

ANFRAGE von Farid Zeroual (CVP, Adliswil) und Mark Wisskirchen (EVP, Kloten)
betreffend Informatik Vorkehrungen gegen Service Unterbrüchen aufgrund von
Virusattacken

Die NZZ berichtete in ihrer Ausgabe vom 23. Mai 2019 unter dem Titel «Die Stadtverwaltung von Baltimore beantwortet derzeit keine E-Mails - weil sie Ziel einer Ransomware-Attacke wurde.» über den Ausfall von Teilen der Informatikdienste der Verwaltung. Am 27. Mai 2019 berichtete der Tages-Anzeiger im Artikel «Baltimore steht still – wegen einer uralten Windows-Sicherheitslücke» über massive Einschränkungen der Stadtverwaltung in Baltimore. Gemäss eigenen Angaben der Stadtverwaltung Baltimore wurde am 7. Mai 2019 eine Virusattacke festgestellt. In der Folge mussten mehrere Computer Systeme, zur Vermeidung von weiteren Schäden, herunter gefahren werden. Am Montag 27. Mai, also rund drei Wochen nach der Attacke, ist der Mail Verkehr mit der Stadt Baltimore weiterhin nicht verfügbar. Dies gemäss eigenen Angaben auf der offiziellen Webseite der Stadt Baltimore.

Auch im Kanton Zürich bilden zuverlässige Informatik Services die Grundlage für den täglichen Betrieb und die Kommunikation mit internen und externen Stellen. Durch die Zentralisierung ins Amt für Informatik wird die Verwaltung von Servern und Endgeräten vereinheitlicht. Damit kann im Falle einer Virenattacke ein erhöhtes Klumpenrisiko entstehen.

Aus diesem Grunde bitten wir den Regierungsrat um die Beantwortung folgender Fragen:

1. In welchem Umfang waren die Informatikeinrichtungen des Kantons Zürich in den vergangenen vier Jahren schon Ziel von Virenattacken?
2. Falls es zu Virenbefall gekommen ist, wie viele Server und PC's waren betroffen? Welche Dienstleistungen intern und extern waren davon betroffen?
3. Wie viele Server und PC's stehen aktuell unter zentraler Verwaltung beim Amt für Informatik? Wie viele Server und PC's werden es im Zielzustand nach der Konsolidierung sein?
4. Wie viele Server und PC's werden mit veralteten Betriebssystem Software betrieben? Falls solche Geräte im Einsatz stehen, wie werden Software Unterhalt und aktueller Virenschutz sichergestellt?
5. Welche Vorkehrungen zum Schutz vor Viren und Schadsoftware sind im Server und PC's generell im Einsatz? Bieten diese Vorkehrungen ausreichenden Schutz vor Epressungssoftware?
6. Welche Notfallpläne für den Informatik Notbetrieb im Falle eines Virenbefalls existieren in der Verwaltung?

Farid Zeroual
Mark Wisskirchen