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, Prüfung des

Schulverwaltungsprogramms "WiSion"

KURZFASSUNG

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 Emp-

fehlungen durch die Magistratsabteilung 56 anzuraten. Ferner sollte sie die Prozessdaten der Zeugniserstellung des Schulinformationssystems "WiSion" im Rahmen der Data Excellence der Stadt Wien bereitstellen.

Der Stadtrechnungshof Wien unterzog in einem ersten Schritt das von der Magistratsabteilung 56 betriebene Schulverwaltungsprogramm "WiSion" einer operativ technischen stichprobenweisen Prüfung und teilte das Ergebnis seiner Wahrnehmungen nach Abhaltung diesbezüglicher Schlussbesprechungen den geprüften Stellen mit. Die von den geprüften Stellen abgegebenen Stellungnahmen wurden berücksichtigt. Allfällige Rundungsdifferenzen bei der Darstellung von Berechnungen wurden nicht ausgeglichen.

INHALTSVERZEICHNIS

ABKÜRZUNGSVERZEICHNIS

Abs.	Absatz
bzw.	beziehungsweise
CR	Change Request
EDV	Elektronische Datenverarbeitung
etc.	et cetera
GJS	Geschäftsgruppe Bildung, Jugend, Information und Sport
http	Hypertext Transfer Protocol
IEEE	Institute of Electrical and Electronics Engineers
IKS	Internes Kontrollsystem
IKT	Informations- und Kommunikationstechnologie
inkl.	inklusive
MA	Magistratsabteilung
Nr.	Nummer
PC	Personal Computer
pdf	Portable Document Format
Pkt.	Punkt
rd.	rund
s.	siehe
StRH	Stadtrechnungshof
u.a.	unter anderem
WiSion	Wiener Schulinformationssystem Online
www	World Wide Web
z.B.	zum Beispiel
z.T.	zum Teil
Zl.	Zahl

LITERATURVERZEICHNIS

IEEE Task Force on Process Mining. 2012. Process Mining Manifest. [Online] 2012. [Zitat vom: 2. August 2018.] http://www.win.tue.nl/ieeetfpm/lib/exe/fetch.php?media=shared:pmm-german-v1.pdf.

GLOSSAR

Prozess Mining

Mit der Datenanalysemethode des Prozess Minings können auf Basis der in einem Informationssystem aufgezeichneten Ereignisse die real abgelaufenen Prozesse erkannt, abgebildet und analysiert werden. Dies ermöglicht u.a. das Analysieren und Verbessern von Geschäftsprozessen bzw. die Entdeckung und Überwachung von Abweichungen zwischen dem Soll-Prozess und dem tatsächlichen Ist-Ablauf (IEEE Task Force on Process Mining, 2012).

Token

Unter einem Token wird eine Komponente (Hardware- oder Softwaretoken) verstanden, die zur Identifizierung und Authentifizierung von Benutzenden an einem Informationssystem zur Zugriffskontrolle bzw. Zwei-Faktor-Authentisierung verwendet wird.

PRÜFUNGSERGEBNIS

1. Prüfungsgrundlagen des Stadtrechnungshofes Wien

1.1 Prüfungsgegenstand

Die gegenständliche Prüfung wurde von der Abteilung Kultur und Bildung des Stadtrechnungshofes Wien durchgeführt.

Die Entscheidung zur Durchführung der gegenständlichen Prüfung wurde in Anwendung der risikoorientierten Prüfungsthemenauswahl des Stadtrechnungshofes Wien getroffen.

Gegenstand der Prüfung war das Schulverwaltungsprogramm "Wiener Schulinformationssystem online" - kurz "WiSion", das seit der Inbetriebnahme im Jahr 2012 an allen allgemein bildenden öffentlichen Pflichtschulen in Wien eingesetzt wurde.

Der Fokus der Prüfung des Schulverwaltungsprogramms "WiSion" lag auf der operativen Anwendung bzw. Verwendung sowie der technischen Betriebsführung

- der Rollen- und Berechtigungsverwaltung,
- der damit in Zusammenhang stehenden Tokenverwaltung und
- dem Prozess der Zeugniserstellung.

Die operative Anwendung bzw. Verwendung der in der Prüfung berücksichtigten Teilaspekte des Schulverwaltungsprogramms "WiSion" erfolgte durch die Benutzenden der Magistratsabteilung 56 sowie durch die Benutzenden des Stadtschulrates für Wien.

Die Betriebsführung des Schulverwaltungsprogramms "WiSion" oblag der Magistratsabteilung 14 bzw. 01 - als verantwortlicher IKT Service Provider - im Zusammenwirken mit einem beauftragten externen Unternehmen.

Nichtziele der Prüfung waren eine Beurteilung der Beschaffung des Schulverwaltungsprogramms "WiSion" sowie des Projektmanagements im Zuge der Einführung des Informationssystems.

In einer weiteren nachfolgenden Prüfung beabsichtigt der Stadtrechnungshof Wien, verstärkt auf nutzendenbezogene Anwendungen einzugehen.

1.2 Prüfungszeitraum

Die gegenständliche Prüfung erfolgte im vierten Quartal 2017 und dem ersten bzw. zweiten Quartal 2018. Die Eröffnungsgespräche mit den geprüften bzw. direkt betroffenen Dienststellen (Magistratsabteilung 56 und Magistratsabteilung 14 bzw. 01) fanden Anfang Oktober 2017 statt. Die Schlussbesprechungen wurden Mitte Oktober 2018 durchgeführt.

Der Betrachtungszeitraum umfasste das Jahr 2017, wobei gegebenenfalls auch frühere, spätere oder aktuelle Entwicklungen in die Einschau einbezogen wurden.

1.3 Prüfungshandlungen

Die Prüfungshandlungen umfassten Dokumentenanalysen, Literatur-, Internet- und Intranetrecherchen, Einstiege in das betreffende Informationssystem, Berechnungen, Belegprüfungen und Interviews bei den geprüften bzw. betroffenen Dienststellen bzw. Organisationseinheiten.

Bei der Durchführung der Prüfung ergaben sich keine Prüfungshindernisse.

1.4 Prüfungsbefugnis

Die Prüfungsbefugnis für diese Gebarungsprüfung ist in § 73b Abs. 1 der Wiener Stadtverfassung festgeschrieben.

Der Stadtschulrat für Wien unterlag zum Prüfungszeitpunkt keiner Prüfungsbefugnis durch den Stadtrechnungshof Wien.

Vom Stadtrechnungshof Wien war in diesem Zusammenhang positiv zu erwähnen, dass neben den Vertretern der Magistratsabteilung 56 ebenso Vertreter des Stadtschulrates für Wien, der Magistratsabteilung 14 bzw. 01 und des beauftragen externen Unternehmens regelmäßig an gemeinsamen Besprechungen teilnahmen. Sie wirkten auch bei der inhaltlichen Bearbeitung von Fragestellungen mit.

1.5 Vorberichte

Der Stadtrechnungshof Wien behandelte Teilaspekte der vorliegenden Prüfung in den Berichten

- MA 56, Prüfung des Wiener Bildungsnetzes, StRH I - 56-1/14 und
- MA 56, Prüfung von Beschaffungsprozessen, Prüfung der Maßnahmenbekanntgabe, StRH I - 4/16.

2. Allgemeines

Die Stadt Wien war gesetzliche Schulhalterin der öffentlichen Pflichtschulen und damit für die Errichtung, Erhaltung und Auflassung dieser zuständig. Gemäß der Geschäftseinteilung für den Magistrat der Stadt Wien nahm die Magistratsabteilung 56 die Aufgaben der Stadt Wien in ihrer Funktion als Schulhalterin wahr.

Am 27. Juni 2007 wurde vom Wiener Gemeinderat mit Beschluss 02378-2007/0001-GJS, P 22 die "Schaffung einer zentralen Schulverwaltungslösung" genehmigt. Im Rahmen eines Vergabeverfahrens wurde in weiterer Folge das Schulverwaltungsprogramm "WiSion" beschafft und im Jahr 2012 in Betrieb genommen.

Zum Prüfungszeitpunkt wurde die Applikation zur Administration der allgemein bildenden öffentlichen Wiener Pflichtschulen eingesetzt und von diesen sowie der Magistratsabteilung 56 und dem Stadtschulrat für Wien verwendet. Es handelte sich um eine webbasierte Software, die ohne eine Installation auf unterschiedlichen IKT Endgeräten verwendet werden konnte (PC, Notebook, Tablet, Smartphone etc.).

Der Magistratsabteilung 14 bzw. 01 oblag gemäß der Geschäftseinteilung für den Magistrat der Stadt Wien die Betriebsführung und Erhaltung des Informationssystems.

Mit dem Schulverwaltungsprogramm "WiSion" wurden verschiedene Abläufe im Schulmanagement wie beispielsweise die Einschreibung von Schülerinnen bzw. Schülern, die Verrechnung der Nachmittagsbetreuung oder die Zeugniserstellung digital abgewickelt. Zum Prüfungszeitpunkt wurden im Schulverwaltungsprogramm "WiSion" rd. 110.000 Schülerinnen- bzw. Schülerdatensätze sowie rd. 15.000 Lehrende verwaltet.

3. Rollen- und Berechtigungsverwaltung

3.1 Auditfunktionalitäten

Das Schulverwaltungsprogramm "WiSion" verfügte über keine expliziten Auditberechtigungen bzw. Auditrollen für Revisionierende. Für den Stadtrechnungshof Wien wurde deshalb für die gegenständliche Prüfung eine Administratorenberechtigung auf einer Testumgebung eingerichtet.

Diese Testumgebung war vom Produktivsystem getrennt und arbeitete mit einer stichtagsbezogenen Datenbankspiegelung. Dadurch war sichergestellt, dass durch den Stadtrechnungshof Wien keine Daten im Produktivsystem verändert werden konnten.

Aufgrund des Fehlens von Auditberechtigungen bzw. Auditrollen für Revisionierende war es für den Stadtrechnungshof Wien nur erschwert möglich, Funktionalitäten des Produktivsystems einzusehen bzw. zu testen. Die Funktionalitäten des Informationssystems wurden vom Stadtrechnungshof Wien in weiterer Folge in der Testumgebung eingesehen. Prüfungsrelevante Fragen und ausgewählte Funktionen wurden zusätzlich von den Mitarbeitenden der Magistratsabteilung 56 und des Stadtschulrates für Wien im Produktivsystem vorgeführt, um zu verifizieren, dass das Produktivsystem in ausgewählten Bereichen in Übereinstimmung mit der Testumgebung stand.

Der Stadtrechnungshof Wien empfahl der Magistratsabteilung 56, künftig bei der Weiterentwicklung des Schulinformationssystems "WiSion" in Zusammenarbeit mit der Magistratsabteilung 01 - als verantwortlichem 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.

Der Stadtrechnungshof Wien empfahl der Magistratsabteilung 01, die Magistratsabteilung 56 bei der Evaluierung der Implementierung von Audit-Berechtigungen bzw. Audit-Rollen für revisionierende Einrichtungen bei der Weiterentwicklung des Schulinformationssystems "WiSion" zu unterstützen und die entsprechenden Ressourcen bereitzustellen.

3.2 Online-Hilfe

Für das Schulverwaltungsprogramm "WiSion" stand eine umfangreiche Online-Hilfe zur Verfügung, in der die Funktionalitäten des Informationssystems beschrieben waren. Die Online-Hilfe wurde von dem beauftragen, externen Unternehmen (Entwicklerfirma) des Schulverwaltungsprogramms "WiSion" betrieben.

Der Zugriff auf die Online-Hilfe stand den Benutzenden in nicht ausreichend gesicherter Form zur Verfügung.

Der Stadtrechnungshof Wien empfahl der Magistratsabteilung 56 in Zusammenwirken mit der Magistratsabteilung 01 sicherzustellen, dass ausschließlich berechtigte Personen auf die Inhalte der Online-Hilfe des Schulverwaltungsprogramms "WiSion" zugreifen können.

Der Stadtrechnungshof Wien empfahl der Magistratsabteilung 01, die Magistratsabteilung 56 bei der Umsetzung des Zugriffs auf die Online-Hilfe des Schulverwaltungsprogramms "WiSion" hinsichtlich der Thematik der Security, Safety und Compliance zu unterstützen und die entsprechenden Ressourcen bereitzustellen.

3.3 Anlage von Benutzenden

3.3.1 Mitarbeitende der Stadt Wien wurden in einer zentralen Personaldatenbank administriert. Darüber hinaus wurde von der Magistratsabteilung 14 bzw. 01 ein Netzwerk-

Verzeichnisdienst zur Verfügung gestellt, in dem die Benutzendenkonten für die verschiedenen Softwareapplikationen der Stadt Wien verwaltet wurden.

Für die Anlage eines neuen Benutzenden im Schulverwaltungsprogramm "WiSion" war grundsätzlich ein Eintrag in die Personaldatenbank der Stadt Wien sowie die Anlage eines Benutzenden in dem von der Magistratsabteilung 14 bzw. 01 zur Verfügung gestellten Netzwerk-Verzeichnisdienst erforderlich. Diese Daten wurden in weiterer Folge über ein Webservice für "WiSion" bereitgestellt.

Es erfolgte täglich ein Abgleich der Benutzenden im Schulverwaltungsprogramm "WiSion" mit dem Netzwerk-Verzeichnisdienst bzw. der Personaldatenbank der Stadt Wien. Veränderte Personaldaten wie beispielsweise Namensänderungen infolge von Eheschließungen wurden dadurch zeitnah in das Schulverwaltungsprogramm "WiSion" übernommen. Sobald Benutzende nicht mehr in der Personaldatenbank der Stadt Wien bzw. dem Netzwerk-Verzeichnisdienst aufschienen (z.B. aufgrund der Beendigung des Dienstverhältnisses), wurden im Zuge des Abgleichs alle Berechtigungen für das Schulverwaltungsprogramm "WiSion" gelöscht und ein Zugriff war nicht weiter möglich.

3.3.2 Berechtigte Personen konnten Benutzende für sonstiges Personal auch manuell im Schulverwaltungsprogramm "WiSion" anlegen. Dadurch war ein Zugriff auf das System unabhängig von einem Eintrag in die Personaldatenbank der Stadt Wien bzw. der Anlage eines Benutzenden im Netzwerk-Verzeichnisdienst der Magistratsabteilung 14 bzw. 01 möglich. Eine manuelle Anlage von Benutzendenkonten wurde für spezielle Berufsgruppen, der betreuten Aufgabenbereiche durchgeführt.

Benutzende, die manuell im Schulverwaltungsprogramm "WiSion" angelegt wurden, mussten auch wieder manuell gelöscht werden. Der oben dargestellte automatische Abgleich mit dem Netzwerk-Verzeichnisdienst bzw. der Personaldatenbank der Stadt Wien war in diesen Fällen nicht möglich.

3.3.3 Im Zuge der Prüfung zeigte sich, dass die manuelle Anlage von Benutzenden im Schulverwaltungsprogramm "WiSion" in keiner Form protokolliert bzw. geloggt wurde.

Dadurch war nicht nachvollziehbar, von wem welche Benutzenden zu welchem Zeitpunkt angelegt wurden. Ein Vieraugenprinzip bei der Anlage von Benutzenden war nicht vorgesehen.

Aus Sicht des Stadtrechnungshofes Wien war mangels geeigneter Kontrollmechanismen ein erhöhtes Risiko gegeben, dass Zugriffsberechtigungen auf das System und somit auf sensible personenbezogene Daten an nicht berechtigte Personen vergeben werden konnten. Dieses Risiko wurde durch den Umstand verstärkt, dass eine Vielzahl von Personen zur manuellen Anlage von Benutzenden in "WiSion" berechtigt war.

Von den Verantwortlichen der Magistratsabteilung 56 wurde noch vor Abschluss der Prüfungshandlungen des Stadtrechnungshofes Wien veranlasst, ein Logging der Uservergabe zu aktivieren. Aufgrund dieser umgehenden Reaktion wurde von einer Empfehlung hinsichtlich der Umsetzung eines Logging von Uservergaben abgesehen.

Der Stadtrechnungshof Wien empfahl der Magistratsabteilung 56, regelmäßige Kontrollen der Loggingdateien über die manuelle Anlage und Löschung von Benutzendenkonten im Schulverwaltungsprogramm "WiSion" im Vieraugenprinzip durchzuführen.

3.4 Rollen und Rechtepakete

3.4.1 Im Aufbau und in der Struktur des Schulverwaltungsprogramms "WiSion" wurde von der Festlegung einer abschließenden Anzahl an Rollen für den Zugriff auf das Schulverwaltungsprogramm "WiSion" abgesehen. Dies deshalb, da nach Angabe der Verantwortlichen der Magistratsabteilung 56 und des Stadtschulrates für Wien eine besondere Flexibilität in der Rechtevergabe sowie eine Minimierung des administratorischen Aufwandes angestrebt wurde. In weiterer Folge wurde im laufenden Betrieb schrittweise ein modulares Rollen- und Berechtigungssystem aufgebaut. Dabei wurde mit Rollencontainern gearbeitet, denen je nach Bedarf Rollen und Rechtepakete zugeordnet werden konnten.

Mit Stand März 2018 waren im Schulverwaltungsprogramm "WiSion" 387 Rollen und Rechtepakete verfügbar. Davon handelte es sich bei 116 Rollen um übergeordnete Rollen, denen weitere Rollen bzw. Rechtepakete untergeordnet waren.

Im Zuge der Prüfung wurde festgestellt, dass vereinzelt Rollen bzw. Rechtepakete mit identen Berechtigungen doppelt unter unterschiedlichen Bezeichnungen angelegt waren. Zudem zeigte sich bei den unterschiedlichen Administratorenrollen, dass einer übergeordneten Rolle z.T. mehrfach dieselben Berechtigungen über unterschiedliche untergeordnete Rollen und Rechtepakete zugewiesen waren. Die festgestellten Doppelgleisigkeiten wurden von den Systemanwendenden u.a. damit begründet, dass dadurch eine bessere Unterscheidbarkeit der Benutzenden möglich war. Aus Sicht des Stadtrechnungshofes Wien ergab sich dadurch jedoch ein erhöhter Administrationsaufwand, da etwaige Änderungen der Berechtigungen dieser Rollen mehrfach an verschiedenen Stellen durchgeführt werden mussten. Dies ging mit einem erhöhten Risiko eines menschlichen Versagens im Hinblick auf eine vollständige Durchführung aller erforderlichen bzw. notwendigen Änderungen der Berechtigung von Rollen einher.

Der Stadtrechnungshof Wien empfahl der Magistratsabteilung 56 in Zusammenwirken mit den Anwendenden des Stadtschulrates für Wien, die bestehenden Rollencontainer, Rollen und Rechtepakte hinsichtlich ihres Erfordernisses sowie hinsichtlich etwaiger Doppelgleisigkeiten zu evaluieren und gegebenenfalls zu bereinigen.

3.4.2 Die Rollen bzw. Rollencontainer mit den umfassendsten Berechtigungen im Schulverwaltungsprogramm "WiSion" wurden als "Superuser" und als "Administrator" bezeichnet.

Ein "Superuser" hatte Vollzugriff auf alle Funktionen und Daten im System. Zum Prüfungszeitpunkt verfügten zwei Mitarbeitende der Magistratsabteilung 14 bzw. 01 - ein Serviceverantwortlicher sowie ein technischer Ansprechpartner - über die Rolle des "Superusers".

Ein "Administrator" hatte grundsätzlich dieselben Berechtigungen wie ein "Superuser", allerdings waren diese Berechtigungen inhaltlich auf die Organisationseinheit des Stadtschulrates für Wien oder der Magistratsabteilung 56 begrenzt. Infolge konnte nur auf die Funktionen und Daten der zugewiesenen Organisationseinheit zugegriffen werden. Innerhalb der zugewiesenen Organisationseinheit bestand ein Vollzugriff.

Zum Prüfungszeitpunkt gab es in der Magistratsabteilung 56 sowie im Stadtschulrat für Wien je zwei "Administratoren". Zudem verfügten im Stadtschulrat für Wien weitere Mitarbeitende über "Administratorenrechte" in Teilbereichen.

Der Stadtrechnungshof Wien empfahl der Magistratsabteilung 56, im Zusammenwirken mit den Anwendenden des Stadtschulrates für Wien die vergebenen "Administratorenberechtigungen" regelmäßig zu evaluieren und gegebenenfalls nicht zwingend erforderliche Berechtigungen zu entfernen.

Der Stadtrechnungshof Wien empfahl der Magistratsabteilung 01, die vergebenen "Administratorenberechtigungen" regelmäßig zu evaluieren und gegebenenfalls nicht zwingend erforderliche Berechtigungen zu entfernen.

3.4.3 Die Aktivitäten von "Superusern" und "Administratoren" wurden zum Prüfungszeitpunkt nicht protokolliert bzw. geloggt. Dies war insofern kritisch zu sehen, als diese Rollen, umfassende Änderungen vornehmen konnten und u.a. dazu berechtigt waren, ihre Rechte zu vererben bzw. an andere Benutzende weiterzugeben.

Der Stadtrechnungshof Wien empfahl der Magistratsabteilung 56, in der Thematik der Security, Safety und Compliance eine Risikoanalyse durchzuführen. Unter Berücksichtigung von Kosten-Nutzen-Aspekten sollten Maßnahmen evaluiert bzw. gesetzt werden, um sicherzustellen, dass die Aktivitäten von "Superusern" und "Administratoren" in sensiblen Bereichen jederzeit nachvollziehbar sind.

Der Stadtrechnungshof Wien empfahl der Magistratsabteilung 01, die Magistratsabteilung 56 in der Thematik der Security, Safety und Compliance bei der durchzuführenden

Risikoanalyse und der Evaluierung von zu setzenden Maßnahmen hinsichtlich der Nachvollziehbarkeit der Aktivitäten der "Superuser" und der "Administratoren" zu unterstützen. Die entsprechenden Ressourcen wären bereitzustellen.

3.5 Vergabe von Berechtigungen

3.5.1 Die Basis für die Berechtigungsvergabe bildeten die beschriebenen Rollencontainer, Rollen und Rechtepakete.

Neue Rollencontainer konnten von den "Superusern" der Magistratsabteilung 14 bzw. 01 sowie den "Administratoren" des Stadtschulrates für Wien und der Magistratsabteilung 56 angelegt werden. Die Rollencontainer wurden dabei mit Rollen und Rechtepaketen ausgestattet, die einem Benutzenden bei der Vergabe dieses Rollencontainers grundsätzlich zugewiesen werden konnten.

Einer bzw. einem neuen Benutzenden wurde automatisch eine Standardrolle zugewiesen, mit der ein Einstieg in das Schulverwaltungsprogramm "WiSion" möglich war. Im System konnten mit dieser Rolle aber keine weiteren Funktionen verwendet werden, weshalb in einem nächsten Schritt direkt in der Applikation Berechtigungen vergeben werden mussten.

Die Berechtigungsvergabe erfolgte in der Regel durch die zuständige Schulleitung, die einem Benutzenden einen oder mehrere bestehende Rollencontainer zuweisen und je nach Bedarf die darin vorgesehenen Rollen und Rechtepakete vergeben bzw. einschränken konnte. Dadurch konnten aus bestehenden Rollen und Rechtepaketen flexibel Kombinationen zusammengestellt werden.

Die vergebenen Berechtigungen ermöglichten Benutzenden im Schulverwaltungsprogramm "WiSion" die Ausübung von Funktionen und den Zugriff auf Daten. Dabei wurde durch die organisatorische Zuordnung von Benutzenden begrenzt, welche Daten konkret eingesehen bzw. bearbeitet werden konnten. Dies bedeutete, dass beispielsweise Lehrende in unterschiedlichen Schulen dieselben Berechtigungen haben konnten, dennoch aber nur auf die Daten der ihnen zugewiesenen Schulen zugreifen konnten.

Bei Bedarf konnten zeitlich befristete oder unbefristete Stellvertretungen in "WiSion" hinterlegt werden. Die Stellvertretung übernahm infolge für den definierten Zeitraum die Berechtigungen und die Organisationseinheit des Benutzenden.

Für die Vergabe von Berechtigungen war zum Prüfungszeitpunkt keine Protokollierung bzw. kein Logging vorgesehen, weshalb nicht nachvollziehbar war, wann und durch wen Berechtigungen Benutzenden zugewiesen bzw. entzogen wurden. Von einer Empfehlung wurde abgesehen, da von der Magistratsabteilung 56 noch während der Prüfung veranlasst wurde, ein Logging der Berechtigungsvergabe zu aktivieren.

Der Stadtrechnungshof Wien empfahl der Magistratsabteilung 56, regelmäßige Kontrollen der Loggingdateien der Berechtigungsvergabe im Vieraugenprinzip mit dem Stadtschulrat für Wien durchzuführen.

3.5.2 Aus Sicht des Stadtrechnungshofes Wien war aufgrund des geringen Grades an Standardisierung im Rahmen der Berechtigungsvergabe schwer nachvollziehbar, ob die Benutzenden tatsächlich nur über jene Berechtigungen verfügten, die für die Erfüllung ihres Aufgabenfeldes unbedingt erforderlich waren. Zudem wurden - wie bereits erwähnt - idente Rollen und Rechtepakete z.T. mehrfach unter verschiedenen Bezeichnungen angelegt, wodurch Doppelgleisigkeiten entstanden.

Der Stadtrechnungshof Wien verkannte allerdings nicht, dass eine vollständige Standardisierung u.a. aufgrund der unterschiedlichen Aufgabenverteilung in den einzelnen Schulen im Rahmen der Schulautonomie bzw. der dadurch erforderlichen Flexibilität in der Praxis nur schwer umsetzbar war.

Der Stadtrechnungshof Wien empfahl der Magistratsabteilung 56, die gewählte Form der Berechtigungsvergabe zu evaluieren. Dabei wären vor allem die Möglichkeiten einer stärkeren Standardisierung sowie der Implementierung von Kontrollschritten - im Rahmen der Thematik eines IKS - zur Vermeidung von Doppelgleisigkeiten zu berücksichtigen.

3.6 Sicherheitsstufen

3.6.1 Eine weitere Einschränkung der Berechtigungen im Schulverwaltungsprogramm "WiSion" war über die darin definierten Sicherheitsstufen möglich. Es waren drei Sicherheitsstufen vorgesehen, wobei für jede gesondert festgelegt werden konnte, welche Funktionen in welcher Ausprägung anwendbar sein sollten.

Um auf die unterschiedlichen Sicherheitsstufen zu gelangen, waren verschiedene Kombinationen von Authentifizierungsmerkmalen vorgesehen:

- Sicherheitsstufe 1: Authentifizierung mittels "Username" und Passwort,
- Sicherheitsstufe 2: Authentifizierung mittels "Username" und Passwort über ein sicheres Netzwerk oder mittels Hardwaretoken,
- Sicherheitsstufe 3: Authentifizierung mittels "Username" und Passwort über ein sicheres Netzwerk und mittels Hardwaretoken.

3.6.2 Zum Zeitpunkt der Einschau des Stadtrechnungshofes Wien war für die Administratorenrollen vorgesehen, dass bereits auf der ersten Sicherheitsstufe innerhalb der zugewiesenen Organisationseinheit sämtliche Funktionen uneingeschränkt verwendet werden konnten und ein Zugriff auf alle Daten möglich war.

Aus Sicht des Stadtrechnungshofes Wien war dies kritisch zu bewerten, da dadurch die Kenntnis des "Usernamens" und des Passwortes eines "Administrators" für nichtberechtigte Dritte ausreichend war, um Zugriff auf das System und die umfassenden Berechtigungen dieser Rolle zu erlangen.

Von der Magistratsabteilung 56 wurde umgehend veranlasst, die Berechtigungen der "Administratoren" auf Sicherheitsstufe 1 stark einzuschränken. Dabei wurden die Berechtigungen, die direkt aus der "Administratorenrolle" abgeleitet wurden, auf der Sicherheitsstufe 1 entzogen. Dadurch wurde noch während der Prüfung des Stadtrechnungshofes Wien sichergestellt, dass eine zusätzliche Authentifizierung erforderlich war, um einen Vollzugriff auf das System zu erlangen. Einzelne Berechtigungen aus

untergeordneten Rollen blieben hingegen weiterhin bereits auf Sicherheitsstufe 1 bestehen.

Der Stadtrechnungshof Wien empfahl der Magistratsabteilung 56, die weiterhin bestehenden Berechtigungen der "Administratoren" auf Sicherheitsstufe 1 zu evaluieren und sicherzustellen, dass der Zugriff auf sensible Daten bzw. Funktionen erst nach Anwendung eines weiteren Authentifizierungsmerkmals möglich ist.

4. Tokenverwaltung

Im Schulverwaltungsprogramm "WiSion" wurden Hardwaretoken in Kombination mit dem "Usernamen" und dem Passwort zur "Zwei-Faktor-Authentisierung" eingesetzt. Zur Abwicklung bzw. Administration dieser "Zwei-Faktor-Authentisierung" wurde von der Magistratsabteilung 14 bzw. 01 das Informationssystem "Identity Guard" genutzt.

Die Useranlage im Informationssystem "Identity Guard" erfolgte automatisiert, indem das System täglich den Netzwerk-Verzeichnisdienst nach "Usern" mit Berechtigungen für das Schulverwaltungsprogramm "WiSion" durchsuchte. Durch ein Webservice erfolgte in weiterer Folge ein Abgleich der Informationen des Informationssystems "Identity Guard" mit dem Schulverwaltungsprogramm "WiSion".

Die Zuweisung sowie die Aufhebung der Zuweisung eines Tokens zu einer Organisationseinheit und einer bzw. einem Benutzenden wurden direkt im Schulverwaltungsprogramm "WiSion" administriert. Die Benutzendenzuweisung wurde in weiterer Folge an das Informationssystem "Identity Guard" übermittelt.

Da die Zuordnung eines Tokens zu einer Organisationseinheit im Informationssystem "Identity Guard" nicht möglich war, waren im Schulverwaltungsprogramm "WiSion" zusätzliche Stati vorgesehen, um dies abzubilden. In einem Ablaufdiagramm war diesbezüglich der Lebenszyklus eines Tokens dokumentiert und es wurde dargelegt, welche Stati ein Token im Schulverwaltungsprogramm "WiSion" einnehmen konnte und welchen korrespondierenden Stati diese im Informationssystem "Identity Guard" entsprachen.

Im Zuge der Prüfung wurde festgestellt, dass das zur Verfügung gestellte Ablaufdiagramm nicht zur Gänze die realen Prozessabläufe abbildete. So gab es beispielsweise in der Realität Zuweisungsmöglichkeiten, die im Ablaufdiagramm nicht oder anders dargestellt waren.

Der Stadtrechnungshof Wien empfahl der Magistratsabteilung 56, in Zusammenarbeit mit der Magistratsabteilung 01 das Ablaufdiagramm über die Tokenverwaltung bzw. den Lebenszyklus eines Tokens zu evaluieren und eine Dokumentation der realen Prozessabläufe sicherzustellen.

Der Stadtrechnungshof Wien empfahl der Magistratsabteilung 01, die Magistratsabteilung 56 bei der Evaluierung des Ablaufdiagramms über die Tokenverwaltung bzw. den Lebenszyklus eines Tokens und der Sicherstellung der Dokumentation der realen Prozessabläufe zu unterstützen und die entsprechenden Ressourcen bereitzustellen.

Ein Abgleich der im Schulverwaltungsprogramm "WiSion" geführten Token mit jenen im Informationssystem "Identity Guard" zeigte, dass die Anzahl der in den jeweiligen Systemen einem Benutzenden zugewiesenen bzw. nicht zugewiesenen Token voneinander abwich.

Diese Abweichungen waren einerseits dadurch zu erklären, dass im Schulverwaltungsprogramm "WiSion" drei Token geführt wurden, die im Informationssystem "Identity Guard" nicht weiter enthalten waren, da diese mangels Lizenz nicht mehr verwendbar waren. Der physische Verbleib dieser Token war zum Prüfungszeitpunkt nicht bekannt.

Darüber hinaus wurden im Schulverwaltungsprogramm "WiSion" zwei Token geführt, die im Informationssystem "Identity Guard" in einer Gruppe administriert wurde, auf die das Schulverwaltungsprogramm "WiSion" im Rahmen des automatisierten Datenabgleichs nicht zugreifen konnte.

Unstimmigkeiten zeigten sich auch in Bezug auf die in den unterschiedlichen Systemen ausgewiesenen Stati einzelner Token. Für den Stadtrechnungshof Wien war nicht nachvollziehbar, wie diese Unstimmigkeiten zustande kamen. Dies deshalb, da im Fall eines fehlerfreien automatisierten Abgleichs zwischen dem Schulverwaltungsprogramm "WiSion" und dem Informationssystem "Identity Guard" eine Übereinstimmung der Stati der einzelnen Token in den beiden Systemen gegeben sein müsste.

Der Stadtrechnungshof Wien empfahl der Magistratsabteilung 56, in Zusammenarbeit mit der Magistratsabteilung 01 die Tokenverwaltung zu evaluieren und sicherzustellen, dass die Daten- bzw. Statuszuweisungen im Schulverwaltungsprogramm "WiSion" und dem Informationssystem "Identity Guard" miteinander übereinstimmen.

Der Stadtrechnungshof Wien empfahl der Magistratsabteilung 01, die Magistratsabteilung 56 bei der Evaluierung der Tokenverwaltung hinsichtlich der Übereinstimmung von Daten bzw. Statuszuweisungen im Schulverwaltungsprogramm "WiSion" und dem Informationssystem "Identity Guard" zu unterstützen und die entsprechenden Ressourcen bereitzustellen.

Der Stadtrechnungshof Wien empfahl der Magistratsabteilung 01 eine regelmäßige Kontrolle der Token des Informationssystems "Identity Guard" in der Verwaltung und Verwendung mit dem Schulverwaltungsprogramm "WiSion" im Vieraugenprinzip mit der Magistratsabteilung 56 bzw. dem Stadtschulrat für Wien zu evaluieren.

4.1 Ausgabe von Token

Von der Magistratsabteilung 56 wurde an die einzelnen Schulen ein Kontingent an Hardwaretoken ausgegeben und diese im Schulverwaltungsprogramm "WiSion" der jeweiligen Organisationseinheit zugeordnet.

In der jeweiligen Organisationseinheit wurden die Token durch die Schulleitungen an die Benutzenden ausgegeben. Dabei war die Übernahme eines Tokens mittels Übernahmebestätigung zu dokumentieren und der ausgegebene Token wurde im Schulver-

waltungsprogramm "WiSion" entsprechend dem jeweiligen Benutzenden zugeordnet. Auch die Rückgabe eines Tokens war schriftlich zu bestätigen.

4.2 Verlust bzw. Diebstahl von Token

Mit der Übernahme eines Tokens verpflichten sich die Benutzenden, den Verlust oder Diebstahl des Tokens unverzüglich über die Schulleitung an die Magistratsabteilung 56 zu melden. Darüber hinaus war eine Verlustanzeige bei einem Magistratischen Bezirksamt bzw. eine Diebstahlanzeige bei der Polizei zu erstatten. Im Schulverwaltungsprogramm "WiSion" wurde in weiterer Folge die Zuordnung der bzw. des Benutzenden und der Organisationseinheit des Tokens entfernt. Dadurch wurde dieser unbrauchbar, konnte aber im Fall der Wiederbeschaffung reaktiviert und erneut verwendet werden.

Eine gesonderte Kennzeichnung gestohlener oder verlorener Token erfolgte weder im Schulverwaltungsprogramm "WiSion" noch im Informationssystem "Identity Guard" der Stadt Wien. Dies war aus Sicht des Stadtrechnungshofes Wien kritisch zu sehen, da keine Möglichkeit zur Auswertung der gestohlenen und verlorenen Token gegeben war und nicht nachvollzogen werden konnte, wenn ein verlorener bzw. gestohlener Token wiedergefunden wurde.

Ferner war im Fall eines Verlustes oder Diebstahls eine Meldung im elektronischen Schadensmeldungsformular der Stadt Wien zu erstatten. Darin wurde in der Regel erfasst, wie viele Token verloren oder gestohlen wurden. Eindeutige Identifikationsmerkmale der Token - wie beispielsweise die Seriennummer - waren nicht verpflichtend anzugeben, weshalb auch mit diesen Aufzeichnungen kein Rückschluss möglich war, welche Token als verloren oder gestohlen gemeldet waren.

Der Stadtrechnungshof Wien empfahl der Magistratsabteilung 56, Maßnahmen zu evaluieren, um die Nachvollziehbarkeit von Verlusten bzw. Diebstählen von Token sowie deren etwaige Wiederbeschaffung zu gewährleisten.

5. Zeugniserstellung

5.1 Prozessablauf

Beurteilungen von Schülerinnen bzw. Schülern konnten im Schulverwaltungsprogramm "WiSion" administriert und Zeugnisse erstellt werden. Dabei wurde zwischen den Beurteilungsarten Schulnachricht, Jahreszeugnis und Beurteilungsvorschlag unterschieden.

Zur Anlage von Zeugnissen bzw. dem Eintragen von Beurteilungen waren die Schulleitungen und deren Stellvertretungen, Klassenvorstände sowie Zeugnisverantwortliche der Schulen berechtigt.

Die Anlage eines Beurteilungsvorschlags war jederzeit auch unterjährig möglich. Schulnachrichten bzw. Jahreszeugnisse konnten lediglich in einem bestimmten, zentral festgelegten Zeitraum erstellt werden.

Pflichtgegenstände und verbindliche Übungen wurden vom Schulverwaltungsprogramm "WiSion" aus der Stundentafel der Schülerin bzw. des Schülers übernommen. Die unverbindlichen Übungen sowie Freigegenstände wurden aufgrund der Klassen- und Gruppeneinteilung zur Verfügung gestellt. Das Beurteilungssystem einer Schülerin bzw. eines Schülers war dabei bereits zum Zeitpunkt der Zeugniserstellung fixiert bzw. leitete sich aus der Stundentafel der jeweiligen Schülerin bzw. des jeweiligen Schülers ab. Die Beurteilungsskalen wurden entsprechend des Beurteilungssystems von "WiSion" geladen und in Form eines Drop-Down-Menüs bereitgestellt.

Wurden alle Beurteilungen eingetragen, hatte die eingebende Person durch die erste Kollationierung die Richtigkeit des Zeugnisses zu bestätigen. Dies war technisch durch eine Freigabe des Zeugnisses mittels Eingabe des Benutzendennamen und des Passworts realisiert. Darüber hinaus war im Zuge der ersten Kollationierung eine Person festzulegen, die die zweite Kollationierung durchführen sollte. Dafür standen alle Lehrpersonen, die die jeweilige Schule als Stammschule zugeordnet hatten, in einem Drop-Down-Menü zur Auswahl.

Mit der zweiten Kollationierung, für die ebenfalls die Eingabe von Benutzendennamen und Passwort erforderlich war, wurde die Richtigkeit der eingebenden Beurteilungen von einer zweiten Lehrperson bestätigt. Im Fall eines Fehlers war die Beurteilung nicht zu kollationieren und in den Status "angelegt" zurückzuführen.

Bis zum Abschluss der zweiten Kollationierung konnte die eingebende Person eine Beurteilung jederzeit wieder in den Status "angelegt" rückführen und die Beurteilung bearbeiten. Nach erfolgter zweiter Kollationierung war eine Veränderung der Beurteilungen nicht mehr möglich. Nach Ablauf der gesetzlichen Einspruchsfrist der Beurteilungen wurde der Status dieser automatisch von "kollationiert 2" auf "gefertigt" geändert.

Sobald eine Beurteilung in den Status "kollationiert 2" überführt wurde, war das Drucken des Originalzeugnisses (Schulnachricht, Jahreszeugnis bzw. Beurteilungsvorschlag) möglich. Diese Funktion konnte wie auch das Eintragen der Beurteilungen nur von den Schulleitungen und deren Stellvertretungen, den Klassenvorständen sowie den Zeugnisverantwortlichen ausgeführt werden. Der Zeugnisdruck war ausschließlich im Sicherheitslevel 3 möglich und somit eine Authentifizierung über ein sicheres Netzwerk mittels Benutzendenname, Passwort und Token erforderlich.

5.2 Nachvollziehbarkeit des Prozesses

5.2.1 Im Rahmen der gegenständlichen Prüfung war vorgesehen, mit Hilfe der Methode des Prozess Minings zu analysieren, ob die tatsächliche Prozessabwicklung im Rahmen der Erstellung von Zeugnissen den Soll-Vorgaben entsprach. Dazu war geplant auf Basis der im Schulverwaltungsprogramm "WiSion" aufgezeichneten Ereignisse die real abgelaufenen Prozesse zu rekonstruieren und die gesamten zur Verfügung stehenden Daten zu analysieren.

Im Zuge der Datenerhebung wurde festgestellt, dass die Zeugniserstellungsprozesse im Schulverwaltungsprogramm "WiSion" bislang nicht im Detail aufgezeichnet wurden. Verspeichert wurde das Datum der Zeugnisanlage und welche Person für die zweite Kollationierung vorgesehen war. Wer, wann welche Note eingetragen hatte, wann und durch wen die erste Kollationierung erfolgte sowie wann und durch wen die zweite Kol-

lationierung und somit die Bestätigung der Ordnungsmäßigkeit der Zeugnisinformationen tatsächlich durchgeführt wurde, war hingegen nicht nachvollziehbar.

Von der Magistratsabteilung 56 wurde noch während der Prüfung des Stadtrechnungshofes Wien die Aktivierung eines Loggings des Zeugniserstellungsprozesses bis inkl. der zweiten Kollationierung veranlasst. Die Loggingdaten wurden dabei in einer Logging-Datenbank verspeichert und waren zum Prüfungszeitpunkt für die Magistratsabteilung 56 nicht direkt zugänglich.

Der Stadtrechnungshof Wien empfahl der Magistratsabteilung 56, unter Berücksichtigung von Kosten-Nutzen-Überlegungen die Möglichkeiten zur Auswertung, Extraktion und Prüfung der Loggingdaten (Eventdaten) des Zeugniserstellungsprozesses zu evaluieren und dadurch die Nachvollziehbarkeit der Erstellung von Zeugnissen sicherzustellen.

Der Stadtrechnungshof Wien empfahl der Magistratsabteilung 01, die Magistratsabteilung 56 bei der Evaluierung der Möglichkeiten zur Auswertung, Extraktion und Prüfung der Loggingdaten (Eventdaten) des Zeugniserstellungsprozesses unter Berücksichtigung von Kosten-Nutzen-Überlegungen hinsichtlich der Sicherstellung der Nachvollziehbarkeit bei der Erstellung von Zeugnissen zu unterstützen. Die entsprechenden Ressourcen wären bereitzustellen.

5.2.2 In der Bereitstellung von Loggingdaten (Eventdaten) des Zeugniserstellungsprozesses des Schulverwaltungsprogramms "WiSion" war vom Stadtrechnungshof Wien ein Zusammenhang zum Programm zur Einführung von Data Excellence Services zu erkennen bzw. herzustellen.

Das Ziel dieses Programms war es sämtliche organisatorische und technische Maßnahmen zur Etablierung eines sicheren, transparenten, effizienten und qualitätsgesicherten Umganges mit Daten der Stadt Wien bereitzustellen ("Data Excellence in der Stadt Wien").

Das Programm wurde am 30. Juni 2018 abgeschlossen und die Organisation der "Data Excellence" in den regulären Betrieb übergeben.

In diesem Programm übernahm die Magistratsabteilung 01 mit dem Fachbereich "Data Excellence" folgende Aufgaben:

- Datenverständnis,
- Datenbereinigung,
- Datenanreichung,
- Datenbereitstellung.

In diesem Zusammenhang wird vom Stadtrechnungshof Wien auf die Stellungnahme der Magistratsabteilung 14 zu Empfehlung Nr. 1 der Maßnahmenbekanntgabe zu MA 14, Servicemanagement, StRH I - 13/16 (Zl. MA 14 - 819776 - 2016 - 13) verwiesen.

Im Pkt. 3 der Stellungnahme zur Umsetzung der Empfehlung Nr. 1 wurde von der Magistratsabteilung 14 Folgendes angeführt:

"3. Die Integration der Daten in Data Excellence und der damit einhergehenden Onlineverfügbarkeit von Prozessdaten erfolgt seitens des Fachbereichs Data Excellence entsprechend der Priorisierung gemäß Bedarfsmanagementprozess. Die Umsetzung der Maßnahme (Teil 1 und Teil 2) wurde seitens des Fachbereichs Data Excellence initiiert. Die eigentliche Maßnahmenerledigung kann nur nach und nach bei der Umsetzung neuer Anwendungen und Prozesse stattfinden. Es handelt sich um eine Empfehlung, die nur langfristig, durch Änderung des Softwareentwicklungsprozesses umgesetzt werden kann. Die notwendigen Änderungen wurden seitens des Fachbereichs Data Excellence initiiert und in die Ziele für das Jahr 2018 der Magistratsabteilung 14 verankert. Die Umsetzung der Maßnahme (Teil 3) wurde im Bedarfsmanagementprozess verankert. Die Integration der verfügbaren Prozessdaten in Data Excellence ist von der Priorisierung sowie von den Ressourcen/Budget abhängig."

Der Stadtrechnungshof Wien empfahl der Magistratsabteilung 01, im Rahmen des Bedarfsmanagementprozesses von Data Excellence die Bereitstellung von Prozessdaten (Loggingdaten bzw. Eventdaten) des Zeugniserstellungsprozesses des Schulverwaltungsprogramms "WiSion" zu evaluieren.

6. Zusammenfassung der Empfehlungen

Empfehlungen an die Magistratsabteilung 56

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 (s. Pkt. 3.1).

Stellungnahme der Magistratsabteilung 56:

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.

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 (s. Pkt. 3.2).

Stellungnahme der Magistratsabteilung 56:

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.

Empfehlung Nr. 3:
Regelmäßige Kontrollen der Loggingdateien über die manuelle Anlage und Löschung von Benutzendenkonten im Schulverwaltungsprogramm "WiSion" sind im Vieraugenprinzip durchzuführen (s. Pkt. 3.3.3).

Stellungnahme der Magistratsabteilung 56:
Die Empfehlung wird einmal jährlich - beginnend mit dem Jahr 2019 - in Kooperation mit dem Stadtschulrat für Wien (künftig Bildungsdirektion) umgesetzt und dokumentiert werden.

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 (s. Pkt. 3.4.1).

Stellungnahme der Magistratsabteilung 56:
Die Empfehlung wird einmal jährlich - beginnend mit dem Jahr 2019 - in Kooperation mit dem Stadtschulrat für Wien (künftig Bildungsdirektion) umgesetzt und dokumentiert werden.

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 (s. Pkt. 3.4.2).

Stellungnahme der Magistratsabteilung 56:

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.

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 (s. Pkt. 3.4.3).

Stellungnahme der Magistratsabteilung 56:

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.

Empfehlung Nr. 7:

Regelmäßige Kontrollen der Loggingdateien der Berechtigungsvergabe sind im Vieraugenprinzip mit dem Stadtschulrat für Wien durchzuführen (s. Pkt. 3.5.1).

Stellungnahme der Magistratsabteilung 56:

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

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 (s. Pkt. 3.5.2).

Stellungnahme der Magistratsabteilung 56:
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.

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 (s. Pkt. 3.6.2).

Stellungnahme der Magistratsabteilung 56:
Die Adaptierung der Berechtigungen für alle "Administratoren" und "Superuser" wurde bereits am 14. Dezember 2017 veranlasst.

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 (s. Pkt. 4.).

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

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 (s. Pkt. 4.).

Stellungnahme der Magistratsabteilung 56:
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.

Empfehlung Nr. 12:
Es sind Maßnahmen zu evaluieren, um die Nachvollziehbarkeit von Verlusten bzw. Diebstählen von Token sowie deren etwaige Wiederbeschaffung zu gewährleisten (s. Pkt. 4.2).

Stellungnahme der Magistratsabteilung 56:
Mit dem Change Request CR_26-045 wird diese Empfehlung umgesetzt werden. Die Produktivsetzung wird voraussichtlich im Dezember 2018 erfolgen.

Empfehlung Nr. 13:
Unter Berücksichtigung von Kosten-Nutzen-Überlegungen sind die Möglichkeiten zur Auswertung, Extraktion und Prüfung der Loggingdaten (Eventdaten) des Zeugniserstel-

lungsprozesses zu evaluieren und dadurch die Nachvollziehbarkeit der Erstellung von Zeugnissen sicherzustellen (s. Pkt. 5.2.1).

Stellungnahme der Magistratsabteilung 56:

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.

Empfehlungen an die Magistratsabteilung 01

Empfehlung Nr. 1:

Die Magistratsabteilung 56 ist bei der Evaluierung der Implementierung von Audit-Berechtigungen bzw. Audit-Rollen für revisionierende Einrichtungen bei der Weiterentwicklung des Schulinformationssystems "WiSion" zu unterstützen und die entsprechenden Ressourcen sind bereitzustellen (s. Pkt. 3.1).

Stellungnahme der Magistratsabteilung 01:

Die Magistratsabteilung 01 nimmt die Empfehlung zustimmend zur Kenntnis.

Empfehlung Nr. 2:

Die Magistratsabteilung 56 ist bei der Umsetzung des Zugriffs auf die Online-Hilfe des Schulverwaltungsprogramms "WiSion" hinsichtlich der Thematik der Security, Safety und Compliance zu unterstützen und die entsprechenden Ressourcen sind bereitzustellen (s. Pkt. 3.2).

Stellungnahme der Magistratsabteilung 01:

Die Magistratsabteilung 01 nimmt die Empfehlung zustimmend zur Kenntnis.

Empfehlung Nr. 3:

Die vergebenen Administratorenberechtigungen sind regelmäßig zu evaluieren und gegebenenfalls sind nicht zwingend erforderliche Berechtigungen zu entfernen (s. Pkt. 3.4.2).

Stellungnahme der Magistratsabteilung 01:
Die Magistratsabteilung 01 nimmt die Empfehlung zustimmend zur Kenntnis.

Empfehlung Nr. 4:
Die Magistratsabteilung 56 ist in der Thematik der Security, Safety und Compliance bei der durchzuführenden Risikoanalyse und der Evaluierung von zu setzenden Maßnahmen hinsichtlich der Nachvollziehbarkeit der Aktivitäten der "Superuser" und der "Administratoren" zu unterstützen. Die entsprechenden Ressourcen sind bereitzustellen (s. Pkt. 3.4.3).

Stellungnahme der Magistratsabteilung 01:
Die Magistratsabteilung 01 nimmt die Empfehlung zustimmend zur Kenntnis.

Empfehlung Nr. 5:
Die Magistratsabteilung 56 ist bei der Evaluierung des Ablaufdiagramms über die Tokenverwaltung bzw. den Lebenszyklus eines Tokens und der Sicherstellung der Dokumentation der realen Prozessabläufe zu unterstützen und die entsprechenden Ressourcen sind bereitzustellen (s. Pkt. 4.).

Stellungnahme der Magistratsabteilung 01:
Die Magistratsabteilung 01 nimmt die Empfehlung zustimmend zur Kenntnis.

Empfehlung Nr. 6:
Die Magistratsabteilung 56 ist bei der Evaluierung der Tokenverwaltung hinsichtlich der Übereinstimmung von Daten bzw. Statuszuweisungen im Schulverwaltungsprogramm "WiSion" und dem Informationssystem "Identity Guard" zu unterstützen und die entsprechenden Ressourcen sind bereitzustellen (s. Pkt. 4.).

Stellungnahme der Magistratsabteilung 01:
Die Magistratsabteilung 01 nimmt die Empfehlung zustimmend zur Kenntnis.

Empfehlung Nr. 7:
Eine regelmäßige Kontrolle der Token des Informationssystems "Identity Guard" ist in der Verwaltung und Verwendung mit dem Schulverwaltungsprogramm "WiSion" im Vieraugenprinzip mit der Magistratsabteilung 56 bzw. dem Stadtschulrat für Wien zu evaluieren (s. Pkt. 4.).

Stellungnahme der Magistratsabteilung 01:
Die Magistratsabteilung 01 nimmt die Empfehlung zustimmend zur Kenntnis.

Empfehlung Nr. 8:
Die Magistratsabteilung 56 ist bei der Evaluierung der Möglichkeiten zur Auswertung, Extraktion und Prüfung der Loggingdaten (Eventdaten) des Zeugniserstellungsprozesses hinsichtlich der Sicherstellung der Nachvollziehbarkeit bei der Erstellung von Zeugnissen unter Berücksichtigung von Kosten-Nutzen-Überlegungen zu unterstützen. Die entsprechenden Ressourcen sind bereitzustellen (s. Pkt. 5.2.1).

Stellungnahme der Magistratsabteilung 01:
Die Magistratsabteilung 01 nimmt die Empfehlung zustimmend zur Kenntnis.

Empfehlung Nr. 9:
Die Bereitstellung von Prozessdaten (Logging- bzw. Eventdaten) des Zeugniserstellungsprozesses des Schulverwaltungsprogramms "WiSion" im Rahmen des Bedarfsmanagementprozesses von Data Excellence ist zu evaluieren (s. Pkt. 5.2.2).

Stellungnahme der Magistratsabteilung 01:

Die Magistratsabteilung 01 nimmt die Empfehlung zustimmend zur Kenntnis.

Der Stadtrechnungshofdirektor:

Dr. Peter Pollak, MBA

Wien, im November 2018