Auszug aus dem Protokoll des Regierungsrates des Kantons Zürich

KR-Nr. 343/2013

Sitzung vom 5. Februar 2014

135. Anfrage (Nachrichtendienstliche Tätigkeiten im Kanton Zürich)

Die Kantonsräte Lorenz Habicher, Zürich, und Jürg Sulser, Otelfingen, haben am 11. November 2013 folgende Anfrage eingereicht:

In verschiedensten Medien herrscht eine Flut von Meldungen betreffend nachrichtendienstliche Tätigkeiten der National Security Agency (NSA) in der Schweiz. Der Wirtschaftsstandort und Finanzplatz Zürich scheint auch im Fokus solcher Spionagetätigkeiten zu sein. Seit dreissig Jahren gibt es solche Tätigkeiten unter befreundeten Ländern und dies sollte, so könnte man glauben, zu keinem medialen Aufschrei führen.

Was im Verdeckten ermittelt wird, kann später in Geschichtsbüchern nachgelesen werden. Die wirtschaftliche Bedrohung existiert aber real und sollte auch von der Politik erkannt und besprochen werden.

Im Melde- und Analysestellen Informationssicherung (MELANI) Halbjahresbericht 2013/1 werden gezielte und professionelle Angriffe auf Unternehmen oder staatliche Stellen genannt. Es handelte sich bei diesen Angriffen meist um sogenannte Advanced Persistent Threats (ATP).

Die zu Beginn dieses Jahres erfolgten, besonders auf US-Firmen zielenden Attacken führten zu zahlreichen Stellungnahmen hochrangiger US-Politiker. Die zahlreichen Attacken auf Schweizer Unternehmen scheinen in der hiesigen Politik kein Augenmerk zu geniessen.

In diesem Zusammenhang stellen sich folgende Fragen:

1. Kann der Regierungsrat solche ATP's gegen den Wirtschafts- und Finanzplatz Zürich bestätigen und das Ausmass beziffern?
2. Welchen Anteil haben dabei organisierte staatliche Angriffe und aus welchen Staaten wurden oder werden diese geführt?
3. Ist der Kanton Zürich auch betroffen und welcher Schaden ist dabei entstanden?
4. Welche Direktionen sind betroffen und welchem Zweck dienten diese Attacken? Sind heikle Daten wie z. B. Steuerdaten entwendet oder missbraucht worden?
5. Welche Massnahmen ergreift der Zürcher Regierungsrat dagegen?

Auf Antrag der Sicherheitsdirektion

beschliesst der Regierungsrat:

I. Die Anfrage Lorenz Habicher, Zürich, und Jürg Sulser, Otelfingen, wird wie folgt beantwortet:

Die Beschaffung von Informationen im In- und Ausland, um Bedrohungen und Gefahren für die Schweiz und ihre Bevölkerung rechtzeitig zu erkennen, ist eine Aufgabe des Bundes. Der Nachrichtendienst des Bundes (NDB) nimmt diese Aufgabe gestützt auf das Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit (BWIS; SR 120) und das Bundesgesetz über die Zuständigkeiten im Bereich des zivilen Nachrichtendienstes (ZNDG; SR 121) wahr. Er wird dabei durch die Vollzugsbehörden der Kantone, im Kanton Zürich durch den Dienst Nachrichtenbeschaffung der Kantonspolizei, unterstützt. Der NDB informiert die Öffentlichkeit jährlich mit dem Lagebericht «Sicherheit Schweiz», in dem er jeweils eine umfassende Beurteilung der Bedrohungslage vornimmt.

Zu Fragen 1 und 2:

Aufgrund der eingangs dargestellten Zuständigkeitsregelung wäre eine über den erwähnten Lagebericht «Sicherheit Schweiz» hinausgehende Information über allfällige Advanced Persistent Threats (ATP) Sache des Bundes. Dabei ist darauf hinzuweisen, dass gerade in diesem sensiblen Bereich der Information aus Sicherheitsgründen enge Grenzen gesetzt sind.

Eine Nachfrage bei der Zürcher Handelskammer und dem Zürcher Bankenverband hat ergeben, dass diese Organisationen dem Schutz vor Cyber-Risiken einen sehr hohen Stellenwert einräumen. Weiter gehende Auskünfte und insbesondere Angaben zu allfälligen ATP wurden aus den genannten Gründen nicht erteilt.

Zu Fragen 3 und 4:

Bis heute konnten keine systematischen und gezielten Angriffe auf Infrastrukturen und Daten im Bereich der Direktionen und der Staatskanzlei festgestellt werden. Entsprechend ist auch kein Diebstahl oder Missbrauch von besonders geschützten Daten oder anderen bekannt.

Zu Frage 5:

Die kantonale Netz-Infrastruktur ist gegen aussen mit den heute zur Verfügung stehenden technischen Mitteln gesichert. Zugriffe über das Internet (WebAccess, E-Mail) und Transaktionen über die Transaktionsplattform ZHservices werden dauernd überwacht. Zudem werden die

Mitarbeitenden für einen sicherheitsbewussten Umgang mit der Informations- und Kommunikationsinfrastruktur sensibilisiert und ausgebildet (Security Awareness).

Der Schutz der Informations- und Kommunikationsinfrastrukturen vor Cyber-Risiken ist ein ständiger Prozess. Das gestützt auf die Verordnung über die direktionsübergreifende Informatik (KITT-Verordnung; LS 170.7) gebildete Kantonale IT-Team (KITT) hat entsprechend eine IT-Sicherheitsorganisation für die kantonale Verwaltung mit einem Kompetenzzentrum für IT-Sicherheit erarbeitet. Damit soll künftig die Sicherheit im Informatikbereich nochmals verbessert werden.

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

Vor dem Regierungsrat
Der Staatsschreiber:
Husi