



Parlamentarischer Vorstoss

Antwort des Regierungsrates

Vorstoss-Nr.: 274-2022
Vorstossart: Interpellation
Richtlinienmotion: ☐
Geschäftsnummer: 2022.RRGR.414

Eingereicht am: 06.12.2022

Fraktionsvorstoss: Nein
Kommissionsvorstoss: Nein
Eingereicht von: Gerber (Hinterkappelen, Grüne) (Sprecher/in)
Riesen (La Neuveville, ES)

Weitere Unterschriften: 0

Dringlichkeit verlangt: Nein
Dringlichkeit gewährt:

RRB-Nr.: 569/2023 vom 17. Mai 2023
Direktion: Finanzdirektion
Klassifizierung: Nicht klassifiziert

Was passiert mit unseren Daten auf nicht mehr verwendeten Datenträgern?

Das Beispiel aus Zürich, wo heikle Daten von Justizbehörden nach der Entsorgung von Datenträgern in falsche Hände gelangt sein sollen, hat gerade wieder deutlich veranschaulicht, wie schwierig es ist, mit Daten in der digitalen Welt korrekt umzugehen. Viele Daten waren verschlüsselt. Diese konnten auf entsorgten Computern wieder lesbar gemacht werden.

Der Regierungsrat wird um Beantwortung folgender Fragen gebeten:

1. Was passiert mit Daten auf ausgedienten Computern und Servern?
2. Der Kanton lagert Daten bei privaten Anbietern. Wie stellt der Regierungsrat sicher, dass die Daten auf ausgedienten Servern nicht in fremde/falsche Hände geraten?
3. Wer ist verantwortlich für die Datensicherheit/Entsorgung bzw. Löschung von Daten?
4. Was weiss der Regierungsrat über den Handel mit Daten auf ausgedienten Servern im Zusammenhang mit kriminellen Absichten?
5. Was konkret unternimmt der Kanton Bern, damit ein Fall wie in Zürich nicht auch bei bernischen Behörden passieren kann?
6. Wie wurde das «Entsorgen» von ausgedienten Computern und Servern vor zehn Jahren gehandhabt?

Antwort des Regierungsrates

Der in der Interpellation erwähnte Zürcher Fall illustriert die steigenden Risiken für die Informations- und Cybersicherheit, die sich aus der Digitalisierung von immer mehr Lebens- und Verwaltungsbereichen ergeben. Der Regierungsrat ist sich dieser Risiken bewusst und will mit dem zurzeit laufenden Projekt IS@BE die rechtlichen, technischen und organisatorischen Grundlagen der Informationssicherheit in der Kantonsverwaltung aktualisieren und verbessern. Zu den Ergebnissen des Projekts gehören das geplante Gesetz über die Cyber- und Informationssicherheit (ICSG), das kürzlich Gegenstand eines Vernehmlassungsverfahrens war, und ein geplantes Informationssicherheitsmanagementsystem (ISMS) für die Kantonsverwaltung nach der internationalen ISO-27001-Norm.

Vor diesem Hintergrund beantwortet der Regierungsrat die Fragen wie folgt:

1. Was passiert mit Daten auf ausgedienten Computern und Servern?

Diese Daten müssen unwiederbringlich gelöscht werden. Die verantwortlichen Behörden klären bei jedem Projekt ab, ob Personendaten oder andere schützenswerte Informationen betroffen sind. Gegebenenfalls vereinbaren sie mit externen Leistungserbringern vertraglich die erforderlichen Massnahmen zur sicheren Löschung nicht mehr benötigter behördlicher Daten oder zur Vernichtung nicht mehr benötigter Datenträger.

2. Der Kanton lagert Daten bei privaten Anbietern. Wie stellt der Regierungsrat sicher, dass die Daten auf ausgedienten Servern nicht in fremde/falsche Hände geraten?

Kantonale Behörden, die private Unternehmen damit beauftragen, im Auftrag des Kantons Daten zu bearbeiten, müssen die Beauftragten vertraglich verpflichten, nicht mehr benötigte Daten unwiederbringlich zu löschen oder die Datenträger zu vernichten (s. Frage 1).

Entsprechende Verträge bestehen namentlich mit den Auftragsdatenbearbeitern der ICT-Grundversorgung der Kantonsverwaltung, wie dem Rechenzentrumsbetreiber Bedag Informatik AG, dem Druckdienstleister Ricoh und dem Endgerätelieferanten Business IT. Die Verträge sowie die Informationssicherheits- und Datenschutzkonzepte sehen vor, dass die Datenlöschung oder Vernichtung nach anerkannten Standards erfolgt, protokolliert wird und vom Auftraggeber und/oder von Aufsichtsbehörden überprüft werden kann.

Heutige Datenträger sind aber auch technisch deutlich besser geschützt als die vor 10 Jahren offenbar in Zürich verloren gegangenen. In Laptops werden Festplatten heute beispielsweise standardmässig verschlüsselt, und in Servern sind Daten so verteilt auf mehrere Festplatten abgespeichert, dass sie aus einzelnen Festplatten nicht rekonstruierbar sind. Gehen Datenträger verloren, ist das Risiko von Informationslecks daher deutlich tiefer.

3. Wer ist verantwortlich für die Datensicherheit/Entsorgung bzw. Löschung von Daten?

Dafür sind die Direktionen und Ämter verantwortlich, welche die Daten bearbeiten oder durch Dritte bearbeiten lassen.

4. Was weiss der Regierungsrat über den Handel mit Daten auf ausgedienten Servern im Zusammenhang mit kriminellen Absichten?

Dem Regierungsrat ist diesbezüglich nichts bekannt.

5. *Was konkret unternimmt der Kanton Bern, damit ein Fall wie in Zürich nicht auch bei bernischen Behörden passieren kann?*

Er führt wie eingangs erwähnt das Projekt IS@BE durch. Es wird unter anderem die Regeln über den Informationssicherheitsgrundsatz überprüfen, initiieren bzw. aktualisieren, wozu auch die Standards für eine sichere Datenlöschung und die Anforderungen an Cloud-Service-Anbieter gehören.

Die Kantonsmitarbeitenden werden regelmässig auf die Risiken und Methoden der Informationssicherheit sensibilisiert. Dies geschieht u.a. mit der Weisung über den Umgang mit ICT in der Kantonsverwaltung für Endanwenderinnen und Endanwender, mit der Ausbildung BE-Secure und mit jährlich wiederholten «Phishing»-Übungen, mit denen Cyberangriffe simuliert und die Mitarbeitenden im Erkennen und Behandeln entsprechender E-Mails geschult werden.

Die Datenschutzaufsichtsstelle (DSA) nimmt im Rahmen der Vorabkontrolle gemäss dem Datenschutzgesetz Stellung zu den Informationssicherheits- und Datenschutzkonzepten der besonders risikobehafteten kantonalen Informatiksysteme vor ihrer Inbetriebnahme. Zudem prüft sie ausgewählte in Betrieb stehende Systeme im Rahmen von Audits. In der Vorabkontrolle beurteilt die DSA u.a. den beschriebenen Plan (Soll) zur sicheren Datenlöschung. Deren erfolgreicher Vollzug (Ist) kann nur durch entsprechende Prüfungshandlungen festgestellt werden.

6. *Wie wurde das «Entsorgen» von ausgedienten Computern und Servern vor zehn Jahren gehandhabt?*

Damals war die Informatik in der Kantonsverwaltung weitgehend dezentral organisiert. Jedes Amt und jede Direktion handhabten den Umgang mit Hardware in eigener Verantwortung. Daher lässt sich diese Frage nicht in allgemeiner Weise für die ganze Kantonsverwaltung beantworten.

Verteiler
– Grosser Rat