STADTKLOTEN

PROTOKOLL GEMEINDERAT KLOTEN

07.02.2022 Beschluss Nr. 23-2023 Interpellation 8576; Hansjürg Schmid, FDP; Wie steht es um die Sicherheit in unseren IT-Systemen gegenüber Cyberattacken?; Beantwortung / Stellungnahme

0.5.4 Parlamentarische Vorstösse

Interpellation 8576; Hansjürg Schmid, FDP; Wie steht es um die Sicherheit in unseren IT-Systemen gegenüber Cyberattacken?; Beantwortung / Stellungnahme

Am 04. Oktober 2022 reichte GR Hansjürg Schmid (FDP) eine Interpellation ein, welche mit Beschluss-Nr. 266-2022 vom 25. Oktober 2022 durch den Stadtrat Kurt Hottinger und Ruedi Ulli zur Beantwortung überwiesen wurde.

Inhalt Interpellation

Fast täglich lesen wir über Cyberattacken in den Tageszeitungen. Betroffen davon sind nicht nur Firmen, Online-Shops, Spitäler oder weltweite Zahlungsdienstleister. Gemäss den beiden Halbjahresberichten der NCSC (National Center for Cybersecurity) wurden im 2021 21'700 Cybersicherheitsvorfälle an das NCSC gemeldet. Gegenüber dem Vorjahr, in welchem ca. 10'700 Meldungen verzeichnet wurden, ist dies eine Steigerung von 102% oder einfacher, eine Verdoppelung der Anzahl Meldungen.

Mittlerweile sind auch öffentliche Verwaltungen zur Zielscheibe von Cyberkriminellen geworden. Zwei bedeutende Beispiele in diesem Jahr,

- *10.01.2022: Cyberangriff auf IT-Dienstleister der Gemeinde Yverdon-les-Bains*
- *18./19.07.2022: Cyberangriff auf die Stadtverwaltung Bülach*

Ein Cyberangriff muss nicht unmittelbar auf eine öffentliche Verwaltung zielen. Angriffe auf die Lieferkette (Supply Chain) von IT-Dienstleistern sind viel effizienter, da diese meist mehrere Kunden auf ihren Systemen als Mandanten beherbergen. Zudem impliziert eine Mehrlieferanten-Strategie das Risiko eines erhöhten Ausfalls von mehreren Fachapplikationskomponenten oder von Geldforderungen aufgrund fremdverschlüsselter Daten. Wie bei allen Arten eines Angriffs erfolgt ein Cyberangriff immer auf potenzielle Schwachstellen, meist auf Schnittstellen zwischen zwei Komponenten. Komponenten können zwei IT-Systeme oder IT-System zu Menschen sein. Im letzteren Fall ist die grösste Schwachstelle der Mensch selbst.

Wir bitten den Stadtrat um die Beantwortung folgender Fragen:

1. *Sicherheitskonzept*
    a. *Wurde das Sicherheitskonzept mit Experten (intern und extern) erarbeitet?*
    b. *Wurden die Lieferanten bei der Erstellung miteinbezogen?*
    c. *Mit welchen Stellen (Bund, Kanton) arbeitet die Stadt Kloten zusammen?*

d. *Ist das Bug Bounty-Programm (Kopfgeldprogramm für das Auffinden von Programmfehlern in Systemen) Teil des Sicherheitskonzepts?*

e. *Durch wen wird das Sicherheitskonzept regelmässig überprüft?*

2. *Sicherheitsprophylaxe in der Stadtverwaltung*

   a. *Wie werden die Mitarbeitenden der Stadtverwaltung sensibilisiert?*

   b. *Wie werden Personen sensibilisiert, die nicht in der Stadtverwaltung arbeiten?*

   c. *Werden die Lieferanten ebenfalls berücksichtigt, bzw. eingebunden?*

3. *Notfallplan (Teil des Sicherheitskonzepts)*

   a. *Wie sieht die Notfallorganisation aus?*

   b. *Wie sieht der Notfall-Ablauf aus?*

4. *Werden derzeit Cyberangriffe detektiert?*

   - *Wenn ja,*

     a. *seit wann?*

     b. *werden diese der NCSC gemeldet?*

     c. *werden daraus Trend-Analysen zu Handen des Stadtrats erstellt?*

     d. *Wie viele Angriffe hat die Stadt Kloten abwehren können?*

Besten Dank für das zeitnahe Beantworten der obenstehenden Fragen, besonders angesichts der sich momentan abzeichnenden kritischen Situation.

Beantwortung

Der Stadtrat beantwortet die Fragen wie folgt:

1) Sicherheitskonzept

1) Wurde das Sicherheitskonzept mit Experten (intern und extern) erarbeitet?

Ja. IT-Sicherheit ist von immer grösser werdender Bedeutung. Einerseits haben immer mehr Mitarbeitende Zugriff auf elektronische Hilfsmittel, andererseits werden immer mehr Services online bezogen. Die permanente Verfügbarkeit von Services bedeutet, dass fast alle Systeme im internen Netzwerk auch auf das Internet zugreifen müssen. Systeme, welche Zugriff auf das Internet benötigen, werden dadurch aber auch von aussen angreifbar. Die Informatik der Stadt Kloten unternimmt viel, um die Systeme gegen aussen abzusichern. Dabei stehen gleich mehrere Verteidigungslinien nach dem Zwiebelschalenprinzip im Einsatz. Jede der Verteidigungslinien steht dabei für eine Schicht der Zwiebel. Wird die erste Schicht durchbrochen, stehen noch weitere zur Verfügung. Das Konzept sieht 7 Schichten vor und wurde von der Informatikabteilung in Zusammenarbeit mit externen Dienstleistern erarbeitet.

a. Wurden die Lieferanten bei der Erstellung miteinbezogen?

Ja. Bei der Evaluierung und Auswahl der einzelnen Schichten wurden die Lieferanten miteinbezogen. Nur so konnte sichergestellt werden, dass die einzelnen Schichten aufeinander abgestimmt sind und sich nicht gegenseitig stören.

b. *Mit welchen Stellen (Bund, Kanton) arbeitet die Stadt Kloten zusammen?*

Die Stadt Kloten bezieht mit LEUnet Dienstleistungen des Kantons. LEUnet ist ein Datennetzwerk des Kantons Zürich für die Gemeinden und die kantonale Verwaltung. Das LEUnet ist in logische Netze (z.B. Gemeinden, Spitäler, Kanton usw.) unterteilt. Das für Verwaltungsaufgaben konzipierte Datennetzwerk mit Garantien für hohe Verfügbarkeit und Betriebssicherheit wird von Swisscom betrieben. Speziell der Sicherheit der Daten wird mit LEUnet durch umfangreiche Massnahmen Rechnung getragen. Mit dem Bund besteht eine (lose) Zusammenarbeit mit dem Nationalen Zentrum für Cybersicherheit (NCSC). Wenn die Stadt Kloten von einem Cybersicherheitsvorfall betroffen ist, wird eine Meldung an das NCSC gemacht.

c. *Ist das Bug Bounty-Programm (Kopfgeldprogramm für das Auffinden von Programmfehlern in Systemen) Teil des Sicherheitskonzepts?*

Nein. Die Stadt Kloten setzt keine selber entwickelte Software ein, sondern setzt auf Standardsoftware. Aus diesem Grund gibt es bei der Stadt Kloten kein solches Programm.

d. *Durch wen wird das Sicherheitskonzept regelmässig überprüft?*

Die Stadt Kloten hat einen externen Informationssicherheitsbeauftragten. Ausserdem wird die Stadt Kloten im Rahmen der Assessments der Datenschutzbeauftragten regelmässigen Kontrollen betreffend Einhaltung des Gesetzes über die Information und den Datenschutz (IDG) unterworfen.

2. *Sicherheitsprophylaxe in der Stadtverwaltung*

a. *Wie werden die Mitarbeitenden der Stadtverwaltung sensibilisiert?*

Mit mehreren Massnahmen. Einerseits werden die Mitarbeitenden von Zeit zu Zeit per E-Mail über Verhaltensweisen in Bezug auf Phishing oder Social Engineering informiert. Andererseits wurden alle Mitarbeitenden im Rahmen einer EasyLearn-Schulung (Online-Learning) in Bezug auf Informationssicherheit und Datenschutz geschult. Seit einigen Wochen verfügt die Stadt Kloten zudem mit Sophos Phish Threat über ein System, mit welchem die Mitarbeitenden systematisch im korrekten Umgang mit Phishing Mails trainiert werden können.

b. *Wie werden Personen sensibilisiert, die nicht in der Stadtverwaltung arbeiten? (Damit sind gemäss H. Schmid z.B. folgende Gruppen gemeint: Gemeinderäte, Stadträte, Kommissionsmitglieder, etc., welche jedoch ebenfalls über einen E-Mailaccount bei der Stadt verfügen)*

Diese Personengruppe wurde in der Vergangenheit deutlich zu wenig berücksichtigt. In der Zukunft sollen diese Nutzenden ebenfalls in Awareness-Kampagnen eingebunden werden und erhalten die Informationen zu den Regelungen bezüglich Informationssicherheit und Datenschutz wie interne Mitarbeitende.

c. *Werden die Lieferanten ebenfalls berücksichtigt, bzw. eingebunden?*

Die Lieferanten sind nicht direkt in die Sensibilisierungskampagnen der Stadt eingebunden. Mittels Verträgen werden die Lieferanten jedoch verpflichtet, das IDG des Kantons einzuhalten. Mitarbeitende der Lieferanten mit Zugriff auf personenbezogene Daten der Stadt Kloten müssen Geheimhaltungserklärungen unterzeichnen.

3. *Werden derzeit Cyberangriffe detektiert?*
   a. *seit wann?*

Seit die Stadt Kloten einen Zugang ins Internet hat, wenn man bereits einen Port-Scan als Cyber-Angriff deklariert. Solche Angriffe finden heutzutage permanent statt. Es gibt kaum einen Internet-Anschluss, welcher nicht regelmässigen Port-Scans ausgesetzt ist. Mit einem Port-Scan kann ein Angreifer überprüfen, mit welchen Protokollen und Ports kommuniziert werden kann. Findet der Angreifer einen Port, welcher eine Kommunikation zulässt, kann er versuchen, Schwachstellen zu finden und diese gezielt auszunutzen.

   b. *werden diese der NCSC gemeldet?*

Nicht generell. Sonst müsste man täglich viele Meldungen an das NCSC machen, was nicht zielführend wäre.

   c. *werden daraus Trend-Analysen zu Handen des Stadtrats erstellt?*

Nein. Es werden derzeit gar keine Trend-Analysen erstellt.

   d. *Wie viele Angriffe hat die Stadt Kloten abwehren können?*

Die Stadt Kloten führt keine Statistik der Angriffe, somit ist diese Zahl nicht bekannt.

Beschluss:

1. Die Antwort des Stadtrats betreffend der Interpellation 8576 wird zur Kenntnis genommen und die Interpellation stillschweigend abgeschrieben.

Mitteilung an:
- Hansjürg Schmid (FDP)
- Gemeinderat
- Bereichsleiter Finanzen + Logistik

Für getreuen Auszug:

Versandt: 08. Feb. 2023

Jacqueline Tanner
Ratssekretärin