wetzikon

Stadtrat

Auszug aus dem Protokoll Sitzung vom 8. Januar 2025

2025/7 9.07.02.02 Infrastruktur
Cyber Security, Umsetzung Massnahmen 2025, Kreditbewilligung

Beschluss Stadtrat

1. Der Umsetzung des Cyber Security Massnahmenkatalogs 2025 wird zugestimmt und die Abteilung Informatik mit der Umsetzung beauftragt.

2. Für die Umsetzung wird ein Kredit über 107'720 Franken inkl. MWST bewilligt.

3. Die Ausgaben sind der Erfolgsrechnung 2025 wie folgt zu belasten:

   Konto 1021.3130.00 107'720 Franken

4. Öffentlichkeit des Beschlusses:
   – Der Beschluss ist per sofort öffentlich.

5. Mitteilung durch Sekretariat an:
   – Mitglieder Geschäftsleitung
   – Abteilungsleiter Informatik
   – Bereichsleiter Stadtentwässerung /ARA
   – Parlamentsdienste (zuhanden Parlament)

Ausgangslage

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.

Mit der Digitalisierung werden nicht nur Datenprozesse bearbeitet und automatisiert, sondern zunehmend auch Produktionsprozesse gesteuert. Die Information Technology (IT) wird durch die Operational Technology (OT) ergänzt. Die OT wird bei den Stadtwerken und der Abwasserreinigungsanlage eingesetzt, um die kritischen Infrastrukturen der Ver- und Entsorgung zu überwachen und zu steuern. Die OT ermöglicht einerseits eine effiziente Prozessführung der komplexen Anlagen. Andererseits führen die digitale Erschliessung und Vernetzung solcher Systeme zu zusätzlichen Angriffsflächen mit entsprechenden Auswirkungen bei einem Ausfall. In der Vergangenheit wurden solche Produktionslinien in der Regel als Offline-Insellösungen realisiert. Im Zuge der Modernisierung und Digitalisierung steigt die Gefahr, dass genau solche Systeme angegriffen und manipuliert werden könnten.

Trotz Annäherung von IT und OT greifen bewährte Sicherheitsprinzipien aus der traditionellen IT aufgrund langer Lifecycle-Zyklen bei OT-Systemen nur langsam.

Erkenntnisse und Massnahmen aus Bericht Postulat

Im Rahmen des Postulat "Sicherung kritischer Infrastruktur durch Cyber Security Audits" wurde in Zusammenarbeit mit InfoGuard AG eine Security Assessment mit Fokus auf die kritischen Infrastrukturen durchgeführt. Die im Assessment identifizierten Risiken wurden den Bereichen Governance, Risiko Management, Dienstleister (Third Party Risk Management, TPRM), Vulnerability und Patch Management, Perimeterschutz sowie Cyber Resilienz zugeordnet.

Obwohl die Stadt Wetzikon und ihre IT-Zulieferer bereits heute wirksame organisatorische und technische Massnahmen zur Abwehr von Cyberangriffen einsetzen, ist eine kontinuierliche Überprüfung und Anpassung des Sicherheitsdispositivs angezeigt. Die Cybersicherheit ist keine einmalige Angelegenheit, denn die Bedrohungslage und damit die Risikosituation ändern sich permanent. Zudem gilt der Grundsatz, wer Geschäftsprozesse digitalisiert, muss sich zwingend auch mit dem Thema Sicherheit auseinandersetzen.

Um einen wirksamen Schutz vor Cyberangriffen zu gewährleisten, ist ein ganzheitlicher Ansatz anzustreben, wobei Prozesse, Technologie und Mensch gleichermassen berücksichtigt werden. Für die Cybersicherheit ist es entscheidend, die Angriffsfläche zu verringern. Neben technischen Massnahmen wie dem Abbau von Schwachstellen und der permanenten Überwachung ist insbesondere der Faktor Mensch von grosser Bedeutung. Sicherheit ist nicht nur "Chefsache"; vielmehr sind alle Mitarbeitenden gefordert, mögliche Sicherheitsrisiken rechtzeitig zu erkennen und angemessen darauf zu reagieren. Häufig werden Cyberangriffe erst durch die Schwachstelle "Mensch" möglich.

Gleichzeitig ist trotz aller Sicherheitsvorkehrungen ein Restrisiko in Kauf zu nehmen, da eine 100-prozentige Sicherheit nicht existiert. Die Stadt Wetzikon muss sich deshalb auch auf einen erfolgreichen Cyberangriff vorbereiten und in der Lage sein, Sicherheitsvorkommnisse zu erkennen, schnell darauf zu reagieren und die Auswirkungen auf ein Minimum zu reduzieren.

Aufgrund der Ergebnisse aus dem Assessment sollen in Anlehnung an das NIST-Framework wirksame Massnahmen umgesetzt werden. Um diesen Prozess in Gang zu bringen, werden externe Ressourcen in Form eines CISO as a Service eingesetzt. Ziel ist es, den Massnahmenplan Cyber- und Informationssicherheit 2025 umzusetzen. Bereits jetzt wurden erste Sofortmassnahmen in verschiedenen Bereichen ergriffen. Bis zum Jahr 2025 sollen zusätzlich organisatorische Grundlagen entwickelt werden, um die Priorisierung der Informationssicherheit und des Risikomanagements zu gewährleisten. Dazu gehört die klare Definition von Verantwortlichkeiten auf strategischer und operativer Ebene der Stadt sowie die Benennung zuständiger Stellen. Auf Basis der erarbeiteten Richtlinien und Massnahmen soll ausserdem ein operatives Risikomanagement eingeführt werden.

Mit der Umsetzung der aus dem Assessment definierten Massnahmen kann die Stadt ihre kritische Infrastruktur besser vor Cyberrisiken schützen und eine sichere Zukunft gewährleisten.

Kosten

Die für 2025 geplanten Massnahmen sollen in einem CISO as a Service-Mandat umgesetzt werden. Damit werden Ressourcen und Expertise auf einer externen Basis in Anspruch genommen. Die Auf-

tragsvergabe erfolgt an die Firma InfoGuard AG, Baar, welche bereits das Security-Assessment im Rahmen des Postulats begleitete.

Zur Umsetzung des Massnahmenplans Cyber- und Informationssicherheit 2025 gehen wir von einem 20% Pensum, 1 Personentag pro Woche, aus:

Kosten CISO as a Service-Mandat

Menge	Einheiten	Beschreibung	Stückpreis	Betrag
48	Tage	Informationssicherheitsbeauftragter Annahme: Im Schnitt 1 Personentag pro Woche (~20% Pensum)	2'080.00	99'840.00
48	Tage	Reisepauschale	100.00	4'800.00
			Zwischentotal	**104'640.00**
			Rabatt 5% (ohne Reisepauschale)	- 4'992.00
			exkl. MWST	**99'648.00**
			inkl. MWST 8.1%	**107'719.50**

Finanzierung

Im Budget 2025 (Konto 1021.3130.00) sind Mittel in der Höhe von 108'000 Franken für die Umsetzung des Massnahmenplans eingestellt. Gemäss Art. 23 Abs. 2 Ziff. 3 Gemeindeordnung ist der Stadtrat für die Bewilligung von im Budget enthaltenen neuen einmaligen Ausgaben bis 325'000 Franken zuständig.

Erwägungen

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.

Vor diesem Hintergrund sind die aus dem Postulat "Sicherung kritischer Infrastruktur durch Cyber Security Audits" hervorgegangenen Risiken zu minimieren und im Rahmen des Massnahmenkatalogs umzusetzen.

Für richtigen Protokollauszug:

Stadtrat Wetzikon
Melanie Imfeld, Stadtschreiberin