Auszug aus dem Protokoll des Regierungsrates des Kantons Zürich

KR-Nr. 165/2019

Sitzung vom 18. September 2019

838. Anfrage (Informatik Vorkehrungen gegen Service Unterbrüchen aufgrund von Virusattacken)

Die Kantonsräte Farid Zeroual, Adliswil, und Mark Anthony Wisskirchen, Kloten, haben am 27. Mai 2019 folgende Anfrage eingereicht:

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?

Auf Antrag der Finanzdirektion

beschliesst der Regierungsrat:

I. Die Anfrage Farid Zeroual, Adliswil, und Mark Anthony Wisskirchen, Kloten, wird wie folgt beantwortet:

Zu Frage 1:

Die kantonale Verwaltung ist fast täglich Virenattacken ausgesetzt. Diese sind meist Teil einer schweizweit angelegten Angriffswelle und finden nicht zielgerichtet gegen die Infrastruktur der kantonalen Verwaltung statt. Die E-Mail-Infrastruktur der kantonalen Verwaltung verarbeitet jährlich rund 80 Mio. E-Mails, davon werden durchschnittlich 0,02% aufgrund infizierter Anhänge (Viren und Schadsoftware) abgewiesen. Weitere Kontrollen (Spam, unbekannte Empfängerinnen und Empfänger, verdächtige Absenderinnen und Absender oder Inhalt, Massenversand usw.) führen dazu, dass insgesamt rund 85% aller E-Mails an die kantonale Verwaltung als gefährlich eingestuft und abgewiesen werden. Gemäss dem deutschen Bundesamt für Sicherheit in der Informationstechnik liegt der Durchschnitt von unerwünschten E-Mails im deutschsprachigen Raum derzeit bei rund 90%.

Zu Frage 2:

In den vergangenen vier Jahren wurden aus den Direktionen und der Staatskanzlei nur vereinzelt Berichte zu Virenbefällen erstattet. Diese beschränkten sich jeweils auf ein System. Zudem ist ein Befall durch einen Verschlüsselungstrojaner (Ransom-Ware) bekannt. In sämtlichen Fällen konnten die Auswirkungen auf die befallenen Systeme begrenzt und die beschädigten Daten aus Datensicherungen wieder hergestellt werden. Dienstleistungen der kantonalen Verwaltung waren in den genannten Fällen keine betroffen.

Zu Frage 3:

Derzeit stehen 3000 Arbeitsplätze und 233 Server unter der zentralen Verwaltung durch das Amt für Informatik (Stand 1. Juli 2019). Nach erfolgter Zentralisierung der IKT-Grundversorgung wird sich die Anzahl der gemanagten Endgeräte vervierfachen. Die Anzahl der dannzumal in Betrieb stehenden Server lässt sich aufgrund der zu erwartenden Konsolidierungen heute nicht zuverlässig schätzen.

Zu Frage 4:

Als veraltete Betriebssysteme gelten jene Systeme, die keine Wartung durch den Hersteller mehr erhalten. Sämtliche durch das Amt für Informatik verwalteten Arbeitsplätze sind mit einem zeitgemässen Betriebssystem ausgerüstet. Auf den 233 Servern gelangen applikationsbedingt unterschiedliche Betriebssysteme zum Einsatz. Sie alle sind Teil eines laufenden Wartungsprogramms. Über den im Amt für Informatik etablierten Patch-Management-Prozess wird sichergestellt, dass sämtliche Betriebssysteme auf dem aktuellen Stand gehalten werden. Sicherheitsupdates werden mit hoher Priorität behandelt und nach einer initialen Überprüfung umgehend ausgerollt.

Zu Frage 5:

Für den Schutz der kantonseigenen Informationswerte vor Schadsoftware verfügt die kantonale Verwaltung über ein mehrstufiges Sicherheitsmodell. Informationsflüsse (E-Mail, Web, Datenaustausch usw.) werden sowohl beim Eintritt in das Netzwerk der kantonalen Verwaltung (LEUnet), auf applikatorischer Ebene als auch auf dem Endgerät auf Schadsoftware überprüft. Zusätzlich wird bei Verdacht die Bearbeitung der Informationen durch eine Benutzerin oder einen Benutzer in einer sogenannten Sandbox simuliert. Das Sicherheitsnetzwerk der kantonalen Verwaltung umfasst auch strategische Partner wie Abraxas oder Swisscom, die für die eingekauften Dienstleistungen ein Security Operation Center betreiben. Die technischen Massnahmen werden zusätzlich durch geeignete Benutzer-Sensibilisierungsprogramme unterstützt. Die getroffenen Massnahmen bieten zurzeit einen ausreichenden Schutz vor Viren und Schadsoftware. Sie müssen jedoch regelmässig auf ihre Wirksamkeit überprüft werden.

Im Rahmen des Programms zur Umsetzung der IKT-Strategie wurden zudem Massnahmen zur weiteren Verbesserung der IKT-Sicherheit getroffen. Teil dieser Massnahmen sind der Aufbau eines Security Operation Centers sowie zusätzliches Personal im Bereich IKT-Sicherheit.

Zu Frage 6:

Der Umgang mit Sicherheitsvorfällen (Notfall und Krisenmanagement) ist derzeit noch dezentral auf Stufe Direktion/Amt geregelt. Diese verfügen alle über entsprechende Notfallpläne, teilweise mit der Unterstützung durch externe Partner. Das Amt für Informatik bzw. das Programm zur Umsetzung der IKT-Strategie befasst sich derzeit mit der Ausarbeitung von entsprechenden Notfall- und Krisenbewältigungsplänen auf Stufe der kantonalen Verwaltung.

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

Vor dem Regierungsrat
Die Staatsschreiberin:
Kathrin Arioli