STADTRECHNUNGSHOF WIEN
Landesgerichtsstraße 10
A-1082 Wien

Tel.: 01 4000 82829 FAX: 01 4000 99 82810
E-Mail: post@stadtrechnungshof.wien.at
www.stadtrechnungshof.wien.at

StRH I - 13/17

MA 56, Maßnahmenbekanntgabe zu

MA 56, Prüfung des

Schulverwaltungsprogramms "WiSion"

INHALTSVERZEICHNIS

ABKÜRZUNGSVERZEICHNIS

bzw.	beziehungsweise
CR	Change Request
EDV	Elektronische Datenverarbeitung
etc.	et cetera
IKS	Internes Kontrollsystem
IKT	Informations- und Kommunikationstechnologie

Nr. ..... Nummer
u.a. ..... unter anderem
WiSion ..... Wiener Schulinformationssystem Online
z.B. ..... zum Beispiel

Erledigung des Prüfungsberichtes

Der Stadtrechnungshof Wien unterzog in einem ersten Schritt das von der Magistratsabteilung 56 betriebene Schulverwaltungsprogramm "WiSion" einer Prüfung. Der diesbezügliche Bericht des Stadtrechnungshofes Wien wurde am 4. Dezember 2018 veröffentlicht und im Rahmen der Sitzung des Stadtrechnungshofausschusses vom 11. Dezember 2018, Ausschusszahl 110/18 mit Beschluss zur Kenntnis genommen.

Kurzfassung des Prüfungsberichtes

Im Rahmen der gegenständlichen Prüfung wurde die operative Anwendung und technische Betriebsführung des Schulverwaltungsprogramms "Wiener Schulinformationssystem online" - kurz "WiSion", das seit der Inbetriebnahme im Jahr 2012 an allen allgemein bildenden öffentlichen Pflichtschulen in Wien eingesetzt wurde, einer Prüfung unterzogen. Der Fokus lag dabei auf der Rollen- und Berechtigungsverwaltung, der damit in Zusammenhang stehenden Tokenverwaltung und dem Prozess der Zeugniserstellung.

In Bezug auf die Rollen- und Berechtigungsverwaltung wurde unter anderem angeregt, die Möglichkeiten von Audit-Berechtigungen bzw. Audit-Rollen für revisionierende Einrichtungen zu evaluieren. Ferner zeigte sich Verbesserungspotenzial hinsichtlich der Nachvollziehbarkeit der manuellen Anlage und Löschung von Benutzendenkonten, der Tätigkeiten der Rolle "Administrator" im System sowie der Standardisierung und Evaluierung der Rollen- und Rechtepakete.

Hinsichtlich der Tokenverwaltung wurde empfohlen, eine Übereinstimmung der Daten des Schulverwaltungsprogramms "WiSion" mit dem angebundenen Informationssystem der Tokenverwaltung der Stadt Wien sicherzustellen. Ferner wären Maßnahmen zu treffen, um die Nachvollziehbarkeit von Verlusten bzw. Diebstählen von Token sowie deren etwaige Wiederbeschaffung zu gewährleisten.

Der Prozess der Zeugniserstellung war nicht vollständig durch aufgezeichnete Daten im Schulinformationssystem "WiSion" nachvollziehbar, weshalb empfohlen wurde die

Nachvollziehbarkeit durch ein entsprechendes, automatisiertes Logging der entsprechenden Daten (Prozessdaten) sicherzustellen.

Der Magistratsabteilung 01 war aufgrund der Verantwortung der Betriebsführung (Informations- und Kommunikationstechnologie Service Provider) des Schulinformationssystems "WiSion" Kontroll- und Unterstützungsleistungen für die Umsetzung der Empfehlungen durch die Magistratsabteilung 56 anzuraten. Ferner sollte sie die Prozessdaten der Zeugniserstellung des Schulinformationssystems "WiSion" im Rahmen der Data Excellence der Stadt Wien bereitstellen.

Bericht der Magistratsabteilung 56 zum Stand der Umsetzung der Empfehlungen

Im Rahmen der Äußerung der geprüften Stelle wurde folgender Umsetzungsstand in Bezug auf die ergangenen 13 Empfehlungen bekannt gegeben:

Stand der Umsetzung der Empfehlungen	Anzahl	Anteil in %
Umgesetzt	8	61,5
In Umsetzung	3	23,1
Geplant	1	7,7
Nicht geplant	1	7,7

Umsetzungsstand im Einzelnen

Begründung bzw. Erläuterung der Maßnahmenbekanntgabe seitens der geprüften Stelle unter Zuordnung zu den im oben genannten Bericht des Stadtrechnungshofes Wien erfolgten Empfehlungen, der jeweiligen Stellungnahme zu diesen Empfehlungen seitens der geprüften Stelle und allfälliger Gegenäußerung des Stadtrechnungshofes Wien:

Empfehlung Nr. 1

Bei der Weiterentwicklung des Schulinformationssystems "WiSion" ist in Zusammenarbeit mit der Magistratsabteilung 01 - als verantwortlicher IKT Service Provider in der Betriebsführung - sowie mit den Anwendenden des Informationssystems (u.a. Stadtschulrat für Wien) die Implementierung von Audit-Berechtigungen bzw. Audit-Rollen für revisionierende Einrichtungen zu evaluieren.

Stellungnahme der geprüften Stelle:

Eine entsprechende Audit-Rolle für revisionierende Einrichtungen ist mit geringem Finanzaufwand durchführbar und wird in einer der nächsten Lieferungen umgesetzt werden. Administrativ kann es bei Audit-Berechtigungen von z.B. Drucksorten, Abfragen etc. zu einem höheren Aufwand kommen, da eine künftige Audit-Rolle auf diese Programmteile von den jeweiligen Erstellern separat berechtigt werden muss.

Maßnahmenbekanntgabe der geprüften Stelle:

Die Empfehlung befindet sich in Umsetzung.

Eine Audit-Rolle wird mit dem Change Request CR_26-068 umgesetzt. Die geplante Produktivsetzung ist im November 2019.

Empfehlung Nr. 2

In Zusammenwirken mit der Magistratsabteilung 01 ist sicherzustellen, dass ausschließlich berechtigte Personen auf die Inhalte der Online-Hilfe des Schulverwaltungsprogramms "WiSion" zugreifen können.

Stellungnahme der geprüften Stelle:

Aufgrund der derzeit stattfindenden Integration des Wiener Bildungsnetzes in das EDV-Netz der Stadt Wien wäre eine derzeitige Inangriffnahme nicht wirtschaftlich und zweckmäßig. Nach dem Ende des laufenden Rollouts wird jedenfalls auch die Integration der "WiSions"-Hilfe in das EDV-Netzwerk der Stadt Wien angestrebt. Eine entsprechende Berechtigung zur Nutzung der Online-Hilfe wird dadurch umgesetzt werden.

Maßnahmenbekanntgabe der geprüften Stelle:

Die Umsetzung der Empfehlung ist geplant.

Die Stellungnahme der Magistratsabteilung 56 bleibt hier aufrecht.

Empfehlung Nr. 3

Regelmäßige Kontrollen der Loggingdateien über die manuelle Anlage und Löschung von Benutzendenkonten im Schulverwaltungsprogramm "WiSion" sind im Vieraugenprinzip durchzuführen.

Stellungnahme der geprüften Stelle:

Die Empfehlung wird einmal jährlich - beginnend mit dem Jahr 2019 - in Kooperation mit dem Stadtschulrat für Wien (künftig Bildungsdirektion) umgesetzt und dokumentiert werden.

Maßnahmenbekanntgabe der geprüften Stelle:

Die Empfehlung wurde umgesetzt.

Aufgrund des Umfanges (mehr als 4.700 Datensätze) konnte nicht jede bzw. jeder manuell angelegte Benutzende kontrolliert werden. Es wurden daher Stichproben gezogen, diese enthielten keine Auffälligkeiten. Weiters wurden alle manuell angelegten Benutzenden, die eine Administratorenrolle erhielten, geprüft. Auch hier gab es keinerlei Auffälligkeiten. Die große Datenmenge ist dadurch zu erklären, dass es sich hier um die erste Prüfung zu dieser Thematik handelt und daher alle manuell angelegten Benutzenden seit Inbetriebnahme von "WiSion" ausgewertet wurden. In den Folgejahren wird versucht noch detaillierter zu überprüfen.

Empfehlung Nr. 4

In Zusammenwirken mit den Anwendenden des Stadtschulrates für Wien sind die bestehenden Rollencontainer, Rollen und Rechtepakte hinsichtlich ihres Erfordernisses sowie hinsichtlich etwaiger Doppelgleisigkeiten zu evaluieren und gegebenenfalls zu bereinigen.

Stellungnahme der geprüften Stelle:

Die Empfehlung wird einmal jährlich - beginnend mit dem Jahr 2019 - in Kooperation mit dem Stadtschulrat für Wien (künftig Bildungsdirektion) umgesetzt und dokumentiert werden.

Maßnahmenbekanntgabe der geprüften Stelle:

Die Empfehlung wurde umgesetzt.

Eine erste Vieraugenkontrolle zwischen der Magistratsabteilung 56 und der Bildungsdirektion für Wien wurde durchgeführt und dokumentiert.

Empfehlung Nr. 5

Die vergebenen Administratorenberechtigungen sind in Zusammenwirken mit den Anwendenden des Stadtschulrates für Wien regelmäßig zu evaluieren und gegebenenfalls sind nicht zwingend erforderliche Berechtigungen zu entfernen.

Stellungnahme der geprüften Stelle:

Die Empfehlung wird einmal jährlich - beginnend mit dem Jahr 2019 - in Kooperation mit dem Stadtschulrat für Wien (künftig Bildungsdirektion) sowie der Magistratsabteilung 01 umgesetzt und dokumentiert werden.

Maßnahmenbekanntgabe der geprüften Stelle:

Die Empfehlung wurde umgesetzt.

Eine erste Vieraugen-Kontrolle zwischen der Magistratsabteilung 56 und der Bildungsdirektion für Wien wurde durchgeführt und dokumentiert.

Empfehlung Nr. 6

In der Thematik der Security, Safety und Compliance ist eine Risikoanalyse durchzuführen. Unter Berücksichtigung von Kosten-Nutzen-Aspekten sind Maßnahmen zu evaluieren bzw. zu setzen, um sicherzustellen, dass die Aktivitäten der "Superuser" und der "Administratoren" in sensiblen Bereichen jederzeit nachvollziehbar sind.

Stellungnahme der geprüften Stelle:

Die Nachvollziehbarkeit der Aktivitäten von "Administratoren" und "Superusern" (Logging) ist aus Sicht der Magistratsabteilung 56 rasch umsetzbar. Die Magistratsabteilung 56 wird die diesbezüglich erforderlichen Schritte veranlassen.

Zur Risikoanalyse in diesem Bereich sowie generell hinsichtlich der Security im "WiSions"-Bereich wird festgestellt, dass dies in den Kompetenzbereich der zuständigen Fachdienststelle Magistratsabteilung 01 fällt. Vor diesem Hintergrund wird daher ein entsprechendes Schreiben an die Magistratsabteilung 01 gerichtet werden.

Maßnahmenbekanntgabe der geprüften Stelle:
Die Empfehlung befindet sich in Umsetzung.

Das Logging im Bereich der Aktivitäten der "Administratoren" und "Superuser" wurde aktiviert. Eine Risikoanalyse findet derzeit in der Magistratsabteilung 01 statt.

Empfehlung Nr. 7
Regelmäßige Kontrollen der Loggingdateien der Berechtigungsvergabe sind im Vieraugenprinzip mit dem Stadtschulrat für Wien durchzuführen.

Stellungnahme der geprüften Stelle:
Die Empfehlung wird einmal jährlich - beginnend mit dem Jahr 2019 - in Kooperation mit dem Stadtschulrat für Wien (künftig Bildungsdirektion) umgesetzt und dokumentiert werden.

Maßnahmenbekanntgabe der geprüften Stelle:
Die Empfehlung wurde umgesetzt.

Bis auf die "Administratoren" ist eine Berechtigungsvergabe durch Benutzende im Rahmen ihrer Kompetenz stark eingeschränkt und an die dienstlichen Erfordernisse angepasst. So kann z.B. eine Schulleiterin bzw. ein Schulleiter ihrem bzw. seinem untergeordneten Personal Klassenführungs-, Freizeitleitungs- aber auch Betreuer-Rechte etc. vererben. Aufgrund dieser Kompetenzzuteilung ist eine zentrale Kontrolle nicht vorgesehen. Die Administratorenberechtigungen wurden im Vieraugenprinzip geprüft und den Gegebenheiten angepasst.

Empfehlung Nr. 8
Die gewählte Form der Berechtigungsvergabe ist zu evaluieren und dabei sind vor allem die Möglichkeiten einer stärkeren Standardisierung sowie der Implementierung von Kontrollschritten - im Rahmen der Thematik eines IKS - zur Vermeidung von Doppelgleisigkeiten zu berücksichtigen.

Stellungnahme der geprüften Stelle:

Eine Standardisierung von Berechtigungen und Rollencontainern ist aus Sicht der Magistratsabteilung 56 sowie des Stadtschulrates für Wien gegeben. Individuelle Berechtigungen kommen vergleichsweise gering vor. Aufgrund der erforderlichen Trennung der Organisationseinheiten im Programm sind manche doppelt angelegten Berechtigungen nicht vermeidbar.

Maßnahmenbekanntgabe der geprüften Stelle:

Die Umsetzung der Empfehlung ist nicht geplant.

Die Stellungnahme der Magistratsabteilung 56 bleibt hier aufrecht.

Empfehlung Nr. 9

Die weiterhin bestehenden Berechtigungen der Administratoren auf Sicherheitsstufe 1 sind zu evaluieren und es ist sicherzustellen, dass der Zugriff auf sensible Daten bzw. Funktionen erst nach Anwendung eines weiteren Authentifizierungsmerkmals möglich ist.

Stellungnahme der geprüften Stelle:

Die Adaptierung der Berechtigungen für alle "Administratoren" und "Superuser" wurde bereits am 14. Dezember 2017 veranlasst.

Maßnahmenbekanntgabe der geprüften Stelle:

Die Empfehlung wurde umgesetzt.

Die Empfehlung wurde mit 14. Dezember 2017 umgesetzt.

Empfehlung Nr. 10

Das Ablaufdiagramm über die Tokenverwaltung bzw. den Lebenszyklus eines Tokens ist in Zusammenarbeit mit der Magistratsabteilung 01 zu evaluieren und eine Dokumentation der realen Prozessabläufe sicherzustellen.

Stellungnahme der geprüften Stelle:
Der Prozessablauf zur Tokenverwaltung wird seitens der Magistratsabteilung 56 überarbeitet und aktualisiert werden.

Maßnahmenbekanntgabe der geprüften Stelle:
Die Empfehlung wurde umgesetzt.

Das Ablaufdiagramm wurde überarbeitet und an die neuesten Änderungen angepasst.

Empfehlung Nr. 11
Die Tokenverwaltung ist in Zusammenarbeit mit der Magistratsabteilung 01 zu evaluieren und es ist sicherzustellen, dass die Daten bzw. Statuszuweisungen im Schulverwaltungsprogramm "WiSion" und dem Informationssystem "Identity Guard" miteinander übereinstimmen.

Stellungnahme der geprüften Stelle:
Diese Empfehlung ist insbesondere aufgrund der unterschiedlichen Statusanzahl in den Systemen "WiSion" und "Identity Guard" nicht 1 zu 1 umsetzbar. Konkret bietet das System "Identity Guard" nicht alle Stati, die das System "WiSion" benötigt.

Ab dem Jahr 2019 wird die Magistratsabteilung 56 einmal jährlich einen manuellen Abgleich der Stati der beiden Systeme in enger Zusammenarbeit mit der Magistratsabteilung 01 durchführen und dokumentieren.

Maßnahmenbekanntgabe der geprüften Stelle:
Die Empfehlung wurde umgesetzt.

Eine Kontrolle zwischen den Systemen "WiSion" und "Identity Guard" fand statt und wurde entsprechend dokumentiert. Eine Angleichung der Stati in den beiden Programmen ist nicht vorgesehen.

Empfehlung Nr. 12

Es sind Maßnahmen zu evaluieren, um die Nachvollziehbarkeit von Verlusten bzw. Diebstählen von Token sowie deren etwaige Wiederbeschaffung zu gewährleisten.

Stellungnahme der geprüften Stelle:

Mit dem Change Request CR_26-045 wird diese Empfehlung umgesetzt werden. Die Produktivsetzung wird voraussichtlich im Dezember 2018 erfolgen.

Maßnahmenbekanntgabe der geprüften Stelle:

Die Empfehlung wurde umgesetzt.

Der entsprechende Change Request CR_26-045 wurde bereits produktiv gesetzt. Die Stati "verloren" und "gestohlen" sind somit auswertbar.

Empfehlung Nr. 13

Unter Berücksichtigung von Kosten-Nutzen-Überlegungen sind die Möglichkeiten zur Auswertung, Extraktion und Prüfung der Loggingdaten (Eventdaten) des Zeugniserstellungsprozesses zu evaluieren und dadurch die Nachvollziehbarkeit der Erstellung von Zeugnissen sicherzustellen.

Stellungnahme der geprüften Stelle:

Das Logging im Zeugnisprozess wurde bereits erweitert. Aufgrund wirtschaftlicher Überlegungen kann das Loggen des letzten Schrittes im Zeugniserstellungsprozess ("Fertigung") derzeit nicht in Angriff genommen werden.

Maßnahmenbekanntgabe der geprüften Stelle:

Die Empfehlung befindet sich in Umsetzung.

Ein entsprechender Change Request CR_04-075 wurde ausgearbeitet und befindet sich derzeit in Umsetzung. Die geplante Produktivsetzung ist im August 2019.

Für den Stadtrechnungshofdirektor:

Mag. Manfred Jordan

Wien, im August 2019