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
DVR: 0000191

StRH I - 23/17

MA 14, Prüfung der IKT-Sicherheit

von ausgelagerten Bereichen

Prüfung der Maßnahmenbekanntgabe

KURZFASSUNG

Der Stadtrechnungshof Wien prüfte die Umsetzung der im Oktober 2016 veröffentlichten Maßnahmenbekanntgabe, die von der Magistratsabteilung 14 zum ursprünglichen Bericht (siehe Tätigkeitsbericht 2015, MA 14, Prüfung der IKT-Sicherheit von ausgelagerten Bereichen; StRH I - 14 -1/15), abgegeben wurde.

Dabei war festzustellen, dass der in der Maßnahmenbekanntgabe geäußerte Stand der Umsetzung bei sieben Empfehlungen mit dem Prüfungsergebnis des Stadtrechnungshofes Wien übereinstimmte. Ferner waren fünf als "in Umsetzung" gemeldete Empfehlungen zwischenzeitlich bereits umgesetzt.

Bei der Vor-Ort-Überprüfung von Sicherheitsmaßnahmen in Räumlichkeiten der IKT-Infrastruktur waren Verbesserungen durch den Stadtrechnungshof Wien erkennbar, die zu einer neuen auszusprechenden Empfehlung hinsichtlich der Evaluierung des Intervalls der Sicherheitsbegehungen führten.

INHALTSVERZEICHNIS

ABKÜRZUNGSVERZEICHNIS

Abs.	Absatz
AGB	Allgemeine Geschäftsbedingungen
AKH	Allgemeines Krankenhaus der Stadt Wien - Medizinischer Universitätscampus
bzgl.	bezüglich
bzw.	beziehungsweise
CERT	Computer Emergency Response Team
d.h.	das heißt

EDV ..... Elektronische Datenverarbeitung
E-Mail ..... Elektronische Post
gem..... gemäß
https..... Hypertext Transfer Protocol Secure
IKT..... Informations- und Kommunikationstechnologie
lt..... laut
MA ..... Magistratsabteilung
Nr..... Nummer
Pkt. ..... Punkt
s..... siehe
Serviceeinheit
Informationstechnologie..... KAV-Informationstechnologie
StRH..... Stadtrechnungshof
u.a. ..... unter anderem
WStV ..... Wiener Stadtverfassung
www..... World Wide Web
z.B. ..... zum Beispiel
z.T. ..... zum Teil

GLOSSAR

"Normatage"
Sind jene Tage, an denen die Soll-Arbeitszeit viereinhalb Stunden beträgt (Karfreitag sowie 24. und 31. Dezember).

PRÜFUNGSERGEBNIS

Die Abteilung Kultur und Bildung des Stadtrechnungshofes Wien unterzog die Maßnahmenbekanntgabe der Magistratsabteilung 14, Prüfung der IKT-Sicherheit von ausgelagerten Bereichen einer stichprobenweisen Prüfung und teilte das Ergebnis seiner Wahrnehmungen nach Abhaltung einer diesbezüglichen Schlussbesprechung der geprüften Stelle mit. Die von der geprüften Stelle abgegebene Stellungnahme wurde berücksichtigt. Allfällige Rundungsdifferenzen bei der Darstellung von Berechnungen wurden nicht ausgeglichen.

1. Bekannt gegebener Umsetzungsstand

Im Rahmen der Äußerung der Magistratsabteilung 14 wurde von der geprüften Stelle folgende Umsetzung in Bezug auf die ergangenen Empfehlungen bekannt gegeben:

Stand der Umsetzung der Empfehlungen lt. Maßnahmenbekanntgabe	Anzahl	Anteil an Gesamt in %
Gesamt	12	100,0
Umgesetzt	7	58,3
In Umsetzung	5	41,7
Geplant	-	-
Nicht geplant	-	-

Die von der geprüften Stelle bekannt gegebenen Umsetzungen der Empfehlungen wurden im Bericht des Stadtrechnungshofes Wien am 7. Oktober 2016 veröffentlicht und im Rahmen der Sitzung des Stadtrechnungshofausschusses vom 14. Oktober 2016, Ausschusszahl 42/15 zur Kenntnis genommen.

2. Umsetzungsstand laut Prüfungsergebnis

Die Prüfung durch den Stadtrechnungshof Wien bezog sich ausschließlich auf den Inhalt der Empfehlungen lt. Maßnahmenbekanntgabe und war somit keine umfassende Nachprüfung.

Folgender Stand der Umsetzung der Empfehlungen wurde festgestellt:

Stand der Umsetzung der Empfehlungen lt. Prüfung	Anzahl	Anteil an Gesamt in %
Gesamt	12	100,0
Umgesetzt	12	100,0
In Umsetzung	-	-
Geplant	-	-
Nicht geplant	-	-

Von den insgesamt zwölf Empfehlungen waren alle umgesetzt.

Der bekannt gegebene Stand der Umsetzung verbesserte sich bei fünf Empfehlungen und stimmte bei den sieben weiteren Empfehlungen mit dem Prüfungsergebnis des Stadtrechnungshofes Wien überein.

Die nachfolgende Tabelle zeigt die angesprochenen Übereinstimmungen bzw. Abweichungen bei der Beurteilung des Standes der Umsetzungen (von der geprüften Stelle bekannt gegebene Umsetzungen "**X**"; vom Stadtrechnungshof Wien festgestellte Umsetzungen "**O**"):

Empfehlungen	umgesetzt	in Umsetzung	geplant	nicht geplant
Empfehlung Nr. 1	**O**	**X**		
Empfehlung Nr. 2	**O**	**X**		
Empfehlung Nr. 3	**O**	**X**		
Empfehlung Nr. 4	**O**	**X**		
Empfehlung Nr. 5	**O**	**X**		
Empfehlung Nr. 6	**X O**			
Empfehlung Nr. 7	**X O**			
Empfehlung Nr. 8	**X O**			
Empfehlung Nr. 9	**X O**			
Empfehlung Nr. 10	**X O**			
Empfehlung Nr. 11	**X O**			
Empfehlung Nr. 12	**X O**			

3. Bekannt gegebener Umsetzungsstand im Einzelnen versus Prüfungsergebnis

In den nachfolgenden Punkten wird das Ergebnis der Prüfung des von der geprüften Stelle bekannt gegebenen Umsetzungsstandes im Einzelnen dargestellt. Dabei wurden

die bisher erfolgten Empfehlungen, Stellungnahmen, allfällige Gegenäußerungen sowie die Begründungen bzw. Erläuterungen der Maßnahmenbekanntgabe berücksichtigt.

Anzumerken ist, dass die Magistratsabteilung 14 im Rahmen ihrer internen Maßnahmenverfolgung noch während der Prüfung des Stadtrechnungshofes Wien die vollständige Umsetzung aller Empfehlungen bekannt gab. Eine aktualisierte Stellungnahme zum Umsetzungsstand der Empfehlungen wurde daher vor der konkreten Einschau in die Umsetzung der einzelnen Empfehlungen an den Stadtrechnungshof Wien zur Information übermittelt. Die Inhalte dieser Stellungnahme wurden im gegenständlichen Prüfungsbericht berücksichtigt, jedoch nicht gesondert bei den einzelnen Empfehlungen angeführt.

3.1 Empfehlung Nr. 1

Der Stadtrechnungshof Wien empfahl, den IKT-Erlass insofern zu hinterfragen, ob weitere explizite Anordnungen für die Unternehmungen, Stadt Wien - Wiener Wohnen und Wien Kanal, nach dem IKT-Erlass erforderlich wären.

Stellungnahme der geprüften Stelle:

Die erforderlichen Maßnahmen und Termine werden ehestmöglich mit den dafür Verantwortlichen abgestimmt.

Maßnahmenbekanntgabe der geprüften Stelle:

Die Empfehlung befindet sich in Umsetzung.

Mit Schreiben vom 28. Mai 2015 fragte die Magistratsabteilung 14 bei der Magistratsdirektion - Geschäftsbereich Organisation und Sicherheit, Gruppe Organisation sowie Gruppe Prozessmanagement und IKT-Strategie im Sinn der Empfehlung des Stadtrechnungshofes Wien bzgl. der Interpretation des Erlasses an. Am 27. August 2015 fand dazu auf Einladung der Gruppe Prozessmanagement und IKT-Strategie eine Besprechung statt, bei der vereinbart wurde, dass die Gruppe Organisation der Magistratsdirektion diese Frage prüfen wird. Dort ist das Thema in Bearbeitung.

Ergebnis der Prüfung des Stadtrechnungshofes Wien:
Die ursprünglich als in Umsetzung bekannt gegebene Empfehlung wurde bereits umgesetzt.

Die Magistratsdirektion - Geschäftsbereich Organisation und Sicherheit, Gruppe Organisation sowie Gruppe Prozessmanagement und IKT-Strategie wurde von der Magistratsabteilung 14 um Unterstützung bei der richtigen Interpretation des Anwendungsbereiches des IKT-Erlasses ersucht. Die Anfrage wurde an die Magistratsdirektion - Geschäftsbereich Recht weitergeleitet, die mit Schreiben vom 29. Oktober 2015 klarstellte, dass der Erlass an alle städtischen Dienststellen gerichtet sei.

Gemäß § 3 Abs. 1 der Geschäftsordnung für den Magistrat der Stadt Wien waren die Magistratsdirektion, die Magistratsabteilungen, die Magistratischen Bezirksämter und der Stadtrechnungshof Wien sowie die Unternehmungen Wiener Krankenanstaltenverbund, Stadt Wien - Wiener Wohnen und Wien Kanal als städtische Dienststellen zu werten. Nach § 3 Abs. 2 der Geschäftsordnung für den Magistrat der Stadt Wien galten die Wiener Kinder- und Jugendanwaltschaft, die Wiener Pflege-, Patientinnen- und Patientenanwaltschaft, die Stelle des Tierschutzombudsmannes, die Umweltanwaltschaft und die Stelle des bzw. der Unabhängigen Bedienstetenschutzbeauftragten ebenfalls als Dienststellen im Sinn des Abs. 1.

Aufgrund der Rückmeldung der Magistratsdirektion - Geschäftsbereich Recht sah die Magistratsabteilung 14 keine Erfordernisse für explizite Anordnungen für die Unternehmungen Stadt Wien - Wiener Wohnen und Wien Kanal und der Erlass war somit direkt anzuwenden.

3.2 Empfehlung Nr. 2

Der Stadtrechnungshof Wien empfahl, die zur Klärung der Anwendbarkeit des Geltungsbereiches des IKT-Erlasses bei den Kundinnen bzw. Kunden, welche nicht als Teil des Magistrats der Stadt Wien anzusehen sind, notwendige Schritte einzuleiten, um damit die durchgängige und ganzheitliche IKT-Sicherheit zu gewährleisten.

Stellungnahme der geprüften Stelle:
Die erforderlichen Maßnahmen und Termine werden ehestmöglich mit den dafür Verantwortlichen abgestimmt.

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

Mit Schreiben vom 28. Mai 2015 fragte die Magistratsabteilung 14 bei der Magistratsdirektion - Geschäftsbereich Organisation und Sicherheit, Gruppe Organisation sowie Gruppe Prozessmanagement und IKT-Strategie im Sinn der Empfehlung des Stadtrechnungshofes Wien bzgl. der Interpretation des Erlasses an. Am 27. August 2015 fand dazu auf Einladung der Gruppe Prozessmanagement und IKT-Strategie eine Besprechung statt, bei der vereinbart wurde, dass die Gruppe Organisation der Magistratsdirektion diese Frage prüfen wird. Dort ist das Thema in Bearbeitung.

Ergebnis der Prüfung des Stadtrechnungshofes Wien:
Die ursprünglich als in Umsetzung bekannt gegebene Empfehlung wurde bereits umgesetzt.

Die Magistratsdirektion - Geschäftsbereich Organisation und Sicherheit, Gruppe Organisation sowie Gruppe Prozessmanagement und IKT-Strategie wurde von der Magistratsabteilung 14 um Unterstützung bei der richtigen Interpretation des Anwendungsbereiches des IKT-Erlasses ersucht. Die Anfrage wurde an die Magistratsdirektion - Geschäftsbereich Recht weitergeleitet, die mit Schreiben vom 29. Oktober 2015 klarstellte, dass der Erlass an alle städtischen Dienststellen gerichtet sei.

Gemäß § 3 Abs. 1 der Geschäftsordnung für den Magistrat der Stadt Wien waren die Magistratsdirektion, die Magistratsabteilungen, die Magistratischen Bezirksämter und der Stadtrechnungshof Wien sowie die Unternehmungen Wiener Krankenanstaltenverbund, Stadt Wien - Wiener Wohnen und Wien Kanal als städtische Dienststellen zu wer-

ten. Nach § 3 Abs. 2 der Geschäftsordnung für den Magistrat der Stadt Wien galten die Wiener Kinder- und Jugendanwaltschaft, die Wiener Pflege-, Patientinnen- und Patientenanwaltschaft, die Stelle des Tierschutzombudsmannes, die Umweltanwaltschaft und die Stelle des bzw. der Unabhängigen Bedienstetenschutzbeauftragten ebenfalls als Dienststellen im Sinn des Abs. 1.

Alle anderen Stellen, die keine Dienststellen gem. § 3 der Geschäftsordnung für den Magistrat der Stadt Wien oder keine Unternehmung nach § 71 WStV waren, waren entsprechend der Definition im Erlass als "externe Stellen" zu qualifizieren. Für diese "externen Stellen" war die Einhaltung des Erlasses vertraglich sicherzustellen, da dieser nicht unmittelbar anzuwenden war.

Die vertraglichen Bedingungen für externe Kundinnen bzw. Kunden der Magistratsabteilung 14 wurden in den "IKT-Sicherheitsrichtlinien für externe KundInnen" festgelegt.

3.3 Empfehlung Nr. 3

Der Stadtrechnungshof Wien empfahl, den Vertrag über die Erbringung von Internet Service Provider Diensten einer externen Kundin, welcher vom Standardvertrag abwich, auf Regelungen des aktuellen technischen Standes zur IKT-Sicherheit zu evaluieren und diese erforderlichenfalls entsprechend vertraglich abzusichern.

Stellungnahme der geprüften Stelle:

Die erforderlichen Maßnahmen und Termine werden ehestmöglich mit den dafür Verantwortlichen abgestimmt.

Maßnahmenbekanntgabe der geprüften Stelle:

Die Empfehlung befindet sich in Umsetzung.

Es wurden "Allgemeine Geschäftsbedingungen für die Bereitstellung von Internet und Kommunikationsdiensten (E-Mail, Telefonie) durch die Magistratsabteilung 14" ausgearbeitet, welche mit jenen Kundinnen bzw. Kunden vereinbart werden sollen, die nicht an Erlässe des Magistrats der Stadt Wien

gebunden sind. Die Allgemeinen Geschäftsbedingungen beinhalten Hinweise zur rechtskonformen Nutzung, den Schutz der Zugangsdaten, die Verantwortung für missbräuchliche oder betriebsgefährdende Nutzung sowie die Durchsetzung und Abwehr von Rechtsansprüchen gegenüber Dritten.

Ergebnis der Prüfung des Stadtrechnungshofes Wien:
Die ursprünglich als in Umsetzung bekannt gegebene Empfehlung wurde bereits umgesetzt.

Die "Allgemeinen Geschäftsbedingungen für die Bereitstellung von Internet und Kommunikationsdiensten (z.B. E-Mail, Telefonie) durch die Magistratsabteilung 14" wurden am 9. Juni 2016 freigegeben. Darin waren u.a. Regelungen zur rechtskonformen Nutzung, Datenschutz, Schutz der Zugangsdaten und Haftung für missbräuchliche Verwendung sowie betriebsgefährdende Nutzungen enthalten.

Die AGB's waren von Neukundinnen bzw. Neukunden bereits zu Beginn der Leistungsbeziehung zu unterfertigen. Für die bestehenden Kundinnen bzw. Kunden lagen zum Prüfungszeitpunkt z.T. bereits unterfertigte AGB's vor, die noch ausstehenden Unterschriften wurden nach und nach eingeholt.

3.4 Empfehlung Nr. 4

Der Stadtrechnungshof Wien empfahl zu evaluieren, ob die IKT-Sicherheit für die erbrachten IKT-Leistungen der Datenübermittlung an eine externe Kundin durch schriftliche Vereinbarungen sicherzustellen wäre.

Stellungnahme der geprüften Stelle:
Die erforderlichen Maßnahmen und Termine werden ehestmöglich mit den dafür Verantwortlichen abgestimmt.

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

Bezüglich der Übermittlungen der Sterbedaten an die "Friedhöfe Wien" im Weg einer definierten Nahtstellenstruktur (Zentrales Melderegister) erging eine Anfrage an die Magistratsabteilung 26 als auftraggebende Stelle im Sinn des Datenschutzerlasses: Inwieweit eine entsprechende Datenschutzvereinbarung vorliegt bzw. abzuschließen wäre und ob die Datenübermittlung auch noch durch eine gesonderte schriftliche Vereinbarung sicherzustellen wäre. Die Magistratsabteilung 26 ist seit 2015 auch inhaltlich für die Standesämter und somit auch für die Übermittlung der Sterbedaten verantwortlich. Die Anfrage blieb bis dato ohne Ergebnis.

Ergebnis der Prüfung des Stadtrechnungshofes Wien:

Die ursprünglich als in Umsetzung bekannt gegebene Empfehlung wurde bereits umgesetzt.

Am 6. Mai 2015 wurde von der Magistratsabteilung 14 bei der Magistratsabteilung 26 angefragt, ob für die Übermittlung der Sterbedaten an die "Friedhöfe Wien" eine entsprechende Datenschutzvereinbarung vorliegt bzw. abzuschließen wäre. Ferner war zu klären, ob die Datenübermittlung auch noch durch eine gesonderte schriftliche Vereinbarung sicherzustellen wäre. Mit Schreiben vom 9. September 2015 wurde diesbezüglich rückgemeldet, dass die Übermittlung der Sterbedaten erneut hinsichtlich Zweck und Rechtsgrundlage zu prüfen und allenfalls eine schriftliche Vereinbarung abzuschließen wäre. Dafür war jedoch ein Antrag der "Friedhöfe Wien" erforderlich.

Die "Friedhöfe Wien" wurden von der Magistratsabteilung 14 aufgefordert einen entsprechenden Antrag an die Magistratsabteilung 26 zu stellen. Ferner wurde mitgeteilt, dass der Service eingestellt werden müsste, sofern nicht bis zum 19. September 2016 ein genehmigter Antrag der Magistratsabteilung 26 vorlag.

Die "Friedhöfe Wien" stellten in weiterer Folge einen entsprechenden Antrag auf Genehmigung der Beibehaltung des Services der Magistratsabteilung 14. Seitens der Magistratsabteilung 26 bestanden in Folge keine Einwendungen gegen eine Beibehaltung der Services. Der Abschluss einer gesonderten Datenschutzvereinbarung wurde als

nicht erforderlich erachtet, da die übermittelten Daten als datenschutzrechtlich nicht relevant eingestuft wurden.

3.5 Empfehlung Nr. 5

Der Stadtrechnungshof Wien empfahl, eine neuerliche Prüfung aller Kundinnen bzw. Kunden betreffend deren genauen Zuordnungen zu den beiden Kundenbereichen (intern bzw. extern) zu evaluieren, um damit die IKT-Sicherheit durch entsprechende Regelungen bestmöglich zu gewährleisten.

Stellungnahme der geprüften Stelle:

Die erforderlichen Maßnahmen und Termine werden ehestmöglich mit den dafür Verantwortlichen abgestimmt.

Maßnahmenbekanntgabe der geprüften Stelle:

Die Empfehlung befindet sich in Umsetzung.

Mit Schreiben vom 28. Mai 2015 fragte die Magistratsabteilung 14 bei der Magistratsdirektion - Geschäftsbereich Organisation und Sicherheit, Gruppe Organisation sowie Gruppe Prozessmanagement und IKT-Strategie im Sinn der Empfehlung des Stadtrechnungshofes Wien bzgl. der Zuordnung zu den unterschiedlichen Kundenbereichen an. Am 27. August 2015 fand dazu auf Einladung der Gruppe Prozessmanagement und IKT-Strategie eine Besprechung statt, bei der vereinbart wurde, dass die Gruppe Organisation der Magistratsdirektion das Thema prüfen wird. Dort ist das Thema in Bearbeitung.

Ergebnis der Prüfung des Stadtrechnungshofes Wien:

Die ursprünglich als in Umsetzung bekannt gegebene Empfehlung wurde bereits umgesetzt.

Die Magistratsdirektion - Geschäftsbereich Organisation und Sicherheit, Gruppe Organisation sowie Gruppe Prozessmanagement und IKT-Strategie wurde von der Magist-

ratsabteilung 14 um Unterstützung bei der richtigen Interpretation des Anwendungsbereiches des IKT-Erlasses ersucht.

Im Antwortschreiben der Magistratsdirektion - Geschäftsbereich Recht vom 29. Oktober 2016 wurde ausgeführt, dass "externe Stellen" im Sinn des Erlasses alle Stellen waren, die weder Dienststelle gem. § 3 der Geschäftsordnung für den Magistrat der Stadt Wien noch Unternehmung gem. § 71 WStV sind.

Gemäß § 3 Abs. 1 der Geschäftsordnung für den Magistrat der Stadt Wien waren die Magistratsdirektion, die Magistratsabteilungen, die Magistratischen Bezirksämter und der Stadtrechnungshof Wien sowie die Unternehmungen Wiener Krankenanstaltenverbund, Stadt Wien - Wiener Wohnen und Wien Kanal als städtische Dienststellen zu werten. Nach § 3 Abs. 2 der Geschäftsordnung für den Magistrat der Stadt Wien galten die Wiener Kinder- und Jugendanwaltschaft, die Wiener Pflege-, Patientinnen- und Patientenanwaltschaft, die Stelle des Tierschutzombudsmannes, die Umweltanwaltschaft und die Stelle des bzw. der Unabhängigen Bedienstetenschutzbeauftragten ebenfalls als Dienststellen im Sinn des Abs. 1.

Alle anderen Stellen, die keine Dienststellen gem. § 3 der Geschäftsordnung für den Magistrat der Stadt Wien oder keine Unternehmung nach § 71 WStV waren, waren entsprechend der Definition im Erlass als "externe Stellen" zu qualifizieren. Für diese "externen Stellen" war die Einhaltung des Erlasses vertraglich sicherzustellen, da dieser nicht unmittelbar anzuwenden war.

3.6 Empfehlung Nr. 6

Der Stadtrechnungshof Wien empfahl, insbesondere bei externen Kundinnen bzw. Kunden die Thematik der IKT-Sicherheit durch eine gut vernetzte Kundinnen- bzw. Kundenbeziehung zu intensivieren sowie durch eine größtmögliche fachliche Unterstützung, wie z.B. durch regelmäßige Beratungs- bzw. Qualitätssicherungsgespräche, zur Aufrechterhaltung der maximal möglichen IKT-Sicherheit beizutragen.

Stellungnahme der geprüften Stelle:
Die erforderlichen Maßnahmen und Termine werden ehestmöglich mit den dafür Verantwortlichen abgestimmt.

Maßnahmenbekanntgabe der geprüften Stelle:
Die Empfehlung wurde umgesetzt.

In der Magistratsabteilung 14 wurde ein Beratungsprozess eingeführt, welcher regelmäßigen persönlichen Kontakt mit den Kundinnen bzw. Kunden vorsieht (mindestens einmal pro Monat). Die Key Account Managerin bzw. der Key Account Manager als Hauptansprechperson der Kundinnen bzw. Kunden bespricht auch laufend Themen rund um die Sicherheit. Zusätzlich werden seitens der Magistratsabteilung 14 auch laufend Publikationen zum Thema "IKT-Sicherheit" veröffentlicht und den Kundinnen bzw. Kunden angeboten.

Ergebnis der Prüfung des Stadtrechnungshofes Wien:
Der von der geprüften Stelle bekannt gegebene Umsetzungsstand entsprach dem Ergebnis der Prüfung.

Seitens der Magistratsabteilung 14 wurden Maßnahmen gesetzt, um das Thema Sicherheit zu intensivieren. Beispielsweise wurde festgelegt, dass - wie in der Stellungnahme der Magistratsabteilung 14 angeführt wurde - regelmäßige Abstimmungen der Key Account Manager mit den Ansprechpersonen in den Dienststellen und zumindest zweimal im Jahr ein umfassendes Abstimmungsgespräch stattzufinden hatten.

In Bezug auf die laufenden Publikationen der Magistratsabteilung 14 zum Thema "IKT-Sicherheit" konnte festgestellt werden, dass im Intranet der Stadt Wien verschiedene Inhalte und Beiträge zum Thema IKT-Sicherheit sowie anlassbezogen Warnungen über beispielsweise Pishing-Mails veröffentlicht wurden. Auch im Newsletter der Magistratsabteilung 14 wurden verstärkt Sicherheitsthemen platziert.

3.7 Empfehlung Nr. 7

Der Stadtrechnungshof Wien empfahl, ein Dokument der IKT-Sicherheitsrichtlinien auf Aktualität zu überprüfen.

Stellungnahme der geprüften Stelle:
Die erforderlichen Maßnahmen und Termine werden ehestmöglich mit den dafür Verantwortlichen abgestimmt.

Maßnahmenbekanntgabe der geprüften Stelle:
Die Empfehlung wurde umgesetzt.

Die Planungsunterlage "Ausstattungsbeschreibung Objektinfrastruktur" wurde aktualisiert und im Intranet veröffentlicht.

Ergebnis der Prüfung des Stadtrechnungshofes Wien:
Der von der geprüften Stelle bekannt gegebene Umsetzungsstand entsprach dem Ergebnis der Prüfung.

Das Dokument der IKT-Sicherheitsrichtlinie aus dem Jahr 2009 wurde am 2. Juni 2015 überprüft und war im Intranet der Stadt Wien abrufbar.

3.8 Empfehlung Nr. 8

Der Stadtrechnungshof Wien empfahl, die erstmalig aufgrund des IKT-Sicherheitserlasses unterzeichneten Vereinbarungen zum Anlass zu nehmen, einen ersten Schwerpunkt - im Sinn eines Beratungs- bzw. Qualitätssicherungsgespräches zur IKT-Sicherheit - bei den externen Kundinnen bzw. Kunden zu setzen.

Stellungnahme der geprüften Stelle:
Die erforderlichen Maßnahmen und Termine werden ehestmöglich mit den dafür Verantwortlichen abgestimmt.

Maßnahmenbekanntgabe der geprüften Stelle:
Die Empfehlung wurde umgesetzt.

Der Prozess für die Sicherheitsbegehungen ist eingerichtet. Es wurden in den Jahren 2014 und 2015 bereits an neun Standorten von externen Kundinnen bzw. Kunden Begehungen durchgeführt. Grundsätzlich handelt es sich um einen laufenden Prozess, d.h. die Begehungen werden in regelmäßigen Abständen wiederholt (je nach Größe und Bedeutung der Standorte alle zwei bis drei Jahre). Für das Jahr 2016 ist geplant, alle relevanten Standorte zu begehen. Das sind Standorte mit eigenem IKT-Raum, wo die Magistratsabteilung 14 IKT-Komponenten (EDV und Telekommunikation) betreibt.

Bei den Begehungen im Beisein der Kundinnen bzw. Kunden wird eine Checkliste auf Basis der Sicherheitsrichtlinien der Magistratsabteilung 14 ausgefüllt. Gleichzeitig erfolgt eine Beratungstätigkeit für die Kundin bzw. den Kunden, vor allem zu den Themen physische Sicherheit und Betriebssicherheit in den IKT-Räumen. In der Checkliste, die gleichzeitig das Begehungsprotokoll ist, werden bei Bedarf entsprechende Umsetzungsmaßnahmen (mit Terminen) festgelegt. Dieses Protokoll wird den Kundinnen bzw. Kunden zur Umsetzung übermittelt. Die Umsetzung wird in der Magistratsabteilung 14 evident gehalten und nach Ablauf der festgelegten Frist überprüft.

Ergebnis der Prüfung des Stadtrechnungshofes Wien:
Der von der geprüften Stelle bekannt gegebene Umsetzungsstand entsprach dem Ergebnis der Prüfung.

Die Vorgehensweise bei den IKT-Sicherheitsbegehungen war in Form eines Flussdiagramms sowie einer weiterführenden Prozessbeschreibung dokumentiert. Laut der Prozessbeschreibung wurden die Kundinnen bzw. Kunden während der Begehungen auch zum Thema physische Sicherheit und Betriebssicherheit in IKT-Räumen beraten.

Vom Stadtrechnungshof Wien erfolgte eine Vor-Ort-Einschau an zwei stichprobenweise ausgewählten Standorten gemeinsam mit Vertretern der Magistratsabteilung 14.

Ein Standort betraf eine Sicherheitsbegehung einer externen Stelle, die zuletzt 2015 überprüft wurde. Auf Basis der Ergebnisse der Sicherheitsbegehung aus dem Jahr 2015 wurde eine Überprüfung der einzelnen Punkte vorgenommen. Die Überprüfung ergab in der Anzahl mehr Beanstandungspunkte als im Jahr 2015, wobei die vorgeschlagenen Maßnahmen zur Behebung aus dem Jahr 2015 nicht vollständig umgesetzt wurden. Im Gesamtergebnis lag eine deutliche Verschlechterung gegenüber dem Jahr 2015 vor.

Der zweite Standort betraf eine Sicherheitsbegehung einer Räumlichkeit der Magistratsabteilung 14 in einem Amtshaus. Vom Stadtrechnungshof Wien war festzustellen, dass die in der letzten Sicherheitsbegehung im März 2017 beanstandeten Mängel nicht zur Gänze behoben waren. Unter anderem betraf dies die Umluftanlage, welche in z.T. geöffnetem Zustand vorgefunden wurde, jedoch eine zeitnah aktuelle Prüfplakette aus dem November 2017 aufwies. Im Gesamtergebnis lag - vor allem im Vergleich zu den vorher angeführten Räumlichkeiten der externen Stelle - ein deutlich besseres Ergebnis vor.

Seitens der Magistratsabteilung 14 wurde mitgeteilt, dass die Intervalle der Sicherheitsbegehungen aufgrund der Bedeutung der Standorte unterschiedlich vorgesehen waren. Im vorliegenden Fall der Sicherheitsbegehung der Räumlichkeiten der externen Stelle, erschien dem Stadtrechnungshof Wien aufgrund der Verschlechterung des Zustandes das Intervall verbesserungswürdig.

Der Stadtrechnungshof Wien sieht die ursprünglich ausgesprochene Empfehlung als umgesetzt an, betreffend des Ergebnisses aus der Vor-Ort-Begehung wird folgende weitere Empfehlung ausgesprochen:

Der Stadtrechnungshof Wien empfahl der Magistratsabteilung 14, die Intervalle der Sicherheitsbegehungen - insbesondere bei Räumlichkeiten der externen Stellen - zu eva-

luieren und gegebenenfalls zu verdichten. Dabei sollten die Bedeutung der Standorte, die vorgefundenen Mängel und die dokumentierten Behebungsmaßnahmen aus den letzten Sicherheitsbegehungen entsprechend berücksichtigt werden.

3.9 Empfehlung Nr. 9

Der Stadtrechnungshof Wien empfahl, die Inhalte der Vereinbarung hinsichtlich der IKT-Komponenten und der Beauftragung von weiteren IKT-Dienstleisterinnen bzw. IKT-Dienstleistern durch externe Kundinnen bzw. Kunden kritisch zu hinterfragen und die dargelegten Inhalte dazu entsprechend zu evaluieren.

Stellungnahme der geprüften Stelle:

Die erforderlichen Maßnahmen und Termine werden ehestmöglich mit den dafür Verantwortlichen abgestimmt.

Maßnahmenbekanntgabe der geprüften Stelle:

Die Empfehlung wurde umgesetzt.

Die entsprechende Fach-Policy wurde überarbeitet und publiziert:
"IKT-Sicherheitsrichtlinien für externe KundInnen".

Ergebnis der Prüfung des Stadtrechnungshofes Wien:

Der von der geprüften Stelle bekannt gegebene Umsetzungsstand entsprach dem Ergebnis der Prüfung.

Die überarbeitete Fach-Policy "IKT-Sicherheitsrichtlinien für externe KundInnen" wurde am 20. Mai 2015 freigegeben und am 8. August 2016 zuletzt überprüft. Im Zuge der Einschau wurde festgestellt, dass im Pkt. "Veränderung von IKT-Komponenten" keine Änderungen vorgenommen wurden, jedoch die gegenständliche Thematik in dem neuen zusätzlichen Pkt. "Überprüfungsrecht durch die MA 14" dargelegt wurde.

In Bezug auf die Beauftragung von weiteren IKT-Dienstleisterinnen bzw. IKT-Dienstleistern wurden dahingehend Änderungen vorgenommen, dass nunmehr die Zu-

stimmung der Magistratsabteilung 14 nur unter folgender Bedingung erfolgte: Jene Bereiche waren zu vereinbaren, in denen Tätigkeiten der IKT-Dienstleisterinnen bzw. IKT-Dienstleister in Abstimmung mit der Magistratsabteilung 14 zu erfolgen hatten.

3.10 Empfehlung Nr. 10

Der Stadtrechnungshof Wien empfahl, generell in Dokumenten enthaltene Verweise auf andere bzw. weitere Vorschriften bzw. Dokumente zu präzisieren.

Stellungnahme der geprüften Stelle:

Die erforderlichen Maßnahmen und Termine werden ehestmöglich mit den dafür Verantwortlichen abgestimmt.

Maßnahmenbekanntgabe der geprüften Stelle:

Die Empfehlung wurde umgesetzt.
In den Sicherheitsvereinbarungen mit den externen Kundinnen bzw. Kunden wurden die entsprechenden Empfehlungen präzisiert und irreführende Begriffe entfernt:

https://www.intern.magwien.gv.at/ma14/ikt-sicherheit/regelungen/
Link: Anschlussbedingungen;

Publizierte Fach-Policy:
"IKT-Sicherheitsrichtlinien für externe KundInnen".

Ergebnis der Prüfung des Stadtrechnungshofes Wien:

Der von der geprüften Stelle bekannt gegebene Umsetzungsstand entsprach dem Ergebnis der Prüfung.

Die überarbeitete Fach-Policy "IKT-Sicherheitsrichtlinien für externe KundInnen" wurde am 20. Mai 2015 freigegeben und am 8. August 2016 zuletzt überprüft. Im Themenpunkt betreffend den Anschluss von IKT-Geräten wurde der Verweis auf "gültige Si-

cherheitsvorschriften" entfernt. Ebenso erfolgte eine Konkretisierung der Anforderungen betreffend Authentisierungsmerkmale.

Im Pkt. "Empfehlungen zur IKT-Sicherheit" wurde weiterhin auf "Empfehlungen oder Services der Magistratsabteilung 14" hingewiesen, ohne diese im Text genauer zu beschreiben. Im Linkverzeichnis der "IKT-Sicherheitsrichtlinien für externe KundInnen" war jedoch ein entsprechender Verweis enthalten.

3.11 Empfehlung Nr. 11

Der Stadtrechnungshof Wien empfahl, die im Zusammenhang mit der Bereitstellung bzw. Nutzung der Netzwerkinfrastruktur der Stadt Wien von den externen Kundinnen bzw. Kunden zu erbringenden Pflichten zu evaluieren und entsprechend klar in der Vereinbarung zur IKT-Sicherheit darzulegen.

Stellungnahme der geprüften Stelle:

Die erforderlichen Maßnahmen und Termine werden ehestmöglich mit den dafür Verantwortlichen abgestimmt.

Maßnahmenbekanntgabe der geprüften Stelle:

Die Empfehlung wurde umgesetzt.

Die entsprechende Fach-Policy wurde überarbeitet und publiziert:
"IKT-Sicherheitsrichtlinien für externe KundInnen".

Ergebnis der Prüfung des Stadtrechnungshofes Wien:

Der von der geprüften Stelle bekannt gegebene Umsetzungsstand entsprach dem Ergebnis der Prüfung.

Die überarbeitete Fach-Policy "IKT-Sicherheitsrichtlinien für externe KundInnen" wurde am 20. Mai 2015 freigegeben und am 8. August 2016 zuletzt überprüft. In Bezug auf die Pflichten der externen Kundinnen bzw. Kunden bei der Wiederherstellung eines störungsfreien Zustandes wurde festgelegt, dass die externen Kundinnen bzw. Kunden -

soweit erforderlich - bei der Störungsbehebung durch die Magistratsabteilung 14 mitzuwirken hatten.

3.12 Empfehlung Nr. 12

Der Stadtrechnungshof Wien empfahl, den betrieblichen Ablauf hinsichtlich der Einbindung des WienCERT zu evaluieren.

Stellungnahme der geprüften Stelle:

Die Empfehlung wird hierorts als bereits umgesetzt angesehen. Auf der Wien Intern-Seite https://www.intern.magwien.gv.at/ wiencert/ wird das WienCERT und dessen Aufgaben vorgestellt. Die Erreichbarkeit des WienCERT ist dort mit Montag bis Freitag (werktags) 8.00 Uhr bis 16.00 Uhr (abweichend davon 8.00 Uhr bis 12.00 Uhr für definierte Kalendertage - "Normatage") angegeben.

Unabhängig von der Erreichbarkeit und betrieblichen Einbindung des WienCert sind Sicherheitsvorfälle an den Helpdesk der jeweils zuständigen IKT-Dienststelle (Magistratsabteilung 14, Serviceeinheit Informationstechnologie oder Allgemeines Krankenhaus - Abteilung Technologie und Informatik) zu melden. Damit ist eine eindeutige Schnittstelle für die Kontaktaufnahme durch Kundinnen bzw. Kunden für den Spezialfall "Sicherheitsfall" vorgesehen.

Maßnahmenbekanntgabe der geprüften Stelle:

Die Empfehlung wurde umgesetzt.

Die Empfehlung war mit Vorliegen des Prüfberichts bereits umgesetzt (s. Stellungnahme oben).

Ergebnis der Prüfung des Stadtrechnungshofes Wien:

Der von der geprüften Stelle bekannt gegebene Umsetzungsstand entsprach dem Ergebnis der Prüfung.

Die Erreichbarkeit des WienCert wurde entsprechend fixiert und Informationen zur Erreichbarkeit im Intranet der Stadt Wien publiziert.

4. Zusammenfassung der Empfehlung

Empfehlung Nr. 1:

Die Intervalle der Sicherheitsbegehungen - insbesondere bei Räumlichkeiten der externen Stellen - sind zu evaluieren und gegebenenfalls zu verdichten. Dabei sollten die Bedeutung der Standorte, die vorgefundenen Mängel und die dokumentierten Behebungsmaßnahmen aus den letzten Sicherheitsbegehungen entsprechend berücksichtigt werden (s. Pkt. 3.8).

Stellungnahme der Magistratsabteilung 14:

Die Umsetzung der Empfehlung wurde bereits veranlasst.

Der Stadtrechnungshofdirektor:

Dr. Peter Pollak, MBA

Wien, im Februar 2018