Auszug aus dem Protokoll des Regierungsrates des Kantons Zürich

KR-Nr. 178/2017

Sitzung vom 4. Oktober 2017

916. Anfrage (Kritische Datensicherheit bei der kantonalen Verwaltung und kantonalen Organisationen)

Die Kantonsräte Hans-Peter Amrein, Küsnacht, und Tumasch Mischol, Hombrechtikon, haben am 26. Juni 2017 folgende Anfrage eingereicht:

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.

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 inssondere 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)?

Auf Antrag der Finanzdirektion

beschliesst der Regierungsrat:

I. Die Anfrage Hans-Peter Amrein, Küsnacht, und Tumasch Mischol, Hombrechtikon, wird wie folgt beantwortet:

Zu Frage 1:

Der Regierungsrat ist der Überzeugung, dass die Datensicherheit eine Daueraufgabe von grosser Wichtigkeit ist. Sie sollte deshalb nicht von einer «Task Force» wahrgenommen werden. In diesem Sinne hat der Regierungsrat schon 2015 ein Competence Center IT-Sicherheit in der Finanzdirektion geschaffen, für dessen Leitung die Stelle einer oder eines Informatik-Sicherheitsbeauftragten des Kantons Zürich bewilligt und dieser bzw. diesem eine ständige Fachgruppe Informatiksicherheit beigeordnet wurde (vgl. RRB Nrn. 129/2015 und 379/2015). Im Rahmen der neuen kantonalen IKT-Organisation (vgl. RRB Nr. 780/2017) wird diese Sicherheitsstruktur auch weiterhin an neue Herausforderungen angepasst werden können.

Zu Frage 2:

Der Regierungsrat trägt der Entwicklung der sogenannten Cybercrime-Phänomene ganz allgemein dadurch Rechnung, dass er in mehreren Beschlüssen die Bekämpfung der Internetkriminalität als Schwerpunkt der Strafverfolgung festgelegt hat (vgl. RRB Nrn. 1068/2009, 659/2012 und 1081/2015), dazu ein Kompetenzzentrum Cybercrime aufgebaut wird und die notwendigen personellen und finanziellen Mittel dafür zur Verfügung gestellt werden. 2015 wurde zudem das Competence Center IT-Sicherheit mit der Stelle einer oder eines Informatik-Sicherheitsbeauftragten des Kantons Zürich und der Fachgruppe Informatiksicherheit geschaffen (vgl. RRB Nrn. 129/2015 und 379/2015), welche die Aktivitäten und Schutzmassnahmen in der kantonalen Verwaltung koordinieren und weiterentwickeln.

Weitere Massnahmen werden auf Direktionsstufe getroffen. Dabei handelt es sich sowohl um organisatorische Massnahmen (z. B. Richtlinien, Schulungen und Newsletters) als auch um technische Vorkehrungen (z. B. Verschlüsselung von Geräten und Datenströmen).

Einer Umfrage zufolge haben die Direktionen und die Staatskanzlei (bzw. die selbstständigen Anstalten in ihrem Zuständigkeitsbereich) schon einzelne Vorfälle mit Ransomware-Viren und Verschlüsselungstrojanern verzeichnet. Diese konnten jedoch erfolgreich abgewehrt oder entfernt werden. Beschädigte Daten konnten aus Datensicherungen wiederhergestellt werden. Lösegeldzahlungen erfolgten keine.

Zu Frage 3:

Die Kontrolle der Passwörter und der Sicherheit vor Datenabfluss (Phishing) ist Sache der Direktionen und Ämter. Direktionsübergreifende Kontrollen zur IT-Sicherheit nehmen der Datenschutzbeauftragte und die Finanzkontrolle vor. Für 2017 ist vorgesehen, erstmals einen Lagebericht für die gesamte kantonale Verwaltung zu erstellen. Ausserdem ist beim Informatik-Sicherheitsbeauftragten eine Passwortrichtlinie für die kantonale Verwaltung in Arbeit. Ab Herbst 2017 werden sodann sämtliche Mitarbeitenden der kantonalen Verwaltung auch ausserhalb des «Notes»-Umfelds verschlüsselte E-Mails versenden können. Eine entsprechende kantonale Plattformlösung wird zurzeit getestet. Bisher wurde teilweise mit IncaMail gearbeitet.

Die in den Direktionen und Ämtern eingesetzten Smartcards und anderen technischen Mittel im Zusammenhang mit der Datensicherheit werden durch die jeweiligen IT-Betriebsorganisationen betreut, konfiguriert und verwaltet. Die Ausstellung und Wartung der Smartcards wird zentral vom Service Center PKI vorgenommen, das zur Hauptabteilung IT im Generalsekretariat der Direktion der Justiz und des Innern gehört. Gegenwärtig werden über 6000 Chipkarten vom Service Center PKI verwaltet. Die Verwendung von Smartcards nimmt in der kantonalen Verwaltung stetig zu.

Zu Frage 4:

Die Verordnung über die Nutzung von Internet und E-Mail vom 17. September 2003 (LS 177.115) regelt die Nutzung und die Verhinderung des Missbrauchs von Internet und E-Mail mit kantonalen Informatikmitteln durch die Mitarbeitenden des Kantons und seiner unselbstständigen Anstalten. Nach dieser Verordnung haben sich die Mitarbeitenden auf ein Mindestmass zu beschränken und sich kurz zu halten, wenn sie das Internet oder das E-Mail während der Arbeitszeit für private Zwecke nutzen (§ 4 Abs. 1). Das Ablegen von dienstlichen E-Mail-Adressen im Internet, der Versand von E-Mails mit starker Netzwerkbelastung (insbesondere der Versand an einen grossen Empfängerkreis oder von grossen Datenmengen) sowie die Teilnahme an interaktiven Medien (insbesondere an Chatrooms) sind zu privaten Zwecken untersagt (§ 4 Abs. 2). Allgemein verboten sind das Anwählen und die Nutzung von Internetseiten mit rechtswidrigem, pornografischem, rassistischem, sexistischem oder gewaltverherrlichendem Inhalt sowie die Weiterverbreitung von E-Mails mit solchen Inhalten (§ 2). Unzulässig sind sodann der Versand von Kettenbriefen, die automatische Umleitung (Forwarding) von E-Mails an externe E-Mail-Adressen sowie das Herunterladen oder die Installation von

Spielen und Audio- und Videodateien aus dem Internet (§ 3 Abs. 1). Die Direktionen können ergänzende Bestimmungen erlassen und die private Nutzung von Internet und E-Mail weiter einschränken (§ 5). Alle Mitarbeitenden mit Zugang zu Internet oder E-Mail unterzeichnen eine Erklärung, wonach sie auf die Nutzungsvorschriften aufmerksam gemacht worden sind und die möglichen straf-, zivil- und personalrechtlichen Konsequenzen eines Missbrauchs von Internet und E-Mail zur Kenntnis genommen haben (§ 6 Abs. 1). Die Erklärung wird im Personaldossier abgelegt (§ 6 Abs. 2). Die Regeln dieser Verordnung gelten zumindest sinngemäss auch für neuere Anwendungen wie beispielweise WhatsApp oder Streaming-Dienste.

Zu Frage 5:

Das Personalamt hat ein «Merkblatt für Home Office im Kanton Zürich» erstellt und dieses ins «Handbuch Personalrecht» eingegliedert. Das Merkblatt hält unter dem Titel «Sicherheit» fest, dass für Home Office die gleichen Richtlinien betreffend den Datenschutz, die Benutzung der IT und den Umgang mit Geschäftsdokumenten gelten wie am Arbeitsplatz. Es gelten insbesondere die spezifischen Informatiknutzungsbestimmungen der Verwaltungseinheiten. Die Mustervereinbarung des Personalamtes zur Regelung von Home Office enthält dementsprechend eine Klausel, mit der die oder der Mitarbeitende bestätigt, die Datenschutzbestimmungen, die Bestimmungen zur Informatiksicherheit (ISV, ISMS) sowie die Weisung betreffend die Nutzung von Informatikmitteln der Verwaltungseinheit zu kennen und einzuhalten. Weiter wird damit bestätigt, dass die Datenbearbeitung im Home Office unter Wahrung der Geheimhaltung erfolgt.

Zu Frage 6:

Der Datentransfer mithilfe von Dritten gehörenden Kommunikationsmitteln gehört heute zum Alltag und ist Teil der digitalen Welt. Gleichzeitig ist ein grosser Teil der Informationen der kantonalen Verwaltung gar nicht als vertraulich einzustufen und stellt deshalb keine besonderen Anforderungen an die Informationssicherheit. Viele Daten weisen sodann höchstens einen geringen wirtschaftlichen Wert für eine denkbare kriminelle Nutzung auf. Vor diesem Hintergrund ist ein allgemeines Verbot des Datentransfers über Kommunikationsmittel, die Dritten gehören, nicht sinnvoll. Vielmehr muss, soweit erforderlich, durch technische Vorkehrungen sichergestellt werden, dass die Übermittlung sicher durchgeführt werden kann. Im Vordergrund steht dabei die Verschlüsselung. Daneben können auch organisatorische Massnahmen einem Missbrauch entgegenwirken.

Zu Frage 7:

Vor- und Nachteile der Publikation von Quellcodes sind im Einzelfall gegeneinander abzuwägen. Zum einen ermöglicht die Publikation interessierten Fachkreisen, die Programmlogik zu überprüfen, was zur Aufdeckung von Lücken und Fehlern beitragen kann. Zum anderen ist nicht auszuschliessen, dass Kriminelle die aus dem Quellcode gewonnenen Erkenntnisse missbrauchen.

Zu Frage 8:

Nach der Einschätzung des Regierungsrates bieten die öffentlichen Cloud-Dienste grundsätzlich eine geringe Sicherheit. Daten der Verwaltung sollten deshalb – wenn überhaupt – nur stark verschlüsselt in öffentlichen Clouds abgelegt werden. Hingegen ist nicht ersichtlich, weshalb von Apple-Betriebssystemen eine erhöhte Gefährdung ausgehen sollte.

Zu Frage 9:

Der Regierungsrat ist sich der Sicherheitsproblematik bei der Anwendung von öffentlichen Cloud-Diensten bewusst. Demgemäss finden solche Dienste in den Direktionen entweder keinen oder nur beschränkten Einsatz (etwa für öffentlich zugängliche Daten). Im Gesundheitsbereich (Gesundheitsdirektion, USZ, KSW, PUK, ipw) sind derzeit keine entsprechenden Anwendungen in Betrieb. Im Bildungsbereich finden sich zwei unterschiedliche Ansätze: Für die Verwendung im Verwaltungsumfeld wird die Benutzung von Open Clouds in der Informatikrichtlinie der Bildungsdirektion untersagt. Im Schul- und Hochschulbereich ist die Nutzung von Cloud-Diensten hingegen von grosser Bedeutung, dies insbesondere für pädagogische Anwendungen im Rahmen des Unterrichts. Zahlreiche Reglemente regeln die erlaubten Anwendungen und untersagen unerwünschte Anwendungen. Aus technischer Sicht besteht die Herausforderung darin, einerseits die Sichtbarkeit der Nutzung von Cloud-Diensten innerhalb der eigenen Infrastrukturen zu verbessern und anderseits Cloud-Dienste gemäss ihrer Vertrauenswürdigkeit zuzulassen oder auszusperren.

Mit Beschluss Nr. 670/2015 erliess der Regierungsrat zudem die «Allgemeinen Geschäftsbedingungen bei der Auslagerung von Datenbearbeitungen unter Inanspruchnahme von Informatikleistungen (AGB Auslagerung Informatikleistungen)» und die «Allgemeinen datenschutzrechtlichen Geschäftsbedingungen bei der Datenbearbeitung durch Dritte (AGB Datenbearbeitung durch Dritte)». Mit dem gleichen Beschluss erklärte er diese AGB zusammen mit den «Allgemeinen Geschäftsbedingungen der Schweizerischen Informatikkonferenz für IKT-Leistungen (AGB der SIK für IKT-Leistungen)» für die ihm unterstellten Verwaltungseinheiten als verbindlich.

Zu Frage 10:

Es bestehen keine direktionsübergreifenden Richtlinien und Sicherheitsstufen betreffend die Verschlüsselung von Gesprächen mittels Mobiltelefonen.

Zu Frage 11:

Der Regierungsrat beschloss am 27. Januar 2016 eine Verordnung über die Datenbearbeitung der Direktion der Justiz und des Innern (LS 172.110.11). Für die anderen Direktionen und die Staatskanzlei bestehen keine solchen Verordnungen.

Dies bedeutet jedoch nicht, dass hier eine Regelungslücke bestünde. Regeln über die Datenbearbeitung, die für die ganze Verwaltung oder für Teile davon gelten, finden sich verstreut in zahlreichen Erlassen. Zu erwähnen sind dabei unter anderem das Gesetz über die Information und den Datenschutz vom 12. Februar 2007 (IDG; LS 170.4), die Verordnung über die Information und den Datenschutz vom 28. Mai 2008 (IDV; LS 170.41), die Informatiksicherheitsverordnung vom 17. Dezember 1997 (LS 170.8), die Verordnung über die Nutzung von Internet und E-Mail vom 17. September 2003 (LS 177.115), das Gesetz über die Gerichts- und Behördenorganisation im Zivil- und Strafprozess vom 10. Mai 2010 (GOG; LS 211.1), das Polizeigesetz vom 23. April 2007 (PolG; LS 550.1) und die Verordnung über das Polizei-Informationssystem POLIS vom 13. Juli 2005 (POLIS-Verordnung; LS 551.103). Weitere Regeln über die Datenbearbeitung finden sich in verwaltungsinternen Weisungen und Richtlinien. Beispielhaft erwähnt werden können hier etwa die Social Media Guidelines des Kantons oder die Dienstbefehle der Kantonspolizei.

II. Mitteilung an die Mitglieder des Kantonsrates und des Regierungsrates sowie an die Finanzdirektion.

Vor dem Regierungsrat
Der stv. Staatsschreiber:
Hösli