Auszug aus dem Protokoll des Regierungsrates des Kantons Zürich

KR-Nr. 375/2021

Sitzung vom 8. Dezember 2021

1464. Anfrage (Kanton Zürich und Datensicherheit)

Kantonsrätin Erika Zahler, Boppelsen, sowie die Kantonsräte Martin Huber, Neftenbach, und Erich Vontobel, Bubikon, haben am 25. Oktober 2021 folgende Anfrage eingereicht:

Die jüngsten Vorkommnisse betreffend Datenschutz bei der öffentlichen Hand sind besorgniserregend. Medien berichteten in letzter Zeit vermehrt über Hackerangriffe in verschiedenen Städten, Gemeinden und Kantonen. Besonders brisant war die Mitteilung, dass auch der Bund von Hackerangriffen betroffen war.

Die drei nachfolgenden Beispiele sollen aufzeigen, wie in kürzester Zeit auf Gemeinde-, Kantons- und Bundesebene Cyberangriffe stattgefunden haben. Die Angriffe gingen von DDos-Attacken bis Ransomware (Schadsoftware) aus, die Daten verschlüsseln und für die Opfer unbrauchbar machen. Mitte Oktober 2021wurde die IT der Stadt Montreux gehackt. Ebenfalls Mitte Oktober 2021 wurde die Kantonswebsite des Kantons St. Gallen gehackt, und beim dritten Beispielwurde die Öffentlichkeit informiert, dass beim Bund das Online-Portal «easygov» gehackt wurde. So ist es den Hackern gelungen, auf der Bundesplattform «easygov» eine Liste mit Namen (bis zu 130000 Unternehmen) zu entwenden, welche im Jahr 2020 Covid-Kredite beantragt hatten.

Wer IT einsetzt und anwendet, wird verwundbar. Deshalb ist es äusserst wichtig, dass Sicherheit und Gegenmassnahmen einem hohen Standard entsprechen. In den Medien wurde aufgezeigt, dass seit der Pandemie die Cyberattacken nicht nur auf KMU, sondern auch auf öffentliche Anstalten wie Kanton, Gemeinden oder Spitäler stark zugenommen haben. Kann der Kanton Zürich die Sicherheit der persönlichen Daten seiner Einwohnerinnen und Einwohner gewährleisten?

In diesem Zusammenhang bitten wir den Regierungsrat um Beantwortung der nachfolgenden Fragen:

1. Kann im Kanton Zürich betreffend Hackerangriffe ein gleiches Ereignis eintreffen wie das erwähnte Beispiel auf Bundesebene?
2. Wie ist der Kanton Zürich gegen Hackerangriffe geschützt, und was sind weitere Pläne diesbezüglich?
3. Gibt es eine einheitliche Strategie betreffend Bekämpfung von Hackerangriffen über die verschiedenen Direktionen hinweg (inkl. Gerichte und Justizvollzug)?

4. Kann es zu Rückkopplungen kommen, wenn zum Beispiel eine Gemeinde infiziert wurde und sie so ein indirektes Einfallstor zu der Kantons-IT wird?
5. Werden die Digitalplattformen regelmässig auf Sicherheitslücken überprüft?
6. In welcher Zeit kann ein Cyber-Angriff auf den Kanton Zürich neutralisiert werden?
7. Was wird getan, wenn sensible Daten von Einwohnerinnen und Einwohnern via Hackerangriffe in falsche Hände kommen?

Auf Antrag der Finanzdirektion

beschliesst der Regierungsrat:

I. Die Anfrage Erika Zahler, Boppelsen, Martin Huber, Neftenbach, und Erich Vontobel, Bubikon, wird wie folgt beantwortet:

Zu Frage 1:

Die genannten Bedrohungen sind real und betreffen auch die kantonale Verwaltung. Die Einheit «IT-Sicherheit und Datenschutz» des Amtes für Informatik (AFI) beobachtet laufend die aktuelle Gefährdungslage und erstellt auf dieser Grundlage periodisch einen Bericht («Bedrohungsradar»).

Absolute Sicherheit gibt es nicht und daher kann auch die kantonale Verwaltung Opfer eines vergleichbaren Hackerangriffs werden. Nach wie vor werden schweizweit zahlreiche «Phishing-Angriffe» (Datenklau per E-Mail) beobachtet. Deren Anzahl ist seit ihrem Höhepunkt im ersten Quartal 2021 ein wenig gesunken, befindet sich jedoch weiterhin auf sehr hohem Niveau, wenn man sie mit dem Zeitraum vor der Coronapandemie vergleicht.

Allgemein gilt es, einen Angriff möglichst früh zu erkennen und darauf entsprechend zu reagieren. Zu diesem Zweck wurde ein Security Monitoring beim AFI aufgebaut, das sicherheitsrelevante Ereignisse zeitnah detektieren kann und in der Folge eine rasche Reaktion auf einen erkannten Cyberangriff erlaubt.

Zu Frage 2:

Im Sommer 2020 hat der Sicherheitsverbund Schweiz (SVS) eine Erhebung zur Verbesserung der Informationssicherheit in den Kantonen durchgeführt. Es wurden die Mindestanforderungen in Bezug auf relevante Prozesse, Aufgaben und Kompetenzen im Kanton Zürich analysiert. Das erkannte Verbesserungspotenzial in den verschiedenen Domänen in der kantonalen Verwaltung wurde bewertet, und gestützt darauf wurde ein Massnahmenkatalog erarbeitet.

Der Schutz gegen Hackerangriffe wird mittels angemessenen präventiven, detektiven und reaktiven Massnahmen kontinuierlich verbessert. Hervorzuheben sind insbesondere folgende Massnahmen:
- Umsetzung der Sicherheitsorganisation in den Direktionen und der Staatskanzlei (RRB Nr. 1193/2020)
- Umsetzung eines einheitlichen Grundschutzes in den Direktionen und der Staatskanzlei (RRB Nr. 1193/2020)
- Aufbau und Inbetriebnahme eines Security Operation Centers (SOC) zur zeitnahen Erkennung von Sicherheitsvorfällen (RRB Nr. 965/2020)
- Auf- und Ausbau der technischen Sicherheitsmassnahmen im Rahmen des IKT-Programms (RRB Nr. 383/2018)

Eine Beschreibung der weiteren Pläne findet sich in der Beantwortung der Frage 3.

Zu Frage 3:

Gemäss der Empfehlung des SVS und der Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren erarbeitet das AFI zusammen mit der Kantonspolizei, der Staatsanwaltschaft sowie dem Bevölkerungsschutz einen Vorschlag für die kantonale Cyberorganisation. Es gilt festzulegen, wie die Verwaltung und der Kanton Zürich langfristig mit dem Thema Cyberrisiken umgehen. Dabei orientiert man sich auch an den Ergebnissen und Strukturen von anderen Organisationen und Behörden, u. a. an den beiden Cyberstrategien im Kanton St. Gallen und im Fürstentum Liechtenstein sowie an der Cybersicherheitsagentur in Baden-Württemberg. Eine Aufgabe der kantonalen Cyberorganisation ist die Vernetzung im Bereich Cybersicherheit mit dem Bund (NCSC), anderen Kantonen sowie den Städten und Gemeinden, der Wirtschaft und den Hochschulen im Kanton Zürich. Mit «mehr Sicherheit» im Kanton Zürich soll ein Wettbewerbsvorteil geschaffen werden, um die Attraktivität des Wirtschaftsstandortes Zürich zu steigern.

Ein Vorschlag für die zukünftige Cyberorganisation im Kanton Zürich soll dem Regierungsrat 2022 vorgelegt werden. In einer ersten Phase liegt der Fokus auf der Minimierung der Sicherheitsrisiken der kantonalen Verwaltung und auf der Stärkung gegenüber Cyberangriffen. In einer zweiten Phase richten sich die Anstrengungen auf weitere, verwaltungsnahe Organe (z. B. Spitäler, Schulen der Sekundarstufe II und Gerichte) und die kritischen Infrastrukturen des Kantons.

Zu Frage 4:

Die Gemeinden und die kantonale Verwaltung sind über das gleiche Netzwerk miteinander verbunden (LEUnet). Aufgrund der technischen Gegebenheiten ist eine Rückkopplung von einer Gemeinde auf die Informatik der kantonalen Verwaltung möglich. Um diesem Risiko zu begeg-

nen, werden nur Services freigeschaltet, die von den Gemeinden tatsächlich benötigt werden, zudem sind verschiedene präventive technische Massnahmen (z. B. Firewalls) auf beiden Seiten für den gegenseitigen Schutz im Einsatz. Für den Fall, dass eine Gemeinde als indirektes Einfallstor dient, bestehen Vorkehrungen und Prozesse, um dies zu erkennen und die betroffene Gemeinde zu isolieren.

Zu Frage 5:

Ja, die kritischen digitalen Plattformen werden mittels technischer Scans sowie Audits der Organisation und Prozesse auf Sicherheitslücken überprüft.

Zu Frage 6:

Die Zeitdauer hängt vom einzelnen Ereignis ab und kann nicht allgemein benannt werden.

Wird ein Cyberangriff nicht sofort bemerkt oder ist dessen Behebung komplex, kann das Analysieren und Neutralisieren erhebliche Zeit beanspruchen.

Das SOC im AFI kann sicherheitsrelevante Ereignisse in Echtzeit verarbeiten. Wird ein Angriff festgestellt, wird er durch den Managed Security Service Provider und durch die Fachexpertinnen und -experten des AFI behandelt. Im Idealfall kann ein Cyberangriff bereits durch technische Massnahmen (z. B. Antivirusprogramm, Firewalls) sofort und automatisch neutralisiert werden.

Zur Illustration kann beispielhaft das Vorgehen bei einer Attacke durch Schadsoftware beschrieben werden: Zuerst gilt es, die Schadsoftware zu identifizieren und zu entfernen. Dies kann bedeuten, dass eine erhebliche Zahl von Endgeräten neu aufgesetzt werden muss. Bei verschlüsselten Daten müssen die Daten aus den Sicherungsdateien wiederhergestellt werden. Hier gilt es, die Wiederherstellungsmassnahmen zu priorisieren und die wichtigsten Geschäftsprozesse zuerst zu berücksichtigen. Werden vertrauliche Daten veröffentlicht, kann der Angriff unter Umständen gar nicht neutralisiert werden. Dann muss mit geeigneten Kommunikationsstrategien versucht werden, den Schaden in Grenzen zu halten.

Zu Frage 7:

Für den Abfluss sensibler Daten sowie weitere Szenarien bestehen spezifische Handlungsanweisungen, die das konkrete Vorgehen und die dafür notwendigen Ressourcen definieren. Diese sehen beispielsweise auch den Einbezug der Kommunikationsstellen, der Fachstelle Cybercrime der Kantonspolizei Zürich sowie des Kompetenzzentrums Cybercrime der Staatsanwaltschaft Zürich vor.

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

Vor dem Regierungsrat
Die Staatsschreiberin:
Kathrin Arioli