Auszug aus dem Protokoll des Regierungsrates des Kantons Zürich

KR-Nr. 243/2023

Sitzung vom 4. Oktober 2023

1149. Anfrage (Wie sicher ist der Kanton Zürich vor Cyberangriffen?)

Kantonsrätin Nicola Yuste, Zürich, sowie die Kantonsräte Florian Heer, Winterthur, und Stefan Schmid, Niederglatt, haben am 26. Juni 2023 folgende Anfrage eingereicht:

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 prorussische 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?

Auf Antrag der Finanzdirektion

beschliesst der Regierungsrat:

I. Die Anfrage Nicola Yuste, Zürich, Florian Heer, Winterthur, und Stefan Schmid, Niederglatt, wird wie folgt beantwortet:

Zu Frage 1:

Das Amt für Informatik ist innerhalb der Verwaltung des Kantons Zürich interner Leistungserbringer und stellt im Rahmen der Grundversorgung den Direktionen und den diesen zugehörigen Organisationseinheiten sowie der Staatskanzlei eine Basisinfrastruktur zur Verfügung. Es nutzt keine Softwaresysteme, die in den vergangenen Monaten von Datendiebstahl betroffen waren.

Aktuell verwenden bei den Direktionen und der Staatskanzlei einzig das Migrationsamt und das Passbüro Anwendungen von Xplain AG. Im Rahmen des in der Anfrage erwähnten Datenklaus sind bei der Xplain AG Projektunterlagen für die Softwareeinführung wie Abnahmedokumente entwendet worden. Die beim Kanton eingesetzte Software war nicht betroffen. Für den Kanton Zürich entstand kein Schaden.

Zu Frage 2:

Im Rahmen des besagten Cyberangriffs im Juni 2023 erhielt der Kanton Zürich keine Kenntnis von Drittschäden an nicht reinen Informatikeinrichtungen. Grundsätzlich aber können durch Abhängigkeiten in der Lieferkette nicht reine Informatikeinrichtungen indirekt Opfer eines Cyberangriffs werden.

Zu Frage 3:

Im Zuge der DDoS-Angriffe (Distributed Denial of Service, verteilte Netzwerkangriffe) in der Schweiz sind auch mehrere im Kanton Zürich registriert worden. Die kantonale Verwaltung konnte diese Angriffe gemeinsam mit den Dienstlieferantinnen und -lieferanten abwehren. Dennoch waren vereinzelte Organisationseinheiten des Kantons Zürich indirekt von den Angriffen betroffen. Als der Bund aufgrund des Angriffs offline war, funktionierten die entsprechenden Schnittstellen zeitweilig nicht mehr. Konkret waren die Webseiten des Zürcher Verkehrsverbunds von DDoS-Angriffen im Frühling 2023 betroffen, wobei kein System kompromittiert und keinerlei Daten gestohlen wurden.

Zu Frage 4:

Die Umsetzung der kantonalen Strategie für Cybersicherheit erfolgt gemäss RRB Nr. 676/2022. Aufgrund der angespannten Situation am Arbeitsmarkt konnten noch nicht alle neu im Kantonalen Zentrum für Cybersicherheit (CCSC) und in weiteren Organisationseinheiten des Kantons geschaffenen Stellen besetzt werden. Der daraus resultierende Engpass wird mit externem Fachpersonal überbrückt. Ausser der in RRB Nr. 676/2022 definierten Aufgabe A 2.3 «Risikomanagement Informationssicherheit» befindet sich die Umsetzung der kantonalen Strategie im Zeitplan. Es besteht kein Bedarf an einer Anpassung, da die aktuellen Vorkommnisse vorausschauend bei der Erarbeitung der Cybersicherheitsstrategie berücksichtigt wurden (vgl. auch Beantwortung der Frage 5). Der rechtliche Anpassungsbedarf wird zurzeit ermittelt.

Die kantonale Cybersicherheitsstrategie verfolgt drei Stossrichtungen:

– Der Kanton Zürich versteht den Schutz vor Cyberrisiken als eine gemeinsame Aufgabe von Staat, Wirtschaft, Wissenschaft und Gesellschaft. Das heisst, die Verwaltung möchte die Vernetzung und Zusammenarbeit zwischen diesen Bereichen innerhalb des Kantons Zürich vorantreiben und fördern.
– Der Kanton Zürich möchte auch innerhalb der Verwaltung die Zusammenarbeit stärken, insbesondere mit der Strafverfolgung sowie der Kantonalen Führungsorganisation.
– Der Kanton Zürich möchte Kräfte innerhalb der Verwaltung bündeln und damit die Cybersicherheitsdienstleistungen zentral organisieren, um einen einheitlichen Standard für alle Direktionen und die Staatskanzlei anbieten zu können. Diese Dienstleistungen können zu einem späteren Zeitpunkt auch von Zielgruppen sowie Partnerinnen und Partnern ausserhalb der kantonalen Verwaltung genutzt werden, sofern und soweit dafür eine rechtliche Grundlage besteht.

Die Umsetzung dieser Stossrichtungen erfolgt durch den etappenweisen Aufbau des CCSC innerhalb der Finanzdirektion.

Die zentralen Dienstleistungen aus dem CCSC stehen den Direktionen und der Staatskanzlei bei der direktionsinternen Umsetzung der Sicherheitsvorgaben gemäss RRB Nr. 1193/2020 zur Verfügung. Demnach ist die Widerstandsfähigkeit der kantonalen Verwaltung eine Verbundaufgabe des CCSC, der Direktionen und der Staatskanzlei.

Zu Frage 5:

Das Cyber Defence Center im Amt für Informatik verfolgt die aktuellen Bedrohungen in der digitalen Landschaft und bereitet die gewonnenen Erkenntnisse in Form eines Lagebildes für die kantonale Verwaltung auf. Das Lagebild berücksichtigt unter anderem Meldungen des Nationalen Zentrums für Cybersicherheit des Bundes (NCSC) sowie von anderen Partnerorganisation und zeigt die aktuelle Cyber-Bedrohungslage sowie Angriffsmethoden der Cyberkriminellen auf.

Die gefährlichsten Cyberbedrohungen für den Kanton Zürich sind heute Mehrfacherpressungen mit Verschlüsselung der Daten und Datendiebstahl, Cyberrisiken in der Lieferkette sowie der Einsatz neuer Technologien (KI, Cloud, IoT/OT). Es befindet sich ein sogenanntes Security-Cockpit im Aufbau, das dem Regierungsrat in Zukunft die Verletzbarkeit gegenüber diesen gefährlichsten Cyberbedrohungen innerhalb der Verwaltung aufzeigen soll. Zudem befindet sich ein Kennzahlensystem für die Beurteilung der Maturität im Bereich Cybersicherheit in den Direktionen und der Staatskanzlei in Umsetzung. Des Weiteren wird die Einhaltung der Sicherheitsvorgaben im Bereich Cybersicherheit regelmässig geprüft, und es werden unabhängige Audits von geschäftskritischen Prozessen und IT-Services durchgeführt. Mithilfe dieser verschiedenen Instrumente wird es dem Regierungsrat möglich sein, die Risiken gegenüber Cyberangriffen innerhalb der kantonalen Verwaltung zu steuern.

Der Kanton Zürich evaluiert den Einsatz von sogenannten Security Rating Services für die kantonale Verwaltung (vgl. Beantwortung der Frage 6). Diese sind ein weiteres Instrument, um die Sicherheitslage im Cyberbereich zu beurteilen. Der Einsatzbereich geht über die kantonale Verwaltung hinaus und vermittelt dem Regierungsrat auch Informationen zur Sicherheitslage von den selbstständigen Anstalten und weiteren staatsnahen Betrieben.

Zu Frage 6:

Der Regierungsrat hat im April 2023 der Durchführung eines Pilotversuchs zum Umgang mit Cyberrisiken in der kantonalen Lieferkette zugestimmt. Das Pilotprojekt wird vom CCSC koordiniert. Neben der kantonalen Verwaltung partizipieren weitere strategische Infrastrukturen im Kanton Zürich, unter anderem die Elektrizitätswerke des Kantons

Zürich, die Flughafen Zürich AG, das Universitätsspital Zürich, das Kantonsspital Winterthur, die Psychiatrische Universitätsklinik Zürich (PUK) sowie die Integrierte Psychiatrie Winterthur – Zürcher Unterland (ipw). Zum einen sollen mithilfe dieses Pilotprojekts Erfahrungswerte im Umgang mit Security Ratings zur Risikobewertung von Lieferantinnen und Lieferanten gesammelt werden. Zum anderen sollen die kantonalen Vorgaben im Bereich Cybersicherheit für öffentliche Vergabeverfahren und bestehende Vertragsverhältnisse auf die heutigen Bedrohungen im Cyberraum angepasst werden.

Das CCSC unterstützt zudem kantonsnahe Organisationen im Bereich der Sicherheitskultur, unter anderem die Gemeinden sowie die PUK und die ipw.

Die IT-Infrastruktur und die IT-Systeme in den Rechenzentren der Verwaltung werden kontinuierlich auf Anomalien untersucht, um möglichst rasch einen Cyberangriff erkennen zu können. Exponierte und kritische Schutzobjekte mit Auswirkungen auf Geschäftsprozesse werden priorisiert überprüft.

In den Bereichen Informationssicherheit und Datenschutz führen die zuständigen Stellen verschiedene Risikoanalysen durch und definieren Massnahmen, um angemessen mit den Risiken umgehen zu können. Zusätzlich ist der weitere Ausbau des integralen Risikomanagements gemäss RRB Nr. 1120/2022 im Gang, um die Weiterführung von kritischen Geschäftsprozessen und entsprechender Infrastruktur im Krisen- und Notfall zu gewährleisten.

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

Vor dem Regierungsrat
Die Staatsschreiberin:
Kathrin Arioli