wetzikon

Geschäftsleitung

Auszug aus dem Protokoll Sitzung vom 8. Mai 2025

2025/22 9.07.02.02 Infrastruktur
Ordnungsrahmen (Leitung, Überwachung und Organisation) für Informationssicherheit

Beschluss Geschäftsleitung

1. Die Geschäftsleitung stimmt dem Antrag a) "Variante Hybrid" und den daraus resultierenden Aktivitäten (b – d) zu, damit auf der Basis einer soliden Organisationsstruktur für Informationssicherheit der Massnahmenplan 2025 für die Stadt Wetzikon erfolgreich umgesetzt werden kann.

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

3. Mitteilung durch Sekretariat an:
   – Mitglieder der Geschäftsleitung
   – Bereichsleiter ARA
   – Bereichsleiter Stadtpolizei
   – Leitung Pflegezentrum Wildbach
   – Abteilungsleiter Informatik
   – Parlamentsdienste (zuhanden Parlament)

Ausgangslage

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. Aufgrund der gewachsenen Bedrohungslage hat der Stadtrat an seiner Sitzung vom 24. Januar 2024 das eingereichte Postulat "Sicherung kritischer Infrastruktur durch Cyber Security Audits" entgegengenommen.

Erkenntnisse und Massnahmen aus Bericht Postulat

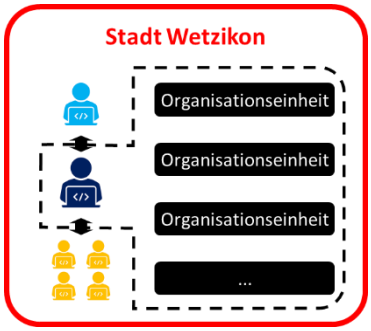
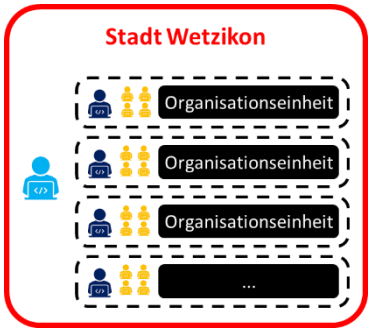
Im Rahmen des Postulats wurde in Zusammenarbeit mit InfoGuard AG ein Security Assessment mit Fokus auf die kritischen Infrastrukturen durchgeführt. Die im Assessment identifizierten Risiken wurden den Bereichen Governance, Risiko Management, Dienstleister (Third Party Risk Management, TPRM), Vulnerability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

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.

Aktuelle Situation der Organisations-Struktur und Geltungsbereich

Nach einer ersten Durchsicht der beiden Dokumente "**Leitlinie** – Informationssicherheit der Stadt Wetzikon" (2022) und "**Leitfaden** – Aufbau und Organisationsstruktur Informationssicherheit in der Stadtverwaltung Wetzikon" (2021) wurden Inkonsistenzen in Bezug auf die Aufbauorganisation für Informationssicherheit identifiziert. Die Leitlinie orientiert sich an einer zentral geführten Sicherheitsorganisation, der Leitfaden hingegen an einer dezentral geführten Organisation.

Die nachfolgenden Abbildungen zeigen die beiden unterschiedliche Organisationsformen in Modellsicht, welche korrigiert werden sollten.

#	Aktuelle Definition	Beschreibung
1	*Leitlinie - Zentral* 	Die beiden dargestellten Organisationsformen repräsentieren die Ansätze, wie sie in der Leitlinie und im Leitfaden beschrieben sind. Die in den Abbildungen dargestellten "Organisationseinheiten" entsprechen den Bereichen, wie sie im Leitfaden unter Artikel 11 aufgeführt sind. Der zentrale Ansatz wird heute nicht gelebt, primär ist der dezentrale Ansatz in der Stadt Wetzikon verbreitet. Die Bereiche (Stadtverwaltung, Pflegezentrum Wildbach, ARA, Stadtwerke, Stadtpolizei) bearbeiten das Thema Informationssicherheit eigenständig, jedoch auf unterschiedlichen Maturitätsstufen, wie aus dem Security-Assessment hervorgegangen ist. Auch finden keine Erfahrungsaustausche oder Koordinationen von Aktivtäten zwischen den Bereichen statt. Abgrenzungen: Stadtpolizei: Vorbereitende Gespräche haben gezeigt, dass die Stadtpolizei ihre IT-Services über die Kantonspolizei Zürich bezieht. Die Informationssicherheit muss deshalb auf kantonaler Ebene gewährleistet werden. Schule: Der pädagogische Teil der Schule untersteht der Geschäftsordnung der Schule Wetzikon und fällt damit in den Aufgaben- und Kompetenzbereich der Schulpflege.
2	*Leitfaden – Dezentral* 	

Rollen

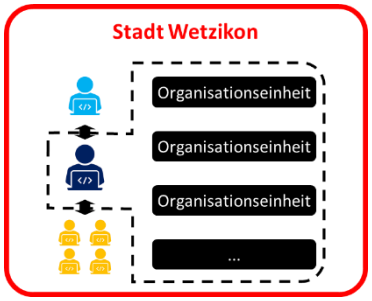
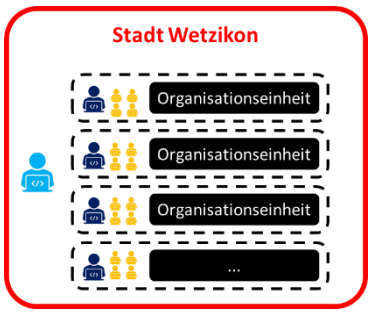
	Informationssicherheit-Verantwortliche / Informationssicherheit-Verantwortlicher Gemäss Leitlinie verantwortlich für die Umsetzung der Informationssicherheitsziele und Überwachung der Einhaltung des angestrebten Sicherheitsniveaus für die ganze Stadt Wetzikon. Allerdings wird im Leitfaden den einzelnen Bereichen (Stadtverwaltung, Pflegezentrum Wildbach, ARA, Stadtwerke, Stadtpolizei) diese Verantwortlichkeit einer bestehenden Rolle zugeordnet.

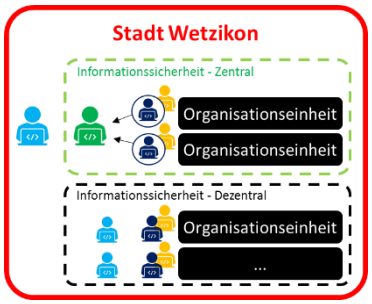
	Anwendungs- und Datenverantwortliche Gemäss Leitlinie verantwortlich für die Bestimmung des jeweiligen Schutzbedarf (Klassifizierung) bestimmt und die Vergabe von Zugriffsberechtigungen von Daten, Anwendungen, IT- und Netzwerksystemen.
	Datenschutzberaterin / Datenschutzberater Gemäss Leitlinie verantwortlich für Umsetzung des Datenschutzes und arbeitet eng mit den Informationssicherheitsverantwortlichen zusammen.

Die Wahl der Organisations-Struktur beantwortet zu weiten Teilen auch die Frage zum Geltungsbereich der Rollen, welche für die Sicherstellung der Informationssicherheit verantwortlich oder involviert sind.

Varianten

Im Fokus der Aufbauorganisation stehen entweder ein zentraler Ansatz für die ganze Stadt (wie in der Leitlinie stipuliert) oder ein dezentraler Ansatz (wie z.T. im Leitfaden aufgeführt). Dies gilt es nun zu bereinigen, damit die für die Informationssicherheit notwendigen Rollen und Verantwortlichkeiten in der Stadt Wetzikon geschärft werden können.

#	Variante	Beschreibung
1	*Zentral* 	Der zentrale Ansatz hat zum Ziel, dass das Thema Informationssicherheit von einer Stelle und übergeordnet für die ganze Stadt betreut und bearbeitet wird. So wird ein einheitlicher, strukturierter und konsistenter Prozess sichergestellt. Für eine Organisation und deren Führung ist dies normalerweise der beste Ansatz, um die Leitung und Überwachung über ein Thema zu haben.
2	*Dezentral* 	Beim dezentralen Ansatz sind die jeweiligen Organisationseinheiten für ein eigenes Informationssicherheit-Rahmenwerk und den Prozess verantwortlich. Falls eine Koordination zwischen den einzelnen Einheiten vorgesehen wäre, würde dies unter Umständen Mehrfachaufwände mindern.

#	Variante	Beschreibung
3	*Hybrid* 	Aufgrund der unterschiedlichen Bedürfnisse und Anforderungen kann auch eine gemischte Form der beiden Varianten 1 und 2 in Betracht gezogen werden. Der CISO nimmt eine zentrale Verantwortung für die Mehrzahl der Organisationseinheiten wahr und stellt die Koordination (Roundtable) dieser sicher. Begründete Ausnahmen verbleiben in einer dezentralen Struktur.

Rollen

	**CISO – Chief Information Security Officer** Diese neu geschaffene Funktion ist analog der Rollenbeschreibung für Informationssicherheit-Verantwortliche/r die zentrale Stelle für die Umsetzung der Informationssicherheitsziele und Überwachung der Einhaltung des angestrebten Sicherheitsniveaus.
	**Informationssicherheit-Verantwortliche/r** In der Summe ist die Rolle Informationssicherheit-Verantwortliche/r die Kombination von CISO und ISO und für alle Sicherheitsbelange in einem Bereich verantwortlich.
	**ISO – Information Security Officer** Ist die Schnittstelle zwischen dem CISO und den Organisationsbereichen und unterstützt diese in der Umsetzung der Informationssicherheitsziele und Überwachung der Einhaltung des angestrebten Sicherheitsniveaus. Der ISO unterscheidet sich insofern von der Rolle Informationssicherheit-Verantwortliche/r, als dies eine ergänzende Rolle zum CISO ist und nicht alle Aufgaben und Verantwortlichkeiten des/der Informationssicherheit-Verantwortliche/r inne hat.
	**Anwendungs- und Datenverantwortliche/r** Beschreibung siehe weiter oben.
	**Datenschutzberater/in** Beschreibung siehe weiter oben.

Bewertung der Varianten

#	Variante	Bewertung	
		Positiv	**Negativ**
1	*Zentral*	• Ein übergeordnetes und einheitliches Framework für Informationssicherheit, welches den Sicherheitsanforderungen der jeweiligen Bereiche den geforderten Maturitätslevel ermöglicht. • Zentrale Koordination, Expertise und Berichterstattung erlauben Transparenz und eine umfassendere Auskunftsbereitschaft. • Kosteneffizienter	• Operativ schwerfälliger, da längere Entscheidungswege und aufwändigere Kommunikation. • Überschreitung von Kompetenzgrenzen
2	*Dezentral*	• Operativ schneller und dynamischer, da kürzere Entscheidungswege. • Einhaltung vorhandener Kompetenzgrenzen	• Unterschiedliche Ansätze das Management von Informationssicherheit, welche zu Mehrfachaufwänden führt. • Mehrfache Berichterstattung, was bei Themen wie Risiko-Management nachteilig ist. • Keine Koordination zwischen den Bereichen • Höhere Kosten
3	*Hybrid*	• Siehe Argumente für # 1 und 2 • **Berücksichtigung der Kompetenzgrenze zu Stadtpolizei und Schule**	

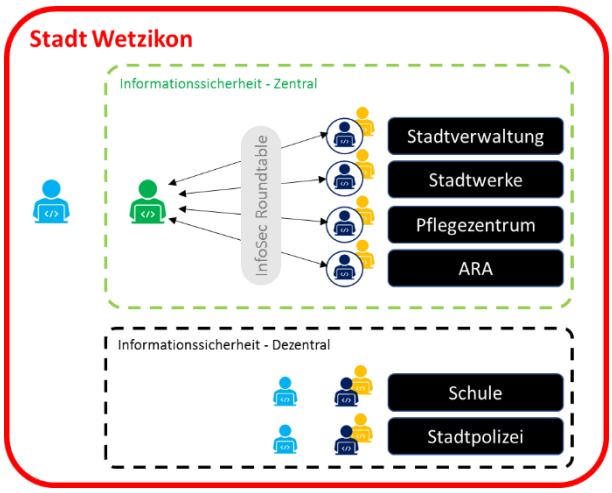
Leitung und Überwachung (Governance)

In Vorfeld wurde auch das Thema Positionierung des CISO sowie die Berichterstattung besprochen:

- Die Funktion CISO ist bis auf weiteres dem IT-Verantwortlichen R. Hölzlberger unterstellt.
- Vierteljährliche Berichterstattung durch den CISO erfolgt an die Geschäftsleitung.
- Je nach Entscheid der Organisationsform, würde für die Varianten 1 (Zentral) oder 3 (Hybrid) ein regelmässiges Info-Sec Roundtable mit den Delegierten (ISOs) der verschiedenen Bereichen / Fachabteilungen eingeführt werden.

Antrag

a) Aufbauorganisation für Informationssicherheit



Aufgrund der aktuellen Gegebenheiten und Rahmenbedingungen bietet sich die Variante "Hybrid" an, welche einen zentralen Ansatz für die Mehrheit der Bereiche verfolgt, wie die Übersicht links zeigt.

Um den Anforderungen der eigenständig agierenden Bereiche wie die Polizei oder die Schule gerecht zu werden, soll die vorgeschlagene Lösung auch den dezentralen Aspekt unterstützten.

Die Abgrenzung begründet sich für die Stadtpolizei Wetzikon dadurch, dass die IT-Lösung von der Kantonspolizei Zürich gestellt ist und von Abraxas Informatik AG betrieben wird. Die Verantwortung für die Informationssicherheit muss somit auf kantonaler Ebene sichergestellt werden.

Die Schule (Bildung / Pädagogik) untersteht der Schulpflege mit entsprechender Entscheidungsgewalt und stellt die Informationssicherheit dezentral sicher.

b) *Aktualisieren der Leitlinie zur Informationssicherheit der Stadt Wetzikon*
Die unter a) vorgeschlagene Änderung bedingt eine Anpassung der Leitlinie. Gleichzeitig soll die Leitlinie auch auf die aktuellen Gegebenheiten und guten Praktiken in Bezug auf Informationssicherheit überprüft und ggf. angepasst werden.

I. Aktualisierung durch den CISO
II. Genehmigung der neuen Version der Leitlinie durch den Stadtrat

c) Aktualisieren und Harmonisieren des Leitfadens Aufbau und Organisationsstruktur Informationssicherheit in der Stadtverwaltung Wetzikon
Ableitend von der neuen Version der Leitlinie soll der Leitfaden für die Stadtverwaltung überprüft und angepasst werden. Falls weitere, ähnliche Leitfäden in den Bereichen vorhanden sind, sollen diese entweder im Leitfaden der Stadtverwaltung integriert oder mit diesem harmonisiert werden.

III. Aktualisierung und Harmonisierung wird durch den CISO koordiniert unter Mithilfe der Bereichs-ISOs.
IV. Genehmigung der neuen Version des Leitfadens durch die Geschäftsleitung

Empfehlung
Änderung des Dokumententitel zu "*Leitfaden Aufbau und Organisationsstruktur Informationssicherheit der Stadt Wetzikon,* um den Geltungsbereich **Informationssicherheit – Zentral** der Variante Hybrid abzubilden.

d) Leitung und Überwachung (Governance)

Etablieren von:

I. Vierteljährlicher Berichterstattung durch den CISO an die Geschäftsleitung

II. Durchführen eines regelmässigen Info-Sec Roundtable mit den Delegierten (ISOs) der verschiedenen Bereiche / Fachabteilungen.

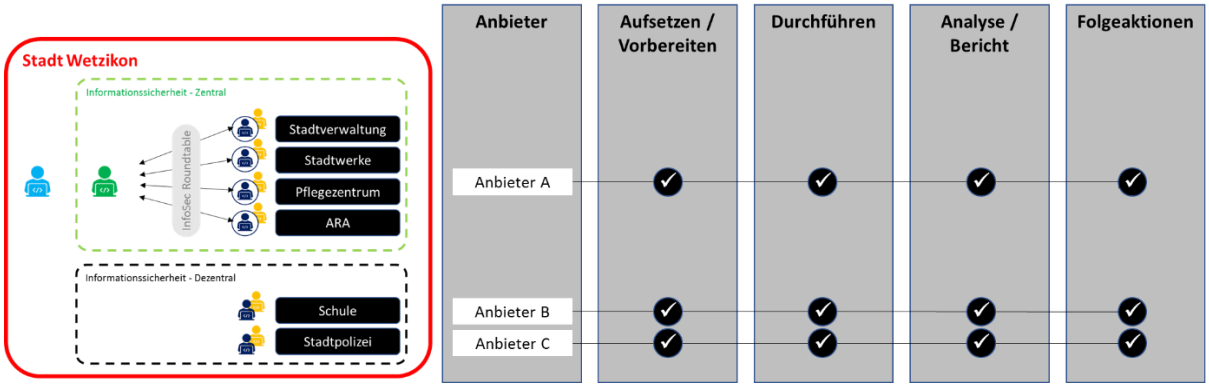
Erwägungen

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. Die durchgeführte Sicherheitsbeurteilung im Jahre 2024, der aus den Ergebnissen erstellte Massnahmenplan sowie das Engagement eines externen CISOs sind wichtige Voraussetzung für eine erfolgreiche Neuausrichtung und Organisationsanpassung der Informationssicherheit.

Anhang - Beispiel mit Phishing-Kampagnen

Das folgende Beispiel soll aufzeigen, wie sich die Aufwände bei dem Beispiel Phishing-Kampagnen manifestieren.

Die Illustration zeigt den Ablauf in Folge von Aktivitäten einer Phishing-Kampagne, wie dies normalerweise Firmen im Angebot haben.



ANBIETER	• **Skaleneffekt für Lizenzen** geht mit mehreren Anbietern verloren • Unterschiedliche Ansätze, Inhalte und Qualität der Kampagnen
AUFSETZEN / VORBEREITEN **DURCHFÜHREN**	• Mehrfachaufwände
ANALYSE / BERICHT	• Unterschiedliche Inhalte und Qualität der Berichte • **Konsolidieren eines einheitlichen Berichts** für die ganze Stadt ist schwierig und aufwändig.
FOLGEAKTIONEN	• Mehrfachaufwände

Für richtigen Protokollauszug:

Geschäftsleitung Wetzikon
Nives Lis-Ventura, Assistentin Stadtschreiberin