

2024/16 0.04.05.03 Postulat

Postulat "Sicherung kritischer Infrastruktur durch Cyber Security Audits", Entgegennahme (Parlamentsgeschäft 23.03.08)

Wählen Sie ein Element aus. Stadtrat

1. Die Erklärung zur Entgegennahme des Postulats "Sicherung kritischer Infrastruktur durch Cyber Security Audits" und die dazugehörige Stellungnahme werden genehmigt.
2. Öffentlichkeit des Beschlusses:
 - Der Beschluss ist per sofort öffentlich.
3. Mitteilung durch Sekretariat an:
 - Parlamentsdienste (als Mitteilung mit Erklärung und Stellungnahme)
 - Mitglieder der Geschäftsleitung
 - Stadtwerke Wetzikon
 - Leitung Informatik
 - Abteilung Bevölkerung + Sicherheit
 - Stadtpolizei Wetzikon
 - Abteilung Tiefbau
 - Bereich Stadtentwässerung /ARA

Erwägungen

Das Ressort Präsidiales, Entwicklung + Kultur unterbreitet dem Stadtrat die Entgegennahme des Postulats "Sicherung kritischer Infrastruktur durch Cyber Security Audits " zur Beantwortung an das Parlament.

Erklärung

Der Stadtrat ist bereit, das Postulat "Sicherung kritischer Infrastruktur durch Cyber Security Audits " entgegenzunehmen.

(Zuständig im Stadtrat Pascal Bassu, Ressort Präsidiales, Entwicklung + Kultur)

Stellungnahme

Ausgangslage

Das nachfolgende Postulat von Gerhard Schwabe (GLP) und Joel Hoff (FDP) und 29 Mitunterzeichnenden ist an der Parlamentssitzung vom 11. Dezember 2023 begründet worden:

Sicherung kritischer Infrastruktur durch Cyber Security Audits

Die Bedeutung von Cyber Security nimmt in unserer zunehmend vernetzten Welt stetig zu. Insbesondere in der Stadt Wetzikon, die über eine Vielzahl kritischer Infrastrukturen verfügt, ist es von entscheidender Bedeutung, Massnahmen zu ergreifen, um die Sicherheit dieser Infrastrukturen vor Cyberangriffen zu gewährleisten.

Die Stadt Wetzikon betreibt kritische Einrichtungen wie beispielsweise die Wasserversorgung und Stromversorgung, auf die wir in unserem täglichen Leben angewiesen sind. Durch die zunehmende Verwendung einer "smarten" Infrastruktur (von Smart Meters bis zu Smart City) steigt die Anfälligkeit für Störungen. Es ist in Anbetracht der massiv steigenden Hackingangriffe auf KMUs wie auch staatliche Einrichtungen besorgniserregend, dass dem Thema Cyber Security in der Stadt Wetzikon (inkl. Stadtwerke) bislang nur wenig Aufmerksamkeit geschenkt wird.

Bisher wurden noch keine externen Cyber Security Audits durchgeführt, um die Sicherheit kritischer Infrastrukturen der Stadt Wetzikon zu gewährleisten. Im Falle eines Cyberangriffs wäre die Stadt Wetzikon nicht nur erpressbar, es entstünden auch erhebliche finanzielle Schäden. Auch der Ausfall zentraler technischer Komponenten kann bedeutende Konsequenzen haben.

Daher reichen wir dieses Postulat ein und fordern den Stadtrat von Wetzikon auf, unverzüglich Massnahmen zu ergreifen. Der Stadtrat soll die kritischsten Infrastrukturen unserer Stadt, insbesondere die Wasserversorgung und Stromversorgung, sowie andere lebenswichtige Dienste, regelmässigen, externen Cyber Security Audits unterziehen.

Diese Audits sollen sicherstellen, dass angemessene Sicherheitsmassnahmen implementiert sind, um unsere Infrastruktur vor potenziellen Cyberbedrohungen zu schützen. Weiter sollen Informationen zu den Ergebnissen im Rahmen des Geschäftsberichts, dem Parlament zur Verfügung gestellt werden.

Die Sicherheit unserer Stadt und unserer Bürgerinnen und Bürger sollte höchste Priorität haben, insbesondere im Hinblick auf die sich ständig weiterentwickelnden Cyberbedrohungen. Dieses Postulat dient dem Schutz unserer kritischen Infrastruktur und der Gewährleistung einer sicheren Zukunft für Wetzikon.

Formelles

Mit einem Postulat verpflichtet das Parlament den Stadtrat gemäss Art. 47 der Geschäftsordnung des Parlaments (GeschO Parlament), im Rahmen eines Berichts zu prüfen, ob eine Vorlage auszuarbeiten ist, die in die Zuständigkeit des Parlaments oder der Stimmberechtigten fällt bzw. eine Massnahme zu treffen, die in Zuständigkeit des Stadtrats fällt. Nach Art. 48 Abs. 2 GeschO Parlament teilt der Stadtrat

innert zwei Monaten mit, ob er bereit ist, das Postulat entgegenzunehmen. Ist eine eigenständige bzw. unterstellte Kommission beteiligt, verlängert sich die Frist auf drei Monate. Mit dem vorliegenden Beschluss ist diese Frist gewahrt.

Erwägungen des Stadtrats

Cyberangriffe sind eine zunehmende Bedrohung weltweit, die auch vor den öffentlichen Institutionen nicht Halt machen. In den vergangenen Jahren haben die digitalen Attacken weiter zugenommen. Zu den Betroffenen gehören nicht nur grosse private Unternehmen und öffentliche Organisationen auf Bundes- oder Kantonsebene, sondern auch zahlreiche Schweizer Gemeinde- und Stadtverwaltungen. Die Ziele der Angreifer sind vielfältig; meist stehen kriminell oder politisch motivierte Angriffe im Vordergrund.

Im Rahmen der Vision Wetzikon 2040 werden die städtischen Dienstleistungen zunehmend digital transformiert, was einerseits effiziente und kundenfreundliche Prozesse ermöglicht, andererseits aber die Menge wichtiger und vertraulicher Daten weiter anwachsen lässt und so die Attraktivität für Cyberangriffe potenziell erhöht wird.

Die IT-Sicherheit muss mit der kontinuierlichen Vernetzung von Systemen und der daraus resultierenden höheren Komplexität unbedingt Schritt halten, ansonsten die Anfälligkeit erfolgreicher Cyberangriffe rasch zunehmen könnte. Im "worst case" hätte eine erfolgreiche Cyberattacke schwerwiegende Auswirkungen zur Folge. Dazu gehören nicht nur hohe Kosten und Gesamt-/Teilausfälle in der Leistungserbringung, sondern auch das Risiko von Datenverlust sowie Geheimnis- und Datenschutzverletzungen. Nicht zu unterschätzen ist zudem der Vertrauensverlust der Bevölkerung in die öffentliche Institution.

Obwohl die Stadt Wetzikon und ihre IT-Zulieferer bereits heute wirksame organisatorische und technische Massnahmen zur Verhinderung von Cyberangriffen einsetzen, ist eine weiterführende Analyse mittels regelmässiger externer Cybersecurity Audits ein wirksames Mittel, um allfällige Lücken im Bereich kritischer Infrastrukturen aufzeigen und schliessen zu können. In Anlehnung an das Postulat werden die kritischsten Infrastrukturen der Wasser- und Stromversorgung, der Stadtentwässerung und der Sicherheit (Stadtpolizei, Feuerwehr, Zivilschutz) einem Cyber Security Audit unterzogen. Beispielsweise das auf Stadtgebiet in der Gesundheitsversorgung tätige GZO Spital Wetzikon ist als eigenständige Unternehmung von diesem Audit abgegrenzt.

Der Stadtrat ist sich dem Risiko bewusst und erachtet den Schutz kritischer Infrastruktur als elementare Voraussetzung für den reibungslosen Betrieb der Stadt Wetzikon. Der Stadtrat unterstützt die Anliegen des Postulats "Sicherung kritischer Infrastruktur durch Cyber Security Audits" und ist bereit, dieses entgegenzunehmen.

Für richtigen Protokollauszug:



Stadtrat Wetzikon

Melanie Imfeld, Stadtschreiberin a.i.