Parlamentarischer Vorstoss. Antwort des Regierungsrates

Vorstoss-Nr.:	060-2015
Vorstossart:	Interpellation
Richtlinienmotion:	☐
Geschäftsnummer:	2015.RRGR.199
Eingereicht am:	19.02.2015
Fraktionsvorstoss:	Nein
Kommissionsvorstoss:	Nein
Eingereicht von:	Streit-Stettler (Bern, EVP) (Sprecher/in)
Weitere Unterschriften:	0
Dringlichkeit verlangt:	Nein
Dringlichkeit gewährt:	
RRB-Nr.:	903/2015 vom 12. August 2015
Direktion:	Finanzdirektion
Klassifizierung:	Nicht klassifiziert

Ist die Informatiksicherheit in der Berner Kantonsverwaltung gewährleistet?

Dem Daten- und Informationsschutz kommt innerhalb der Berner Kantonsverwaltung unbestritten eine hohe Bedeutung zu. Heute erfolgt der Austausch von Daten jedoch fast ausschliesslich auf elektronischem Weg. Dementsprechend setzt ein wirksamer Datenschutz fast immer auch die Sicherheit der Informatik voraus. In diesem Zusammenhang stellt sich die Frage, inwiefern in der Berner Kantonsverwaltung die Aufsicht über die Informatiksicherheit wirksam und unabhängig funktioniert. Während die Datenschutzaufsichtsstelle eine unabhängige Aufsichtsbehörde ist, untersteht der Informationssicherheitsbeauftragte des Kantons (IT-SIBE) der Leitung des KAIO und kann daher seine wichtige Aufsichtsfunktion nur beschränkt wahrnehmen.

Der Regierungsrat wird um Beantwortung folgender Fragen gebeten:

1. Die Direktionsverordnung über Informationssicherheit und Datenschutz (ISDS DV) legt in Artikel 10 fest, dass die kantonale Datenschutzaufsichtsstelle mit der IT-SIBE zusammenarbeitet. Wie läuft diese Zusammenarbeit institutionell ab?

2. Ist der Regierungsrat auch der Meinung, dass die Datenaufsichtsstelle und der IT-SIBE eng zusammenarbeiten müssen?

3. In Artikel 11 der bereits erwähnten Verordnung heisst es, dass jede Direktion ein/e Informationssicherheitsverantwortliche/n (IT-SIVE) als Kontaktstelle des IT-SIBE bezeichnet. Inwiefern wird dieser Weisung nachgelebt? Wie funktioniert die Zusammenarbeit zwischen IT-

SIBE und IT-SIVE? Wie viele Stellenprozente sind in den jeweiligen Direktionen dafür eingestellt? Sind sämtliche Direktionen damit ausgerüstet?

4. Welche Kompetenzen hat der IT-SIBE, wenn eine Direktion bzw. eine Dienststelle seinen Weisungen nicht nachkommt?

5. Inwiefern wird in der Berner Kantonsverwaltung dafür gesorgt, dass neue Informatikprojekte bzw. -anwendungen routinemässig auf Sicherheitsaspekte überprüft werden?

6. Inwiefern ist die Unabhängigkeit des IT-SIBE als Aufsichtsperson innerhalb des KAIO gewährleistet?

7. Wäre eine Integration des IT-SIBE in die Datenschutzaufsichtsstelle aus Sicht des Regierungsrats denk- bzw. wünschbar?

Antwort des Regierungsrates

1. Informationssicherheit und Datenschutz (ISDS) sind kritische Erfolgsfaktoren des Einsatzes von Informations- und Kommunikationstechnik (ICT). Der Datenschutz (DS) hat das Ziel, Personen vor missbräuchlicher Datenbearbeitung durch Behörden zu schützen. Die Informationssicherheit (IS) umfasst die Vertraulichkeit, Verfügbarkeit und Integrität der bearbeiteten Informationen.

   Die Einhaltung von IS und DS bei der Bearbeitung von personenbezogenen Daten durch die Verwaltung werden durch die verwaltungsunabhängige Datenschutzaufsichtsstelle (DSA) beaufsichtigt. Die Gewährleistung der IS bei der Bearbeitung von nicht personenbezogenen Daten wird durch die oder den kantonalen IT-Sicherheitsbeauftragten (IT-SIBE) des Amtes für Informatik und Organisation (KAIO) beaufsichtigt.

   Die Einhaltung von IS und DS ist stark voneinander abhängig: So kann etwa der Datenschutz nicht gewährleistet werden, wenn die Informationssicherheit verletzt ist. Zudem wenden beide oft gleiche Massnahmen an, um ihre Ziele effizient zu erreichen. Eine ISDS-konforme und wirtschaftliche Umsetzung von Vorhaben der kantonalen Verwaltung bedingt damit eine enge Zusammenarbeit zwischen DSA und IT-SIBE. Deshalb legt die ISDS DV im Artikel 10 fest, dass die DSA mit der oder dem IT-SIBE zusammenarbeitet und durch den oder die IT-SIBE bei ihrer Aufsicht unterstützt wird.

   Alle ICT-Projekte und -Anwendungen der kantonalen Verwaltung müssen unabhängig von ihrem Schutzbedarf den Anforderungen eines einheitlichen Grundschutzes entsprechen. Dieser Grundschutz wird durch den IT-SIBE beaufsichtigt und überprüft. Projekte mit erhöhtem Schutzbedarf werden zusätzlich wie in Art. 17a des Datenschutzgesetzes (KDSG) vorgesehen einer Vorabkontrolle durch die DSA unterzogen. Dabei kann die DSA die Einhaltung des Grundschutzes bereits voraussetzen.

   Gemäss Art. 6 ISDS DV müssen Anträge auf Kreditbewilligungen und Unterlagen zur Vorabkontrolle die erarbeiteten ISDS-Unterlagen enthalten. Bei erhöhten ISDS-Anforderungen müssen diese Unterlagen sowohl der DSA als auch dem IT-SIBE unterbreitet werden. Beide prüfen die ISDS-Unterlagen auf die Einhaltung der ISDS-Vorgaben in ihrem Verantwortungsbereich. Fehlen die ISDS-Unterlagen oder ergibt sich aus ihnen, dass IS oder DS nicht ge-

währleitet sind, darf vor der Behebung der Mängel keine Inbetriebnahme erfolgen (Art. 7 ISDS DV).

2. Ja. Eine enge und konstruktive Zusammenarbeit zwischen DSA und IT-SIBE, wie sie heute erfolgt, ist notwendig für eine wirksame und wirtschaftliche Umsetzung der ISDS-Vorschriften.

   Die Datenschutzaufsichtsstelle ist eine regierungsunabhängige Aufsichtsstelle. Nach unserem Wissensstand geht sie aber ebenfalls von der Wichtigkeit einer engen Zusammenarbeit aus.

3. Die Direktionen, die Staatskanzlei und die Justiz (DIR/STA/JUS) und die Finanzkontrolle setzen gemäss eigenen Angaben folgende Personalressourcen für die Rolle der oder des IT-Sicherheitsverantwortlichen (IT-SIVE) ein:

Staatskanzlei	3%
Volkswirtschaftsdirektion des Kantons Bern	30%
Gesundheits- und Fürsorgedirektion	10%
Justizverwaltung	10%
Justiz-, Gemeinde- und Kirchendirektion	50%
Polizei- und Militärdirektion (ohne Kantonspolizei)	30%
Kantonspolizei	5%
Finanzdirektion	50%
Erziehungsdirektion	40%
Bau-, Verkehrs- und Energiedirektion	35%
Finanzkontrolle	2%

   Die oder der IT-Sicherheitsbeauftragte (IT-SIBE) besetzt eine 100%-Stelle im KAIO. Ein wichtiges institutionelles Arbeitsmittel des IT-SIBE sowie der IT-SIVE der DIR/STA/JUS ist die Fachgruppe Informationssicherheit (FG IS) der Kantonalen Informatikkonferenz (KIK), dem Koordinations- und Konzeptgremium für gesamtstaatliche Fragen des ICT-Einsatzes.

   Die von der oder dem IT-SIBE geleitete FG IS ist das kantonale Fachgremium für Informationssicherheit. Sie stellt die Aktualisierung und den Vollzug der IS-Vorschriften sicher, verfolgt die Entwicklung der Informationssicherheit und erarbeitet Hilfsmittel und Vorschriften. Die IT-SIVE der DIR/STA/JUS sind stimmberechtigte Mitglieder. Die DSA ist in der FG IS beratend vertreten.

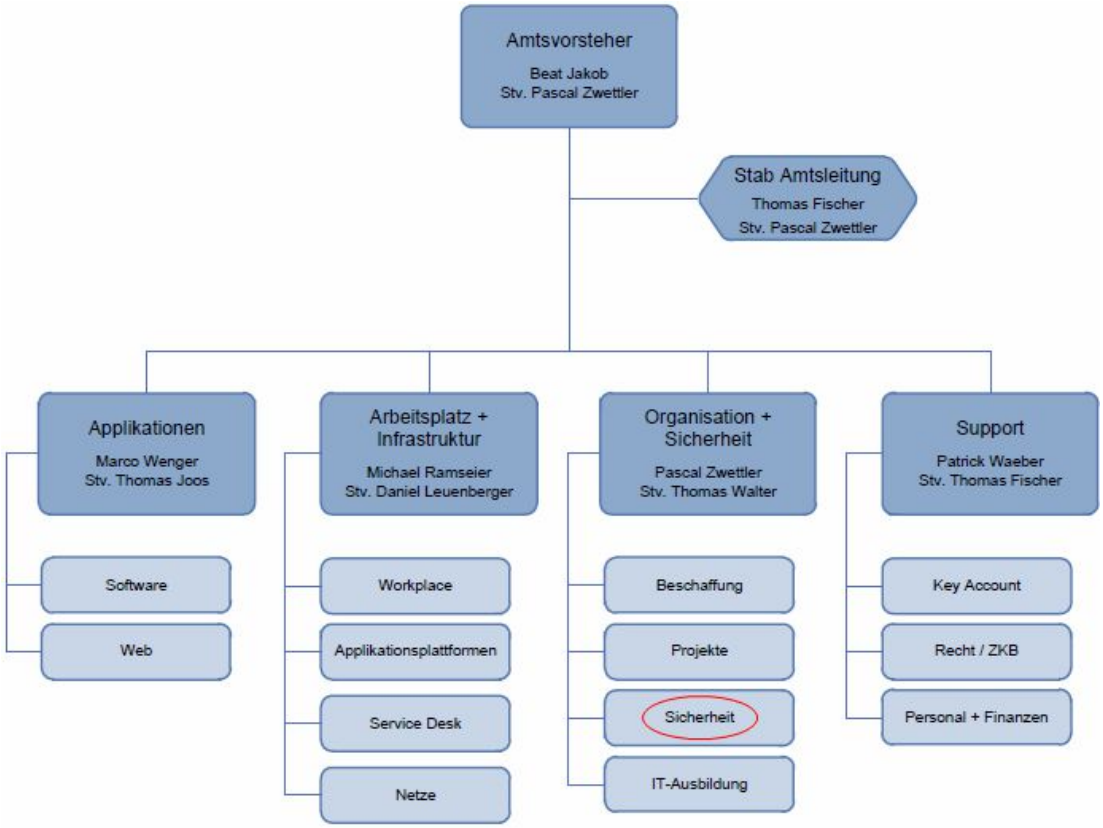
4. Die oder der IT-SIBE hat keine kantonsweite Weisungsbefugnis. Setzt eine Verwaltungsstelle ISDS-Vorschriften nicht um, so kann die oder der IT-SIBE dies im Rahmen der Kenntnisnahme von ISDS-Unterlagen gemäss Art. 6 ISDS DV oder im Rahmen ihrer bzw. seiner Aufsichtsaufgabe nach Art. 10 Abs. 3 ISDS DV feststellen, und kann der vorgesetzten Stelle oder - als Leiterin oder Leiter der FG IS - darüber der KIK Bericht erstatten. Die DIR/STA/JUS entscheiden im Rahmen ihrer Führungsverantwortung über die daraus zu ziehenden Konsequenzen.

5. Die ISDS DV und die in der Verwaltung vorgeschriebene Projektführungsmethode HERMES regeln dies wie folgt:

Bei jedem ICT-Projekt bestimmt der Projektausschuss im Rahmen der Projektorganisation einen ISDS-Verantwortlichen. Dieser beurteilt in der Phase Voranalyse mittels ISDS-Analyse die datenschutzrechtliche Konformität des Vorhabens und bestimmt mit einer Schutzbedarfsklassifizierung, ob bei dem Projekt erhöhte ISDS-Anforderungen bestehen. Ergibt diese ISDS-Analyse, dass erhöhte ISDS-Anforderungen bestehen, ist spätestens in der Phase Konzept ein ISDS-Konzept zu erstellen. Im Rahmen dieses Konzepts wird eine Risikoanalyse erstellt. Daraus werden die organisatorischen und technischen ISDS-Massnahmen abgeleitet.

Die ISDS-Konzepte zu Vorhaben mit erhöhten ISDS-Anforderungen müssen der DSA zur Stellungnahme und dem IT-SIBE zur Kenntnis zugestellt werden (Art. 6 ISDS DV).

6. Die oder der IT-SIBE leitet den Fachbereich Sicherheit in der Abteilung Organisation und Sicherheit des KAIO. Dieser Fachbereich ist für die Gewährleistung der IS der vom KAIO erbrachten ICT-Grundversorgung verantwortlich. Er ist im folgenden Organigramm des KAIO markiert:



Die Unabhängigkeit der oder des IT-SIBE gegenüber der Kantonsverwaltung mit Ausnahme des KAIO ist durch die Ansiedlung der Stelle im Querschnittsamt KAIO sichergestellt. Gegenüber den vorgesetzten Abteilungs-, Amts- und Direktionsleitenden ist die oder der IT-SIBE infolge der hierarchischen Unterstellung grundsätzlich nicht unabhängig, wohl aber gegenüber den für die ICT-Leistungen operativ verantwortlichen Fach- und Führungspersonen, weil diese anderen Abteilungen des KAIO oder anderen Ämtern der Verwaltung angehören. Eine unabhängige Aufsicht über die IS des KAIO erfolgt zudem bereits durch die DSA und die Finanzkontrolle, die ebenfalls über IS-Fachpersonal verfügen.

7. Diesbezüglich ist zwischen den Aufsichtsaufgaben und den Unterstützungs- bzw. fachlichen Führungsaufgaben der oder des IT-SIBE zu unterscheiden:

   Die Aufgabe der verwaltungsunabhängigen Aufsicht über die IS wird im Rahmen der (sehr weitgehenden) Berührungspunkte zum Datenschutz bzw. zu der Revisionstauglichkeit der ICT-Systeme bereits heute durch die DSA und die Finanzkontrolle wahrgenommen. Grundsätzlich wäre es aus der Sicht des Regierungsrates denkbar, einer dieser bestehenden Aufsichtsbehörden durch eine Gesetzesänderung auch eine umfassende IS-Aufsichtsaufgabe zu übertragen. Infolge ihrer Unabhängigkeit können diese Behörden aber heute schon frei entscheiden, in welchem Umfang sie im Rahmen ihrer Aufsichtstätigkeit auch IS-Aspekte berücksichtigen.

   Demgegenüber sind die anderen Aufgaben der oder des IT-SIBE, u.a. die fachliche Leitung und Koordination der IS-Tätigkeiten der Verwaltung sowie die Erarbeitung von Hilfsmitteln, Verwaltungsvorschriften und Grundlagen, nach der Meinung des Regierungsrates Exekutivaufgaben, die durch die Verwaltung und nicht durch eine Aufsichtsbehörde zu erfüllen sind. Die organisatorische Nähe der oder des IT-SIBE zu den Personen und Fachbereichen des KAIO stellt zudem sicher, dass sie oder er jederzeit unmittelbaren Kontakt zu den Verantwortlichen der technischen Einrichtungen, der gemeinsamen Grundversorgung im ICT-Bereich des Kantons sowie der Planung und Durchführung von ICT-Projekten hat. Eine organisatorische Herauslösung aus dem KAIO würde diese Erfolgsvoraussetzungen gefährden.

   Im Projekt IT@BE wird aber zurzeit die Führung und Organisation der ICT der Verwaltung neu gestaltet. Die zukünftige Rolle der oder des IT-SIBE hängt auch von den Ergebnissen dieses Projekts ab.

Verteiler
- Grosser Rat