Parlamentarischer Vorstoss

Antwort des Regierungsrates

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.:	167/2024	vom 21. Februar 2024
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.

Antwort des Regierungsrates

Der Regierungsrat teilt die Meinung des Interpellanten, dass die fortschreitende Digitalisierung von Gesellschaft, Wirtschaft und Verwaltung die Gewährleistung der Informationssicherheit immer herausfordernder macht, dass ein risikobasierter Ansatz zum Umgang mit diesen Herausforderungen erforderlich ist und dass diese Herausforderungen im Verbund mit anderen Behörden am wirksamsten angegangen werden können. Aus diesen Gründen legte der Regierungsrat dem Grossen Rat im August 2023 den Entwurf eines Gesetzes über die Informations- und Cybersicherheit (ICSG) vor. Für eine vertiefte Auseinandersetzung mit den hier aufgeworfenen Fragen verweist der Regierungsrat auf die Materialien zu diesem Gesetz (s. www.be.ch/icsg), weshalb er die Fragen hier relativ knapp beantwortet.

1. *Ist es sinnvoll, dass jeder Kanton individuell prüft, ob und unter welchen Bedingungen Cloud-Anbieter genutzt werden können?*

   Obwohl sich diese und andere Fragen nur auf Cloud-Anbieter beziehen, stellen sich die hier aufgeworfenen Informationssicherheitsfragen aus der Sicht des Regierungsrates in weitgehend gleicher Weise bei allen Auftragsdatenbearbeitungen für Behörden durch Dritte, unabhängig davon, ob sie als Cloud-Service oder in konventionellen Rechenzentren angeboten

werden. Aus der Sicht des Regierungsrates ist die relevante Frage daher, unter welchen Sicherheits- und Datenschutzbedingungen Behörden überhaupt Dritte mit der Bearbeitung behördlicher Daten beauftragen sollen, ob in einer Cloud oder nicht.

Aus einer Sicherheitsperspektive ist es tatsächlich nicht sinnvoll, wenn jeder Kanton und der Bund diese Frage separat zu beantworten versuchen, zumal die Risiken und die Rahmenbedingungen überall dieselben sind. Landesweit einheitliche gesetzliche Regeln über Informationssicherheit und Datenschutz (ISDS) würden die Ausbildung des Personals sowie die Umsetzung und die Kontrolle der Regeln stark vereinfachen. Leider fehlt auf Bundesebene die verfassungsrechtliche Grundlage für die Vereinheitlichung des Informationssicherheits- und Datenschutzrechts in der Schweiz. Der Regierungsrat setzt sich daher dafür ein, dass die Kantone und der Bund sich bei ihrer Gesetzgebung aneinander sowie an nationalen und internationalen Standards orientieren.

Gab es einen Austausch mit anderen Kantonen oder dem Bund zu diesem Thema? Könnten wir von den Erfahrungen anderer Kantone oder des Bundes profitieren?

Die Sicherheits- und Datenschutzfachbehörden des Kantons stehen laufend im Austausch mit ihren Kolleginnen und Kollegen im Bund und in den anderen Kantonen, um von ihren Erfahrungen zu profitieren.

2. *Wie ist die Zusammenarbeit und Kommunikation mit der Digitalen Verwaltung Schweiz (DVS) in Bezug auf dieses Thema?*

   Die DVS ist noch im Aufbau. Sie verfügt aber bereits über eine Arbeitsgruppe Informations- und Cybersicherheit. Diese hat die Aufgabe, Best Practice-Regeln zu erarbeiten, Sicherheitsaspekte neuer Technologien und Trends zu beurteilen und Massnahmen zur Risikominderung zu empfehlen.

3. *Wer ist im Kanton Bern verantwortlich für die Risikobewertung bei der Nutzung von Cloud-Diensten durch die kantonale Verwaltung?*

   Verantwortlich für ISDS, und damit auch für die Risikobewertung, sind die Behörden, die Daten bearbeiten oder durch Dritte bearbeiten lassen. Diese Behörden sind namentlich das Amt für Informatik und Organisation (KAIO) für die von ihm angebotene ICT-Grundversorgung (z. B. kantonales Netzwerk, kantonaler Arbeitsplatz), die Fachämter der Kantonsverwaltung für die von ihnen verantworteten Fach- und Konzernapplikationen sowie die anderen Behörden im Kanton (wie Gemeinden, Hochschulen, Anstalten) für die von ihnen eingesetzten ICT-Mittel.

4. *Welche Kriterien liegen dieser Risikobewertung zugrunde?*

   Risiken werden nach dem Umfang des Schadens für das geschützte Gut – die zu wahrenden öffentlichen Interessen bzw. die Grundrechte der betroffenen Personen – bewertet, der eintreten kann, wenn sich das Risiko verwirklicht, und nach der Wahrscheinlichkeit, dass das Risiko eintritt. Massgeblich für den Schadensumfang sind die Schutzziele der Informationssicherheit (Vertraulichkeit, Verfügbarkeit, Integrität) und des Datenschutzes (Vertraulichkeit, Richtigkeit, Rechtmässigkeit, Verhältnismässigkeit), ebenso wie weitere Schadenspotenziale wie Schaden von Personen bzw. Persönlichkeitsrechten oder an Sachen, finanzieller Schaden oder Reputationsschaden. Zur Risikobewertung gehört auch die Überprüfbarkeit der Massnahmen, mit denen die (sog. Brutto-) Risiken beseitigt oder auf ein tragbares Mass (Restrisiken) gesenkt werden sollen.

5. *Welche Ergebnisse hat die Risikobewertung ergeben?*

   Die Risikobewertung muss von der verantwortlichen Behörde (s. zu Frage 3) für jede Datenbearbeitung bzw. jedes ICT-Mittel neu durchgeführt werden, abhängig von den Zielen und Rahmenbedingungen des jeweiligen Vorhabens. Daher gibt es nicht eine einzige Risikobewertung, deren Ergebnisse hier vorgestellt werden können. Im Hinblick auf die Einführung von M365 in der Kantonsverwaltung sind die Ergebnisse im Bericht «Restrisiken beim Einsatz von M365» an den Regierungsrat ausgewiesen, und er hat die Risiken am 30. Juni 2023[1] akzeptiert.

   Was sind die Ergebnisse der Bewertung des Supply-Chain-Risikos bei der Nutzung von Cloud-Diensten (inkl. der aktuellen Anbieter)?

   Das Supply-Chain-Risiko (also das Risiko, dass Leistungen wegen unterbrochener Lieferketten nicht mehr verfügbar sind) ist wie jedes Risiko im Einzelfall zu beurteilen. Grundsätzlich sind aber grosse internationale Cloud-Anbieter («Hyperscaler») wegen ihrer Grösse, ihrer globalen geografischen Aufstellung und ihrer Fähigkeit, ihre Leistungen zu skalieren, weniger anfällig auf Lieferkettenrisiken als andere Anbieter.

6. *Wer trägt im Kanton Bern letztlich die Verantwortung für die Datensicherheit und den Datenschutz bei der Nutzung von Cloud-Diensten?*

   Siehe oben zu Frage 3. Für den Datenschutz ist jene Behörde verantwortlich, die Personendaten zur Erfüllung ihrer gesetzlichen Aufgaben bearbeitet oder bearbeiten lässt (Art. 8 KDSG). Bei der kantonalen ICT-Grundversorgung ist zwar das KAIO dafür verantwortlich, dass die Dienste rechtskonform und sicher genutzt werden können, aber ob dies tatsächlich geschieht, liegt in der Verantwortung der die Leistungen nutzenden Direktionen und Ämter.

   Wie wird die Einhaltung der festgelegten Regeln kontrolliert?

   Die verantwortlichen Behörden kontrollieren die Einhaltung der ISDS-Vorschriften durch die Leistungserbringer mit risikoangemessenen, vertraglich vereinbarten Kontrollinstrumenten, wie
   - einer laufenden Berichterstattung durch die Leistungserbringer über die ergriffenen Sicherheitsmassnahmen und sicherheitsrelevante Ereignisse,
   - der Herausgabe von Auditberichten und anderen Sicherheitsunterlagen durch die Leistungserbringer, oder
   - der Durchführung von Sicherheitsaudits bei den Leistungserbringern.

7. *Welche KPIs werden zur Messung einer sicheren und effizienten Nutzung von Cloud-Diensten herangezogen?*

   Die Leistungskennzahlen (*key performance indicator,* KPI) werden im Einzelfall abhängig von den Anforderungen des Geschäftsfalls festgelegt. Zu ihnen gehören etwa die Verfügbarkeit bzw. die maximale Ausfallrate sowie die Reaktions- oder Störungsbehebungszeit im Störungsfall. Weil es aber in der Natur von Cloud-Leistungen liegt, dass sie hoch standardisiert statt individuell auf die Bedürfnisse der Kundschaft angepasst erbracht werden, besteht bei Cloud-Leistungen oft wenig Spielraum für das Festlegen von KPIs durch die Kundschaft.

[1] Medienmitteilung und Bericht unter: Berner Kantonsverwaltung führt Microsoft 365 ein

8. *Wie beurteilt der Kanton die Anwendbarkeit des neuen Datenschutzgesetzes des Bundes auf kantonale Angelegenheiten?*

   Das Datenschutzgesetz des Bundes (DSG) ist auch in seiner neuen Fassung vom 25. September 2020 auf Datenbearbeitungen durch kantonale und kommunale Behörden nicht anwendbar. Das ergibt sich aus (Art. 2 Abs. 1 DSG), wonach das DSG nur für Datenbearbeitungen durch private Personen und Bundesorgane gilt. Der Datenschutz bei Datenbearbeitungen durch kantonale und kommunale Behörden richtet sich daher nach dem kantonalen Datenschutzgesetz (KDSG).

Verteiler
– Grosser Rat