Zürich, Winterthur und Niederglatt, 26. Juni 2023

KR-Nr. 243/2023

A N F R A G E von Nicola Yuste (SP, Zürich), Florian Heer (Grüne, Winterthur) und Stefan Schmid (SVP, Niederglatt)

Betreffend Wie sicher ist der Kanton Zürich vor Cyberangriffen?

Im Mai und Juni dieses Jahres wurde die Schweiz von verschiedenen Hackerangriffen heimgesucht. Einerseits erbeutete die Ransomware-Bande «Play» Daten von zahlreichen staatlichen Akteuren bei der Berner IT-Dienstleisterin Xplain AG, die auf Software für die staatliche Verwaltung spezialisiert ist. Gemäss Medienberichten sind vom Datenklau diverse Institutionen der Bundesverwaltung (Staatssekretariat für Migration, Bundesamt für Justiz, Bundespolizei Fedpol, VBS, etc), die Stadtpolizei Zürich sowie zahlreiche kantonale Behörden betroffen. Anfang Juni hat das Nationale Zentrum für Cybersicherheit NCSC kommuniziert, dass sich unter den verschlüsselten und entwendeten Daten der Firma Xplain AG auch operative Daten aus der Bundesverwaltung befinden. Am 14. Juni gab die Hackergruppe schliesslich bekannt, dass sie den gesamten entwendeten Datensatz (mutmasslich 907 Gigabyte) im Darknet veröffentlicht haben.
Wohl unabhängig davon hat die pro-russische Hackergruppe «NoName» Mitte Juni massive Distributed-Denial-of-Service (DDoS oder verteilter Dienstverweigerungsangriff) Angriffe auf Webseiten der Bundesverwaltung, der Parlamentsdienste, zahlreicher Schweizer Städte und Kantone verübt.

Im Kanton Zürich nimmt der Regierungsrat die übergeordnete politische Verantwortung für die Cybersicherheit war. Vor diesem Hintergrund bitten wir die Regierung um die Beantwortung der folgenden Fragen:

1. Nutzt die kantonale Verwaltung Softwaresysteme wie z.B. der Firma Xplain AG, welche in den vergangenen Monaten von Datenklau betroffen waren und welche Ämter resp. Art von Daten (Personendaten oder andere sensitive Daten) wurden Opfer dieser Angriffe?

2. Ist es möglich, dass auch Infrastrukturen, die nicht reine Informatiklösungen sind, betroffen sind? (Zum Beispiel Infrastrukturen zur Energieerzeugung, Wasserversorgung, Spitäler, etc.)

3. Welche weiteren Cyberangriffe wie z.B. DDoS-Angriffe auf kantonale Websiten, welche zu einer Einschränkung der Services oder zu Datenabgriffen geführt haben, gab es im letzten Jahr auf den Kanton Zürich, resp. die staatsnahen Betriebe?

4. Wie weit ist die Regierung mit der Umsetzung ihrer Cybersicherheitsstrategie und sieht die Regierung aufgrund der aktuellsten Vorkommnisse bereits die Notwendigkeit, Anpassungen vorzunehmen resp. rechtliche Schritte einzuleiten?

5. Wie schätzt die Regierung die Sicherheitslage des Kantons Zürich im Cyberbereich ein?

6. Was macht der Kanton Zürich um seine strategischen Infrastrukturen in den eigenen Werken und bei staatsnahen Betrieben (z.B. zur Energieerzeugung, Wasserversorgung, Spitäler, etc.) zu schützen?

Nicola Yuste
Florian Heer
Stefan Schmid