Parlamentarischer Vorstoss. Antwort des Regierungsrates

Vorstoss-Nr.:	115-2016
Vorstossart:	Interpellation
Richtlinienmotion:	☐
Geschäftsnummer:	2016.RRGR.593
Eingereicht am:	05.06.2016
Fraktionsvorstoss:	Nein
Kommissionsvorstoss:	Nein
Eingereicht von:	Graber (La Neuveville, SVP) (Sprecher/in)
Weitere Unterschriften:	0
Dringlichkeit verlangt:	Nein
Dringlichkeit gewährt:	
RRB-Nr.:	1378/2016 vom 7. Dezember 2016
Direktion:	Finanzdirektion
Klassifizierung:	Nicht klassifiziert

Datensicherheit

Am 12. Mai 2016 berichteten die Medien, dass Hacker bei einem Cyber-Spionage-Angriff zweifellos sehr vertrauliche Daten, die der Bund bei der RUAG gelagert hatte, entwendet haben. Zu diesem äusserst bedauerlichen Vorfall konnte es kommen, weil das Bundesamt für Informatik und Telekommunikation (BIT) im vergangenen Jahr sämtliche Personaldaten des Bundes an den bundeseigenen Rüstungskonzern RUAG geliefert hat. Bei diesem Hackerangriff könnten auch die Personalien von Mitarbeitern des Nachrichtendienstes in ausländische Hände geraten sein.

Bei diesem Vorfall stellt sich einmal mehr das Problem der Sicherheit von Daten, die von öffentlich-rechtlichen Körperschaften verwaltet und bearbeitet werden.

Es ist unerlässlich, dass sich die Personen, deren Daten von der Kantonsverwaltung registriert, bearbeitet und aufbewahrt werden, darauf verlassen können, dass diese Daten vollständig gesichert sind und nicht durch unglückliche Umstände durch Einzelpersonen oder Personengruppen mit unlauteren und inakzeptablen Absichten entwendet werden können.

Dieser Vorfall der Bundesdaten, die in unberechtigte Hände gefallen sind, wirft Fragen auf.

Der Regierungsrat wird um Beantwortung folgender Fragen gebeten:

1. Wo werden die digitalisierten Daten der Einwohnerinnen und Einwohner des Kantons Bern, die Daten der Angestellten des öffentlichen Dienstes sowie die Daten weiterer Bevölkerungskategorien, welche die Kantonsbehörden richtigerweise und zu Recht besitzen, aufbewahrt?

2. Welche Massnahmen hat der Regierungsrat ergriffen, um sicherzustellen, dass diese Daten nicht an unbefugte Personen oder Personengruppen gelangen?

3. Hat der Vorfall auf Bundesebene bewirkt, dass der Kanton zusätzliche Massnahmen vorsieht, um die Sicherheit der sich in seinem Besitz befindlichen digitalen Daten zu gewährleisten?

Zusatzbemerkung: Selbstverständlich verlangen wir vom Regierungsrat keine Auskünfte, die er uns aus Sicherheitsgründen nicht geben kann.

Antwort des Regierungsrates

Zu Frage 1:

Personendaten werden in vielen einzelnen Applikationen der Verwaltung bearbeitet. Diese gliedern sich wie folgt:

- Fachapplikationen werden zur Unterstützung von spezialisierten Verwaltungsprozessen oder Anforderungen eingesetzt.
- Konzernapplikationen unterstützen wesentliche Verwaltungsprozesse und breit abgestützte Anforderungen. Sie stehen der ganzen Verwaltung zur Verfügung.
- Die ICT-Grundversorgung dient der ganzen Verwaltung und umfasst ICT-Systeme und ICT-Dienstleistungen in den Bereichen Arbeitsplatz, Netzwerk und Kommunikation, einschliesslich der für den Betrieb aller Applikationen erforderlichen Server.

Die Verantwortung für die Fach- und Konzernapplikationen liegt bei der jeweiligen Direktion bzw. beim jeweiligen Fachamt. Die Verantwortung für die zentralen ICT-Systeme und ICT-Leistungen der Grundversorgung liegt beim Amt für Informatik und Organisation (KAIO).

Der Regierungsrat hat in seiner Antwort auf die Interpellation 297-2013, Sancar (Bern, Grüne) „Wo sind die die hoch vertraulichen und sensiblen Daten des Kantons Bern gelagert?“ bereits darauf hingewiesen, dass ein Grossteil der sensitiven Daten der Verwaltung, namentlich die Daten des Personal-, Finanz- und Steuerwesens sowie die harmonisierten Daten der Einwohner- und Stimmregister in den Schweizerischen Rechenzentren der kantonseigenen Bedag Informatik AG bearbeitet und gespeichert werden. Ein zentrales, öffentlich zugängliches Register unter http://www.jgk.be.ch/jgk/de/index/aufsicht/datenschutz/register_der_datensammlungen.html gibt über die Datensammlungen Auskunft.

Die ICT-Strategie 2016 – 2020 des Kantons Bern sieht vor, dass alle Applikationen der Verwaltung zentral betrieben werden. Diese Leistung erbringt das KAIO im Rahmen der ICT-Grundversorgung durch Applikationsplattformen. Diese werden zurzeit durch die kantonseigene Bedag Informatik AG an redundanten Standorten in der Schweiz betrieben. Erst mit dem Abschluss des Programms IT@BE, voraussichtlich im Jahr 2021, wird die Strategie umgesetzt sein und damit auch die Überführung aller Applikationen auf die zentralen Applikationsplattformen und die Schaffung eines Applikationsportfolios zum Überblick über alle Applikationen. Erst dann wird es möglich sein, Auskunft über den Ort der elektronischen Bearbeitung aller Daten der Verwaltung zu geben. Weil die ICT-Strategie die Kantonspolizei und die Schulen im Zuständigkeitsbereich der Gesundheits- und Fürsorgedirektion von der Pflicht der Nutzung der Grundversorgung ausnimmt, werden aber auch in Zukunft keine zentralen Aussagen über die Datenbearbeitungen dieser Organisationen möglich sein.

Zu Frage 2:

Die verantwortliche Behörde, die Personendaten bearbeitet oder ein Datenkommunikationsnetz zur Verfügung stellt, sorgt mit technischen und organisatorischen Massnahmen für die Vertraulichkeit, die Verfügbarkeit und die Richtigkeit der Daten. Die technischen und organisatorischen Vorgaben sind in Art. 4 und 5 der Datenschutzverordnung vom 22. Oktober 2008 (DSV, BSG 152.040.1) genannt. Für die Gewährleistung der Informationssicherheit und des Datenschutzes (ISDS) ist die Behörde verantwortlich, die Personendaten zur Erfüllung ihrer gesetzlichen Aufgaben bearbeitet oder durch Dritte bearbeiten lässt.

Die Datenschutzgesetzgebung und die ISDS-Vorschriften der Verwaltung sehen Folgendes vor: Die verantwortliche Stelle prüft mit einer ISDS-Analyse, ob ein erhöhter Schutzbedarf besteht. In diesem Fall erstellt sie ein ISDS-Konzept und legt darin fest, wer auf die Daten in welcher Weise zugreifen darf und welche Informationsschutzmassnahmen zu ergreifen sind. In den von der Gesetzgebung vorgesehenen Fällen, in denen ein besonders hohes ISDS-Risiko besteht, prüft zudem die unabhängige kantonale Datenschutzaufsichtsstelle vor dem Beginn der Datenbearbeitung im Rahmen eines Vorabkontrollverfahrens, ob die Datenschutzgesetzgebung und die ISDS-Vorschriften eingehalten sind.

Nebst der Überprüfung der ISDS-Vorschriften und der Einhaltung der Datenschutzgesetzgebung müssen externe ICT-Dienstleister im Rahmen standardisierter vertraglicher Vereinbarungen mit dem Kanton in der Regel Geheimhaltungsklauseln und weitere Verpflichtungen zur Erfüllung technischer und organisatorischer Massnahmen gewährleisten, welche einen Missbrauch von Daten unterbinden sollen und im Verletzungsfall Konventionalstrafen nach sich ziehen würden.

Zu Frage 3:

Der genannte Vorfall hatte keine zusätzlichen Massnahmen zur Folge, weil das KAIO gemeinsam mit den Direktionen bereits vorher die Informationssicherheitslage laufend überwachte. Zusammen mit seinen Lieferanten, vor allem Bedag Informatik AG (Rechenzentrum), SPIE ICS (Netzwerk) und Swisscom (Telefonie) hat es bereits verschiedene technische und organisatorische Massnahmen zur Verbesserung der Sicherheit umgesetzt, oder solche befinden sich in der Realisierung. Dazu gehören die folgenden:

- Die Sensibilisierung und Schulung der Mitarbeitenden für Anliegen der Sicherheit und des Datenschutzes erhält ein zunehmendes Gewicht.

- Die laufende Überprüfung sowie die kontinuierliche Verbesserung und Weiterentwicklung der Sicherheitssysteme sind eine Daueraufgabe der ICT-Organisation des Kantons.

- Die Betreiberin der Applikationsplattformen des Kantons, die Bedag Informatik AG, ist nach der internationalen Norm ISO/IEC 27001 zertifiziert. Diese Norm regelt die Anforderungen an ein Informationssicherheits-Managementsystem (ISMS). Mit der Zertifizierung nach ISO/IEC 27001 stellt eine Organisation unter Beweis, dass sie geeignete organisatorische und technische Massnahmen zur Gewährleistung eines angemessenen Sicherheitsniveaus im ICT-Betrieb lebt. Auch das KAIO als ICT-Grundversorger wird voraussichtlich ab 2017 nach dieser Norm zertifiziert sein. Damit werden alle sicherheitsrelevanten Aspekte der kantonalen ICT-Grundversorgung durch ein ISMS gesteuert, das sicherstellt, dass Sicherheitsrisiken systematisch erfasst und behandelt werden.

- Restrisiken und unerlaubte Datenzugriffe können nie vollständig ausgeschlossen, jedoch mit organisatorischen und technischen Massnahmen im Kanton Bern auf ein vertretbares Minimum reduziert werden.

Verteiler
- Grosser Rat