wetzikon

Stadtrat

Auszug aus dem Protokoll Sitzung vom 13. November 2024

10 0.04.05.03 Postulat
Postulat "Sicherung kritischer Infrastruktur durch Cyber Security Audits", Bericht und Antrag (Parlamentsgeschäft 23.03.08)

Beschluss Stadtrat

1. Antrag und Bericht zum Postulat "Sicherung kritischer Infrastruktur durch Cyber Security Audits" werden genehmigt und dem Parlament zur Beschlussfassung unterbreitet.

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

3. Mitteilung durch Sekretariat an:
   – Parlamentsdienste (als Antrag und Bericht, mit Hinweis auf die Vertraulichkeit)
   – Mitglieder Geschäftsleitung
   – Abteilungsleiter Informatik
   – Abteilungsleiter Bevölkerung + Sicherheit
   – Kommandant Stadtpolizei Wetzikon
   – Abteilungsleiter Tiefbau
   – Bereichsleiter Stadtentwässerung /ARA

Erwägungen

Das Ressort Präsidiales, Entwicklung + Kultur unterbreitet dem Stadtrat den Antrag und den Bericht zum Postulat "Sicherung kritischer Infrastruktur durch Cyber Security Audits" zur Überweisung an das Parlament.

Antrag und Bericht an das Parlament

Parlamentsgeschäft 23.03.08

Antrag

Der Stadtrat beantragt dem Parlament, es möge folgenden Beschluss fassen:
(Zuständig im Stadtrat Pascal Bassu, Ressort Ressort Präsidiales, Entwicklung + Kultur)

Dem Bericht des Stadtrats wird zugestimmt und das Postulat "Sicherung kritischer Infrastruktur durch Cyber Security Audits" abgeschrieben.

Bericht

Ausgangslage

Das Parlament hat dem Stadtrat am 11. März 2024 das Postulat "Sicherung kritischer Infrastruktur durch Cyber Security Audits" zur Berichterstattung und Antragstellung überwiesen. 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. ob eine Massnahme zu treffen ist, die in die Zuständigkeit des Stadtrats fällt. Nach Art. 49 Abs. 1 GeschO Parlament hat der Stadtrat über ein überwiesenes Postulat innert neun Monaten Bericht zu erstatten und Antrag zu stellen. Mit dem vorliegenden Beschluss ist diese Frist gewahrt.

Der Stadtrat hatte demnach zu prüfen, ob das bestehende Sicherheitsdispositiv infolge zunehmender Digitalisierung kritischer Infrastruktur angepasst werden muss und welche Massnahmen zu ergreifen sind, um Cyberangriffe erfolgreich abwehren zu können.

Einleitung

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.

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.

Vorgehen und Umfang

Das Postulat fordert den Stadtrat auf, unverzüglich Massnahmen zu ergreifen und die kritischsten Infrastrukturen, insbesondere die Wasserversorgung und Stromversorgung, sowie andere lebenswichtige Dienste, regelmässigen, externen Cybersecurity Audits zu unterziehen. In Anlehnung an diese Forderung hat der Stadtrat entschieden, den Fokus auf folgende Organisationseinheiten und Infrastrukturen zu legen:

Stadtwerke	Versorgung Strom, Wasser, Gas
Stadtentwässerung	Abwasserreinigung ARA
Sicherheit	Blaulichtorganisationen Stadtpolizei und Feuerwehr Zivilschutz

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.

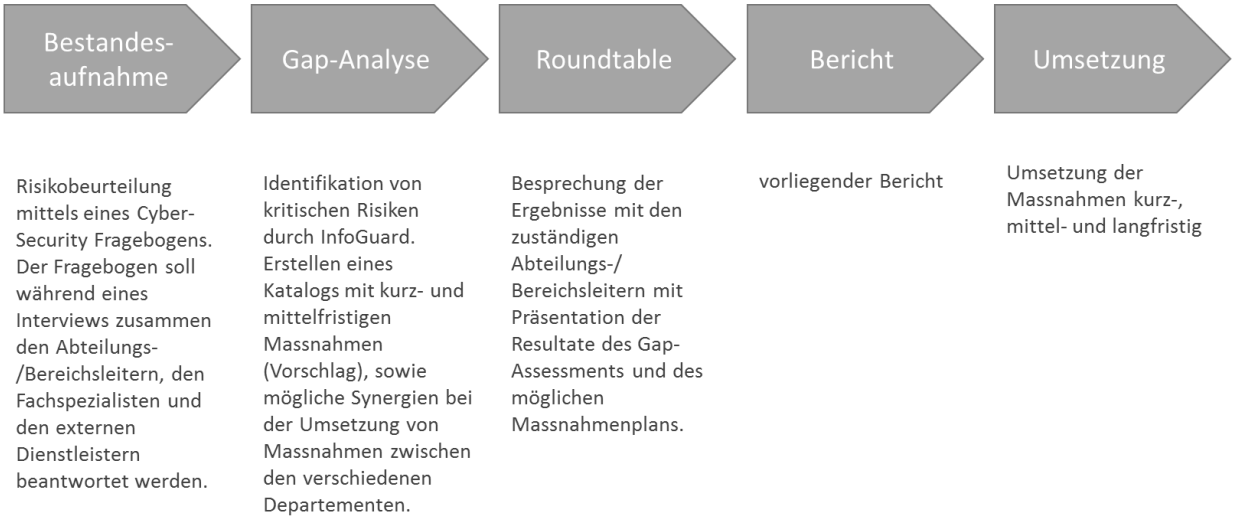
Um diesen ganzheitlichen Ansatz zu verfolgen, hat der Stadtrat die Firma InfoGuard AG, eine der führendenden Schweizer Firma für umfassende Cybersicherheit, mit der Erstanalyse beauftragt. Dieses Assessment erfolgte auf Basis des Cybersecurity Frameworks NIST, welches sich aus den folgenden Elementen zusammensetzt:

Abbildung 1: Cyber Security Framework NIST

1. Identifizieren (Identify)
2. Schützen (Protect)
3. Erkennen (Detect)
4. Reagieren (Respond)
5. Wiederherstellen (Recover)

- **Identifizieren**: Um sich vor Cyberangriffen zu schützen, muss das Cybersicherheits-Team genau wissen, was die wichtigsten Assets und Ressourcen des Unternehmens sind. Die Funktion "Identifizieren" umfasst Kategorien wie Asset-Management, wirtschaftliche Rahmenbedingungen, Governance, Risikobewertung, Risikomanagementstrategie und Risikomanagement in der Lieferkette.
- **Schützen**: Die Funktion "Schützen" deckt einen Grossteil der Kontrollmechanismen für technische und physische Sicherheit zum Entwickeln und Implementieren geeigneter Sicherheitsmassnahmen und zum Schützen der kritischen Infrastruktur ab. Zu diesen Kategorien gehören Identitätsmanagement und Zugriffssteuerung, Sensibilisierung und Schulung, Datensicherheit, Informationsschutzprozesse und -verfahren, Wartung und Schutztechnologie.
- **Erkennen**: Die Funktion "Erkennen" implementiert Massnahmen, um ein Unternehmen auf Cyberangriffe aufmerksam zu machen. Die Kategorien dieser Funktion schliessen Anomalien und Ereignisse, Sicherheit, die durchgehende Sicherheitsüberwachung und Erkennungsprozesse ein.
- **Reagieren**: Die Kategorien der Funktion "Reagieren" stellen die angemessene Reaktion auf Cyberangriffe und andere Cybersicherheits-Ereignisse sicher. Zu den spezifischen Kategorien gehören Reaktionsplanung, Kommunikation, Analyse, Risikominderung und Verbesserungen.
- **Wiederherstellen**: Die Aktivitäten für die Wiederherstellung implementieren Pläne für Cyberresilienz und stellen die Business-Continuity im Falle eines Cyberangriffs, einer Sicherheitsverletzung oder eines anderen Cybersicherheits-Ereignisses sicher. Zur Funktion "Wiederherstellen" gehören Verbesserungen bei der Planung der Wiederherstellung und die Datenübertragung.

InfoGuard führte das Security Assessment wie folgt durch:



Zur Erarbeitung der Bestandesaufnahme wurden die verantwortlichen Kader sowie verschiedene IT-Lieferanten zu Interviews eingeladen.

Ergebnisse und Massnahmen

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. Aus Sicherheitsgründen können die Ergebnisse und spezifischen Massnahmen nicht detailliert im Postulatsbericht offengelegt werden. Der vollständige Assessmentbericht wird jedoch den beiden Postulanten und der zuständigen Parlamentskommission (RPK) präsentiert.

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.

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.

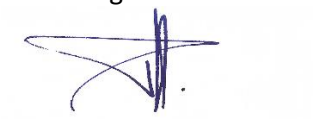
Mit der Umsetzung der aus dem Assessment definierten Massnahmen kann die Stadt, insbesondere ihre kritische Infrastruktur, besser vor Cyberrisiken geschützt werden und eine sichere Zukunft gewährleisten.

Glossar

Begriff	Beschreibung
NIST	National Institute of Standards and Technology, und stellt mit dem Cybersecurity Framework (CSF) eine Reihe von Richtlinien zur Abschwächung organisatorischer Cybersicherheitsrisiken bereit. Die 5 Hauptbereiche von CSF sind Govenrnance, Identify, Protect, Detect, Respond und Recover.
ISO27001/2	Die internationale Norm ISO/IEC 27001 Informationtechnology – Security techniques – Information security management systems – Requirements spezifiziert die Anforderungen für Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines dokumentierten Informationssicherheits-Managementsystems unter Berücksichtigung des Kontexts einer Organisation
Statement of Applicability (SoA)	Statement of Applicability (Anwendbarkeitserklärung, Dokumenten-Geltungsbereich), als Teil der ISO/IEC 27001, eines Information Security Management Systems (ISMS)
Third Party Risk Management (TPRM)	TPRM stellt sicher, dass Lieferanten, Service- und andere Dienstleister einer Organisation den Anforderungen für Informationssicherheit genügen.
Vulnerability Management	Vulnerability Management (auch Schwachstellen Management) bezeichnet den Prozess der Erkennung, Bewertung, Meldung und Behandlung von Sicherheitslücken in Computersystemen. Als Unterdomäne des IT-Risikomanagements ist es fundamental für Informations- sowie Netzwerksicherheit, Schwachstellen können mithilfe von Vulnerability Scannern aufgedeckt werden.
Patch Management	To patch; ist eine Korrekturauslieferung für Software oder Daten aus Endanwendersicht, um Fehler zu beheben, bekannt gewordene Sicherheitslücken zu schließen sowie bislang nicht vorhandene Funktionen nachzurüsten.
BCM/DR	Business Continuity Management stellt unterbrechungsfreie Geschäftsabläufe sicher und Desaster Recovery steht für das Notfallmanagement der IT und die Wiederherstellung der operativen IT Services und Infrastruktur.
Cyber Resilienz	Der Begriff "Cyber-Resilienz" bezieht sich auf die Fähigkeit eines Unternehmens, trotz Cyber-Angriffen kontinuierlich die beabsichtigten Ergebnisse zu erzielen. Die Resilienz gegenüber Cyber-Angriffen ist für IT-Systeme, kritische Infrastrukturen, Geschäftsprozesse, Organisationen und Gesellschaften von entscheidender Bedeu-

	tung.
Penetration-Test	Penetrationstest, kurz Pentest(ing), ist der fachsprachliche Ausdruck für einen umfassenden Sicherheitstest einzelner Rechner oder Netzwerke jeglicher Grösse. Ein Penetrationstest prüft die Sicherheit von Systembestandteilen und Anwendungen eines Netzwerks oder Softwaresystems mit Mitteln und Methoden, die tauglich sind, um unautorisiert in das System einzudringen (Penetration).
MFA	Die Multi-Faktor-Authentifizierung (MFA), auch Multifaktor-Authentisierung, ist eine Verallgemeinerung der Zwei-Faktor-Authentisierung, bei der die Zugangsberechtigung durch mehrere, unabhängige Merkmale (Faktoren) überprüft wird.
Security by Design	"Secure by Design" bedeutet in der Softwaretechnik, dass Softwareprodukte und -funktionen so entwickelt wurden, dass sie grundlegend sicher sind.
PLS / SPS	Ein Prozessleitsystem (PLS) dient zum Führen einer verfahrenstechnischen Anlage, zum Beispiel einer Kläranlage. Dazu gehören typischerweise auch sogenannte prozessnahe Komponenten wie SPS (eine speicherprogrammierbare Steuerung welche zur Steuerung oder Regelung einer Maschine oder Anlage eingesetzt werden und auf digitaler Basis programmiert sind).
OT	Operationelle Technologie (OT) ist Hard- und Software, die durch die direkte Überwachung und/oder Steuerung von industriellen Anlagen, Vermögenswerten, Prozessen und Ereignissen eine Veränderung feststellt oder herbeiführt.

Für richtigen Protokollauszug:



Stadtrat Wetzikon
Melanie Imfeld, Stadtschreiberin