Küsnacht und Hombrechtikon, 26. Juni 2017

KR-Nr. 178/2017

A N F R A G E von Hans-Peter Amrein (SVP, Küsnacht) und Tumasch Mischol (SVP, Hombrechtikon)

betreffend Kritische Datensicherheit bei der kantonalen Verwaltung und kantonalen Organisationen

---

Neben Chancen ist der Kanton Zürich mit sehr grossen Risiken der Digitalisierung konfrontiert. Trotz dieser besorgniserregenden Situation hat der Regierungsrat bis dato keine Kompetenzstelle Digitalisierung (Prävention) etabliert. Während dieses Jahr 20 neue Stellen bei den Strafverfolgungsbehörden (Kantonspolizei und Staatsanwaltschaft/Kompetenzzentrum Cybercrime) geschaffen wurden, fehlt es auf Stufe des Regierungsrates gänzlich an einer beauftragten Stelle oder Taskforce, welche sich mit der Prävention befasst. Auch ein zentral kontrolliertes, umfassendes, departementsübergreifendes Geschäftsverwaltungssystem fehlt. Die geltende kantonale Informationssicherheitsverordnung (ISV) ist dringlichst revisionsbedürftig. Gemäss Jahresbericht 2016 des Datenschutzbeauftragten (DSB) stellt dieser immer wieder grundlegende Mängel bei der Informationssicherheit fest. Der DSB moniert, der Entwurf einer neuen Verordnung über die Informationsverwaltung und –sicherheit (VO IVS) weise in eine falsche Richtung, ja, der Entwurf sei ein nicht nachvollziehbarer Rückschritt. Die bisherige Informatiksicherheitsverordnung (ISV) aus dem Jahre 1997 sei zwar revisionsbedürftig, biete aber den öffentlichen Organen einen weit besseren Orientierungsrahmen für die Informationssicherheit. Und der DSB stellt weiter fest, dass auch in Bezug auf die vom Regierungsrat am 7. Dezember 2016 verabschiedete Strategie «Digitale Verwaltung» mit dem Verordnungsentwurf ein fragwürdiges Zeichen gesetzt würde. Von allen Direktionen verfügt einzig die Direktion der Justiz und des Innern über eine öffentlich publizierte Verordnung über die Datenbearbeitung (172.110.11). Die Verordnung über die Datenbearbeitung im Bildungsbereich wird auf den 1. Juli 2017 aufgehoben.

178/2017

In diesem Zusammenhang bitten wir den Regierungsrat um die Beantwortung folgender Fragen:

1. Wann will der Regierungsrat, wie vom DSB anlässlich seiner Pressekonferenz vom 21. Juni 2016 eingefordert, eine verwaltungsübergreifende «Taskforce Datensicherheit» etablieren und mit welchen konkreten Vorgaben und Kompetenzen wird diese Stelle bedacht und ausgestattet? Wenn nicht vorgesehen ist, eine solche Stelle einzurichten, warum nicht und soll sich überhaupt eine kantonale Stelle gemäss Absicht des Regierungsrates mit dem Thema Datensicherheit/Prävention befassen und ab wann?

2. Welche wirksamen Massnahmen gegen Datenabfluss hat der Regierungsrat vor dem Hintergrund zunehmender Cyberattacken bis dato verwaltungsübergreifend verfügt? Sind kantonale Verwaltungsstellen und Organisationen (inklusive Universität und Spitäler etc.) in der Vergangenheit schon Opfer entsprechender Erpressungsversuche oder sogar «gelungener» Erpressungen geworden?

3. Werden regelmässige und verwaltungsübergreifende Kontrollen betreffend Passwörtersicherheit und der Sicherheit vor Datenabfluss (Pishing) vorgenommen und wenn ja, durch wen werden überhaupt Kontrollen betreffend Sicherheit mobiler und fest installierter, dem Staat gehörender elektronischer Kommunikationsmittel vorgenommen? Und durch wen? Wie ist und wird die Sicherheit persönlicher elektronischer Kommunikationsmittel sichergestellt, welche für die Arbeitstätigkeit oder im Zusammenhang mit der Arbeitstätigkeit für den Kanton oder kantonale Organisationen genutzt werden? Kommen dabei Smartcards zum Einsatz, und wer konfiguriert und verwaltet diese?

4. Gibt es verwaltungsübergreifende Vorschriften - wenn überhaupt erlaubt - betreffend das Führen persönlicher Gespräche (inklusive WhatsApp etc.) sowie die Bearbeitung und den Tansfer persönlicher Daten via und mit dem Kanton gehörenden und den einzelnen Mitarbeitern zur Verfügung gestellten elektronischen Kommunikationsmitteln (Mobiltelefone, I-Pad‘s, Officecomputer, USB-Datensticks, Smartcards, mobile WLAN-Router etc.)?

5. Welche Vorschriften bestehen für die den Umgang, die Bearbeitung und den Transfer mit dem Staat gehörender oder den Staat betreffender Daten und Informationen bei der Arbeit von zuhause aus (Stichwort Home-Office) und bestehen in diesem Zusammenhang unterschiedliche Vorschriften je nach Art des persönlichen elektronischen Kommunikations-, Hilfs- und Speichergeräts (Mobiltelefon, I-Pad, Home-Computer, USB-Datensticks, Smartcards etc.)?

6. Erachtet der Regierungsrat den Datentransfer „kantonseigener“ Daten via Dritten gehörenden, elektronischen Kommunikationsmittel (Mobiltelefone, I-Pad’s, Home-Computer, USB-Datensticks, mobile WLAN-Router etc.) überhaupt als sicher oder grundsätzlich als unsicher? Ist die Benutzung erwähnter Kommunikationsmittel, welche sich nicht im Eigentum des Staates befinden, generell zu verbieten und entsprechender Missbrauch konsequent zu ahnden?

7. Was hält der Zürcher Regierungsrat generell von der Publikation von Quellcodes, dies ins-sondere im Zusammenhang mit dem geplanten Electronic Voting und vor dem Hintergrund von in den vergangenen Monaten vonseiten Krimineller eingesetzter Software-Trojaner?

8. Was hält der Regierungsrat von der Anwendung von Open-Clouds durch die Verwaltung und wie schätzt er generell die Sicherheit der Verwaltung und des Transfers von Daten via Open-Clouds ein? Ist vor dem Hintergrund, dass viele Mitarbeiter der Verwaltung (insbesondere auch im Bildungsbereich) mehrheitlich Apple-Betriebssysteme anwenden, die Sicherheit sensitiver Daten (Beispiel Personen- und Steuerdaten) überhaupt gewährleistet?

9. Verfügt der Kanton Zürich über Vorschriften betreffend die Anwendung von Cloud-Computing in der Verwaltung und insbesondere bei besonders gefährdeten kantonalen Organisationen (Universität Zürich und Fachhochschulen, Spitäler etc.)? Wurde oder wird ein Verbot der Anwendung von Open-Clouds versus nur verwaltungs- oder organisationsinterne Cloud-Anwendungen angedacht, und ist sich der Regierungsrat der entsprechenden Datensicherheits-Problematik bewusst?

10. Bestehen verwaltungsübergreifende Richtlinien (und verschiedene Sicherheitsstufen) betreffend die Verschlüsselung von Gesprächen mittels Mobiltelefonen?

11. Welche Direktionen und Verwaltungsstellen verfügen über direktions- und verwaltungsinterne Verordnungen über die Datenbearbeitung (Bitte um Auflistung und Datum deren Inkraftsetzung sowie um Link zu deren Einsicht)?

Hans-Peter Amrein
Tumasch Mischol