Gesamtbildes. Die Entscheidung zwischen einem eigenen Server und einer Cloud-Lösung erfordert eine sorgfältige Abwägung von Verantwortlichkeiten, Risiken und Chancen. Die grössten Risiken sind bei der Übermittlung der Daten zwischen dem User bzw. Endgerät und der Datenspeicherung vorhanden. Hier bedarf es einer effizienten Verschlüsselung. Ein weiteres nicht zu unterschätzendes Risiko ist der Mensch selbst. Wenn man also beispielsweise meint, dass bei einer Microsoft-Cloud die Daten durch eine unerwünschte Person gelesen werden können, so ist dies auch mit der heutigen Lösung möglich. Cloud-Technologie bietet Flexibilität und Skalierbarkeit, aber sie erfordert auch eine klare Strategie in Bezug auf Verschlüsselung, Compliance und Risikomanagement. Die Auswahl eines Cloud-Anbieters, ob in der Schweiz oder im Ausland, sollte deshalb auf einer gründlichen Analyse der Bedürfnisse und der regulatorischen Anforderungen basieren.

Der Regierungsrat wird um Beantwortung folgender Fragen gebeten:

1. Ist es sinnvoll, dass jeder Kanton individuell prüft, ob und unter welchen Bedingungen Cloud-Anbieter genutzt werden können? Gab es einen Austausch mit anderen Kantonen oder dem Bund zu diesem Thema? Könnten wir von den Erfahrungen anderer Kantone oder des Bundes profitieren?
2. Wie ist die Zusammenarbeit und Kommunikation mit der Digitalen Verwaltung Schweiz (DVS) in Bezug auf dieses Thema?
3. Wer ist im Kanton Bern verantwortlich für die Risikobewertung bei der Nutzung von Cloud-Diensten durch die kantonale Verwaltung?
4. Welche Kriterien liegen dieser Risikobewertung zugrunde?
5. Welche Ergebnisse hat die Risikobewertung ergeben? Was sind die Ergebnisse der Bewertung des Supply-Chain-Risikos bei der Nutzung von Cloud-Diensten (inkl. der aktuellen Anbieter)?
6. Wer trägt im Kanton Bern letztlich die Verantwortung für die Datensicherheit und den Datenschutz bei der Nutzung von Cloud-Diensten? Wie wird die Einhaltung der festgelegten Regeln kontrolliert?
7. Welche KPIs werden zur Messung einer sicheren und effizienten Nutzung von Cloud-Diensten herangezogen?
8. Wie beurteilt der Kanton die Anwendbarkeit des neuen Datenschutzgesetzes des Bundes auf kantonale Angelegenheiten?

Begründung der Dringlichkeit: Aktuell werden viele IT-Projekte umgesetzt oder zur Beschaffung empfohlen. Diese Fragen helfen mit, eine Beurteilung für die Entscheidungsfindung von zukünftigen Projekten zu schaffen. Schlussendlich schafft Transparenz auch ein Sicherheitsgefühl der Bevölkerung.

Verteiler

– Grosser Rat