Protokollauszug vom 14.08.2019

Departement Finanzen / Informatikdienste:
Projekt-Nr. 19583 Identity und Access Management (IAM): Gebundenerklärung und Ausgabenfreigabe von 1 905 000 Franken
IDG-Status: öffentlich
SR.19.557-1

Der Stadtrat hat beschlossen:

1. Die Aufwendungen für die Erneuerung des Identity- und Access-Management-Systems (IAM) im Betrag von 1 905 000 Franken werden gestützt auf § 5 Gemeindeverordnung und § 7 Gesetz über die Information und den Datenschutz als gebundene Ausgaben im Sinne von § 103 Abs. 1 Gemeindegesetz bezeichnet und zu Lasten der Investitionsrechnung des Verwaltungsvermögens, Projekt-Nr. 19583, freigegeben.

2. Mitteilung an: Departement Finanzen, Informatikdienste, Finanzamt, Investitionsstelle; Finanzkontrolle.

Vor dem Stadtrat
Der Stadtschreiber:

A. Simon

Begründung:

1. Einleitung

Unter einem Identity- und Access-Management-System (IAM) wird ein Identitäts- und Berechtigungsverwaltungs-System verstanden. Damit werden alle internen und externen IT-Benutzer und Benutzerinnen und deren Zugriffsrechte auf IT-Anwendungen verwaltet. Die Anforderungen an ein solches System sind in den letzten Jahren stark gestiegen und werden mit der zunehmenden Digitalisierung weiter steigen.

Das bestehende Identitäts- und Berechtigungsverwaltungs-System (IAM) ist veraltet und muss daher dringend erneuert werden. Ein erneuertes IAM hat den gesetzlichen Anforderungen zu entsprechen sowie den Bedürfnissen der Nutzerinnen und Nutzern und der internen Stellen, welche die entsprechenden Dienstleistungen anbieten, gerecht zu werden.

2. Projekt

Mit Bezug auf die Kontrolle dieser Zugriffsrechte auf Applikationen und Daten bestehen seitens der Finanzkontrolle klare Vorstellungen. Die Finanzkontrolle empfiehlt die Vorgaben von Standards, wie die Vergabe und Bewirtschaftung der Zugriffsrechte erfolgen soll sowie eine institutionalisierte und zentralisierte Kontrolle dieser Rechte.

Die bis anhin geltende Praxis, wonach bei speziellen bzw. dezentralen Fachanwendungen die Verantwortung für die Benutzung und die Verwaltung der dazugehörigen Rechte bei den Fachbereichen liegt, hat sich nicht bewährt und erfüllt die erwähnten Anforderungen der Finanzkontrolle nicht. So besteht bei Austritten oder Übertritten von Mitarbeitenden heute keine Gewähr, dass die bestehenden Zugriffsrechte entzogen werden. Das erneuerte IAM beseitigt diese Schwachstellen, indem in Zukunft die Prozesse für die Prüfung aller Zugriffsrechte zentral geführt und mit einer periodischen Kontrolle durch die Vorgesetzten und die Applikationsverantwortlichen unterstützt werden. Mit einem neuen IAM wird die Qualität hinsichtlich der Zugriffsrechte stark verbessert. Dies geschieht, indem mit einer nachweisbaren Kontrolle gewährleistet wird, welche internen und externen Nutzerinnen und Nutzer Zugriff auf Anwendungen und Daten haben.

Im Weiteren gilt es zu beachten, dass in Zukunft die Digitalisierung und damit die Interaktion zwischen der Stadt Winterthur sowie externen Nutzerinnen und Nutzern zunehmen wird. Es ist davon auszugehen, dass in den nächsten fünf Jahren mehr als 10 000 externe Nutzerinnen und Nutzer Dienstleistungen der Stadtverwaltung in elektronischer Form beziehen werden und dadurch einen Zugang zu ihren Anwendungen benötigen. Damit verbunden ist eine Vervielfachung der zu verwaltenden Benutzerinnen und Benutzer und deren Zugriffsrechte, wobei strenge Qualitätsanforderungen zu berücksichtigen sind. Hinzu kommt auch die stete Anpassung an neue Technologien. Beide Faktoren stellen hohe Anforderungen an die Informatikdienste (IDW). Die zahlreichen manuellen Schritte, die im heutigen IAM vorzunehmen sind, können diesen quantitativen und qualitativen Anforderungen nicht mehr gerecht werden. Hinzu kommt, dass das Know-how im Umgang mit dem derzeitigen IAM auf wenige Personen bei der IDW beschränkt ist und infolge altersbedingter Abgängen kontinuierlich verloren geht.

Im Zusammenhang mit der künftigen Nutzung der elektronischen Dienstleistungen der Stadt Winterthur stellt ein zentrales Bürgerlogin, mit dem sich Einwohnerinnen und Einwohner registrieren können und damit Zugang zu Informationen erhalten, eine wichtige und zentrale Infrastruktur dar. Mit der Weiterentwicklung von E-Government und Smart City besteht das dringende Bedürfnis, ein einheitliches und zeitgemässes Autorisierungssystem für sämtliche bestehenden und künftigen städtischen Online-Services anzubieten. Dies erfolgt künftig über einen einheitlichen zentralen Zugang, den Dienst «Mein Konto». Der Stadtrat hat diesem Projekt mit Beschluss vom 10. April 2019 zugestimmt und die entsprechenden Kosten als gebunden erklärt (SR.19.234-1). Mit einem erneuerten IAM kann dieser Dienst für die Benutzerregistrierung und den Login von weiteren Anwendungen genutzt werden. Damit können Kosten gespart werden, indem auf den Aufbau individueller Lösungen für jeden einzelnen Fachbereich verzichtet werden kann.

Als weiterer Faktor kommt hinzu, dass IT-Infrastrukturen und IT-Dienstleistungen zunehmend standardisiert aus dem Internet bezogen werden (Cloud-Computing). So verwendet auch die Stadt Winterthur aufgrund der wirtschaftlichen Vorteile bereits heute und in Zukunft noch vermehrt entsprechende Ressourcen und Dienste. Dem Datenschutz und der Zugriffskontrolle kommen beim Einsatz von Cloud-basierten Infrastrukturen eine erhöhte Bedeutung zu. Das erneuerte IAM soll einen wesentlichen Beitrag zu einer zentralen Zugangssteuerung und zu einer verbesserten Kontrolle von Cloud-basierten Services leisten.

Beim IAM handelt es sich um ein Verwaltungssystem für Identitäten und Rechte und nicht um das eigentliche Berechtigungssystem (dazu zählen Anwendungen, Internet Portale oder Zugriffsinfrastrukturen). Die Zugriffsrechte werden vom IAM an die entsprechenden Berechtigungssysteme verteilt. Als Verwaltungssystem bearbeitet das IAM Identitäts- und Zugriffs-Anträge, Bewilligungsprozesse, Mutationsmeldungen (Austritte und Funktionswechsel), regelmässige Überprüfung der Rechte und Identitäten sowie deren Löschung. Das erneuerte IAM integriert sich in bereits bestehende Berechtigungssysteme, unter anderem auch in die Lösung, welche im Rahmen des Projektes «Mein Konto» für den Zugriff von externen Nutzerinnen und Nutzern auf Portale und Anwendungen in der Stadtverwaltung aufgebaut wird.

Ursprünglich wurde davon ausgegangen, dass mit der Erneuerung des IAM im 2013 gestartet wird. Der entsprechende Projektierungskredit in der Höhe von 250 000 Franken wurde vom GGR mit dem Budget 2013 zulasten Projekt-Nr. 19341 (Rollenbasierendes Zugriffsmanagement IAM) bewilligt. Für eine Vorstudie sowie die Unterstützung bei der Submission wurde der konstitutiv bewilligte Betrag von der Departementsvorsteherin Finanzen im November 2017 freigegeben (DFI.17.296-1).

Aufgrund personeller Engpässe und Sparprogrammen, die sich sowohl auf die Ressourcen als auch auf die Prioritäten auswirkten, verzögerte sich das Vorhaben. Der operative Betrieb des bestehenden IAM konnte nur dank eines erhöhten Personaleinsatzes aufrechterhalten werden. Dieser Einsatz lässt sich jedoch in Zukunft aufgrund der bereits erwähnten Gründe, vor allem wegen der Vervierfachung der Benutzerzahlen durch die Bürger-Logins, nicht mehr weiterführen, weshalb die Erneuerung des IAM keinen weiteren Aufschub erträgt und jetzt dringend umzusetzen ist.

Einordnung des Projekts IAM:

Projekt-Nr. 19341: Rollenbasierendes Zugriffsmanagement IAM

Projektierungskredit für eine Vorstudie IAM.

Projekt 19782: Mein Konto

Schaffung der konzeptionellen und technischen Grundlagen für den Dienst «Mein Konto».

Projekt 19674: Migration nicht mehr unterstützter Plattformen

Konsolidierung von bestehenden Authentifizierungsprozessen für den zentralen Zugang über «Mein Konto» mit dem Ziel, Mitarbeitenden der Verwaltung ohne IT-Account Zugriff auf das Intranet und der Kundschaft von Stadtwerk Zugriff auf das Kundenportal zu ermöglichen. Damit verbunden ist auch die Migration von bestehenden Plattformen auf den neuen Login.

Projekt-Nr. 19583: Identity und Access Management (IAM)

Das umfassende Management der Identitäten und Zugriffsrechte ist Gegenstand des vorliegenden Projekts «Identity und Access Management, IAM». Dieses setzt sich aus den folgenden Komponenten zusammen:

Basissystem internes IAM:

Das Basissystem löst das bestehende IAM ab. Die heute vorhandenen Identitäten und Zugriffsrechte werden vom alten System integral auf das neue System migriert. Die im alten System erforderlichen manuellen Interaktionen werden soweit möglich eliminiert und damit die bis anhin notwendigen, personellen Ressourcen stark entlastet.

Externes IAM:

Mit dem externen IAM werden die erweiterten Anforderungen an das IAM erfüllt. Diese umfassen den externen Zugriff auf städtische Anwendungen von städtische Mitarbeitende ohne IT-Account, von Kundinnen und Kunden von Stadtwerk sowie von weiteren Einwohnerinnen und Einwohnern.

Aufbau Rollenkonzept und Self-Servicing:

Das Optimum des IAM wird mit dem Bereitstellen eines Self-Servicing erreicht. Dabei können die Antragstellenden ihre Rechte im IAM selber bestellen, und nach dem Durchlaufen der notwendigen Prüfungen werden die gewünschten Rechte direkt erteilt. Um dieses Ziel zu erreichen, müssen die heute bestehenden ca. 6000 Rechte in für die Antragstellenden verständliche Rollen umgewandelt werden.

3. Kosten

3.1. Kostenzusammenstellung

Die Kostenzusammenstellung basiert auf einer Grobkostenschätzung der IDW:

Bezeichnung	**Fr.**	**Betrag**
Lizenzen für Software internes und externes IAM	Fr.	500 000.00
Migration des bestehenden IAM	Fr.	455 000.00
Aufbau des externen IAM	Fr.	475 000.00
Aufbau Rollenkonzept mit Self-Servicing	Fr.	475 000.00
Total Gebundenerklärung	**Fr.**	**1 905 000.00**

3.2. Investitionsplanung

Das Vorhaben ist wie folgt im Investitionsprogramm des allgemeinen Verwaltungsvermögens eingestellt:

Projekt-Nr.	19583
Projektbezeichnung	IAM (Rollenbasierendes Zugriffsmanagement)

Kostenart	**Bezeichnung**		**Betrag**
520000	Software		1 905 000.00
Gesamtbetrag		**#**	**1 905 000.00**

Planung	**Kostenart 520000**	**Gesamtbetrag**
2019	955 000	955 000
2020	950 000	950 000

Die Investitionsplanung wurde mit dem Budget 2020 wie folgt angepasst:

Kostenart	**Gebundenerklärung**		**Betrag**
520000	Software		1 905 000.00
Gesamtbetrag		**§**	**1 905 000.00**

Planung	Kostenart 520000	Gesamtbetrag
2019	505 000.00	505 000.00
2020	1 400 000.00	1 400 000.00

4. Gebundenerklärung der Ausgaben

4.1. Rechtsgrundlagen

Gebundene Ausgaben der Investitionsrechnung sind vom Stadtrat zu bewilligen (Art. 57 Abs. 1 Vollzugsverordnung über den Finanzhaushalt der Stadt Winterthur).

Gemäss § 103 Abs. 1 Gemeindegesetz (GG) gelten Ausgaben als gebunden, wenn die Gemeinde durch einen Rechtssatz, durch einen Entscheid eines Gerichtes oder einer Aufsichtsbehörde oder durch einen früheren Beschluss der zuständigen Organe oder Behörden zu ihrer Vornahme verpflichtet ist und ihr sachlich, zeitlich und örtlich kein erheblicher Ermessensspielraum bleibt.

4.2. Vorgabe durch übergeordnetes Recht

Ausgaben gelten nach Lehre und Rechtsprechung als gebunden, wenn sie zur Erfüllung der gesetzlich geordneten Verwaltungsaufgaben unbedingt erforderlich sind (Kommentar zum Zürcher Gemeindegesetz, 2017, T. Jaag, M. Rüssli, V. Jenni, N. 3 zu § 103 GG). Informatikleistungen gelten als unverzichtbare Mittel zur Erfüllung der Verwaltungsaufgaben, weshalb die damit verbundenen Ausgaben dann als gebunden zu betrachten sind, wenn im konkreten Fall kein erheblicher Ermessensspielraum gegeben ist (Kommentar, N. 3 und 21 zu § 103 GG).

Im Übrigen ist die Gemeinde gemäss § 5 Gemeindeverordnung (VGG) verpflichtet, ihre Sachwerte laufend so zu unterhalten, dass ihre Substanz erhalten bleibt, die Gebrauchsfähigkeit und Funktionstüchtigkeit gewährleistet ist und keine Personen-, Sach-, oder Bauschäden auftreten. Zur Unterhaltspflicht nach § 5 VGG zählen auch Anpassungen an den zeitgemässen Komfort und an den Stand der Technik sowie die Erfüllung von gesetzlichen Auflagen und Vorschriften.

Die Vorschriften des Gesetzes über die Information und den Datenschutz (IDG) gebieten die Nachvollziehbarkeit von Zugriffen und die Gewährleistung des Datenschutzes im Internet durch organisatorische und technische Massnahmen (§ 7 IDG). Es muss überprüft werden können, ob die Benutzenden berechtigt sind und welche Funktionen sie ausüben dürfen, resp. für welche Applikationen sie eine Berechtigung haben.

4.3. Örtliche, sachliche und zeitliche Gebundenheit

In sachlicher Hinsicht darf sich der Handlungsspielraum nicht auf wichtige Elemente des Ausgabenbeschlusses beziehen. Die sachliche Gebundenheit ist gegeben, wenn sich die Entscheidungsfreiheit auf technische Details beschränkt (Kommentar zum Gemeindegesetz, N. 23 zu § 103 GG). In zeitlicher Hinsicht genügt es, wenn sich der vorgesehene Zeitpunkt sachlich rechtfertigen lässt (Kommentar zum Gemeindegesetz, N. 25 zu § 103 GG).

Örtliche Gebundenheit:
Diesbezüglich besteht bei der Beschaffung von Informatikmitteln und IT-Dienstleitungen kein Handlungsspielraum.

Sachliche Gebundenheit:
Aus den vorstehenden Ausführungen geht hervor, dass das bestehende IAM in verschiedener Hinsicht den heutigen Anforderungen an eine sichere Identitäts- und Berechtigungsverwaltung nicht mehr zu genügen vermag. Insbesondere fehlt heute eine zentralisierte Verwaltung und Kontrolle der Zugriffsrechte. Im Zusammenhang mit der Einrichtung des zentralen Bürgerlogins «Mein Konto» sowie im Hinblick auf weitere Online-Services der Stadt und eines gesicherten Zugriffs auf Cloud-basierte Dienste ist eine Anpassung des IAM gestützt auf die Vorschriften des IDG

unabdingbar. Die Erneuerung des IAM ist geeignet, die Verwaltung der Identität und der Zugriffsrechte aller IT-Benutzerinnen und Benutzer auf dem aktuellen und gebräuchlichen Stand der Technik sicherzustellen. Der sachliche Entscheidungsspielraum beschränkt sich auf die Wahl des Systems und ist somit rein technischer Natur.

Zeitliche Gebundenheit:
Die Erneuerung des bestehenden IAM musste insbesondere aus personellen sowie finanziellen Gründen aufgeschoben werden. Eine weitere Verzögerung ist nicht mehr zu vertreten, weshalb die Erneuerung jetzt umzusetzen ist.

4.4. Gebundenerklärung und Ausgabenfreigabe

Aufgrund der vorstehenden Ausführungen steht fest, dass die Voraussetzungen von § 103 Abs. 1 GG erfüllt sind. Die entsprechenden Ausgaben sind deshalb für gebunden zu erklären und zu Lasten der Investitionsrechnung des allgemeinen Verwaltungsvermögens, Projekt-Nr. 19583, freizugeben.

5. Weiteres Vorgehen

Nach Bewilligung der gebundenen Ausgaben und der Ausgabenfreigabe durch den Stadtrat sind folgende Schritte geplant:

- 2019: Submission IAM, Vergabeentscheid Stadtrat
- 2019: Projektstart, Aufbau des Basissystems
- 2020: Migration des bestehenden IAM auf die neue Plattform
- 2020: Aufbau externes IAM
- 2020: Rollenkonzept mit Self-Servicing
- 2021: Projekt Abschluss

6. Kommunikation

Es ist keine Medienmitteilung erforderlich.

Da der Kredit als neue Ausgabe mit Sperrvermerk im Budget eingestellt worden ist, wird das DFI die zuständige Aufsichtskommission über die Gebundenerklärung informieren.