



Protokollauszug
17. Sitzung vom 20. September 2023

212/2023 9.5.2.1 Kleine Anfrage von Daniel Laubi betreffend "IT-Security der Stadt Schlieren" Beantwortung

1. Kleine Anfragen

Am 5. Juli 2023 wurde von Gemeindeparlamentarier Daniel Laubi die folgende Kleine Anfrage betreffend "IT-Security der Stadt Schlieren" eingereicht.

"Schweizer Behörden mussten sich zurzeit gleich mit mehreren Cyber-Attacken auseinandersetzen. Ende Mai 2023 wurde der IT-Dienstleister Xplain angegriffen, zu dessen Kunden Bundesbetriebe wie die Fedpol und die Schweizer Armee, aber auch mehrere Kantons Polizeien gehören. Hierbei stellte sich heraus, dass auch «operative Daten» aus der Bundesverwaltung betroffen sind. Diese wurden dann am 14. Mai 2023 im Umfang von einem Terabyte im Darknet geleakt. Neben dem IT-Angriff auf Xplain wurden sodann die Websites von verschiedenen Schweizer Behörden, Kantonen und Städten mittels DDoS-Attacken (Distributed Denial of Service) angegriffen. Die neusten Angriffe zeigen, dass nicht nur Unternehmen, sondern auch Städte und Kantone zunehmend attraktive Ziele für Hacker werden.

Ich bitte daher um Beantwortung folgender Fragen:

- *Wurde die Stadt Schlieren bzw. deren beauftragten IT-Dienstleistern kürzlich ebenfalls von Hackern attackiert?*
- *Werden im Lichte der jüngsten Ereignisse durch die Stadt Schlieren Massnahmen betreffend ihrer IT-Security ergriffen?*
- *Werden dabei auch die Verträge mit ihren Informatikdienstleistern überprüft (wie dies zurzeit auch der Bund tut)?*
- *Hat die Stadt Schlieren im Falle eines Cyber-Angriffes einen inzident Response Plan und wird hierbei externe Hilfe geholt?"*

2. Antwort des Stadtrats

Frage 1: Wurde die Stadt Schlieren bzw. deren beauftragte IT-Dienstleister kürzlich ebenfalls von Hackern attackiert?

Antwort:

Die Stadt Schlieren und insbesondere deren beauftragte Dienstleister sind regelmässigen Cyberangriffen ausgesetzt. Aus diesem Grund sind entsprechende Sicherheitsmassnahmen seit langer Zeit umgesetzt und sie werden in regelmässigen Abständen überprüft. Bis anhin war keine der ausgeführten Attacken erfolgreich.

Frage 2: Werden im Lichte der jüngsten Ereignisse durch die Stadt Schlieren Massnahmen betreffend ihrer IT-Security ergriffen?

Antwort:

Der Stadtrat hat schon vor einiger Zeit Massnahmen ergriffen, um das Risiko eines erfolgreichen Cyber-Angriffs zu minimieren. So wird beispielsweise das Antivirusprogramm mehrmals täglich aktualisiert, die Firewall wird durch externe Dienstleister zusätzlich aktiv überwacht, der Fernzugriff kann nur mit einer 2-Faktor-Authentisierung erfolgen, Mitarbeitende werden regelmässig sensibilisiert. Als Träger kritischer Infrastrukturen ist die Stadt Schlieren in ein Infosystem des Nationalen Cyber Security Centers (NCSC) eingebunden. Mit der Aktualisierung des Incident Response Plans werden sich wahrscheinlich zusätzliche Massnahmen ergeben.

Frage 3: Werden dabei auch die Verträge mit ihren Informatikdienstleistern überprüft (wie dies zurzeit auch der Bund tut)?

Antwort:

Die wichtigsten Informatikdienstleister der Stadt Schlieren verfügen über Zertifizierungen im Bereich Security Management (ISO 27001) und IT-Service Management (ISO 20000). Der Stadtrat ist sich aber bewusst, dass trotz allen Zertifizierungen und vertraglichen Abmachungen mit Dienstleistungsunternehmen die Verantwortung für die Daten bei der Stadt verbleibt. Diese Verantwortung wird wahrgenommen.

Frage 4: Hat die Stadt Schlieren im Falle eines Cyber-Angriffes einen Incident Response Plan und wird hierbei externe Hilfe geholt?

Antwort:

Es besteht ein Incident Response Plan, welcher mit externen Security-Spezialisten aktualisiert und überarbeitet wird.

Der Stadtrat beschliesst:

1. Die Kleine Anfrage von Daniel Laubi betreffend "IT-Security der Stadt Schlieren" wird im Sinne der vorstehenden Ausführung beantwortet.
2. Mitteilung an
 - Fragesteller
 - Gemeindeparlament
 - Abteilungsleiter Finanzen und Liegenschaften
 - Archiv

Status: öffentlich

Stadtrat Schlieren

Markus Bärtschiger
Stadtpäsident

Janine Bron
Stadtschreiberin