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 - 14-1/15

Maßnahmenbekanntgabe zu

MA 14, Prüfung der IKT-Sicherheit von ausgelagerten Bereichen

INHALTSVERZEICHNIS

ABKÜRZUNGSVERZEICHNIS

AKH-DTI	Allgemeines Krankenhaus - Direktion der Teilunternehmung Technologie und Informatik
bzgl.	bezüglich
bzw.	beziehungsweise
CERT	Computer Emergency Response Team
d.h.	das heißt
EDV	Elektronische Datenverarbeitung

E-Mail ..... Elektronische Post
https..... Hypertext Transfer Protocol Secure
IKT..... Informations- und Kommunikationstechnologie
KAVIT..... Krankenanstaltenverbund Informationstechnologie
Nr..... Nummer
s..... siehe
www..... World Wide Web

Erledigung des Prüfberichtes

Der Stadtrechnungshof Wien unterzog die Magistratsabteilung 14 hinsichtlich der IKT-Sicherheit von ausgelagerten Bereichen einer stichprobenweisen Prüfung. Der diesbezügliche Bericht des Stadtrechnungshofes Wien wurde am 13. Mai 2015 veröffentlicht und im Rahmen der Sitzung des Stadtrechnungshofausschusses vom 21. Mai 2015, Ausschusszahl 42/15 mit Beschluss zur Kenntnis genommen.

Kurzfassung des Prüfberichtes

Der Stadtrechnungshof Wien unterzog die Magistratsabteilung 14 hinsichtlich der IKT-Sicherheit von ausgelagerten Bereichen einer Prüfung.

Die Prüfung zeigte Abgrenzungsprobleme im Zusammenhang der korrekten Zuordnung zu den internen bzw. externen Kundinnen- bzw. Kundenbereichen auf.

Bei den Inhalten der Vereinbarungen der IKT-Sicherheit mit den externen Kundinnen bzw. Kunden waren sowohl inhaltliche Verbesserungspotenziale bei einzelnen Bereichen (unter anderem Wortwahl, Controlling von vereinbarten Maßnahmen, schriftliche Vereinbarungen, Verweise), als auch die Einbindung des WienCERT beim betrieblichen Ablauf des Managements von IKT-Sicherheitsvorfällen zu erkennen.

Die angesprochenen Empfehlungen zielten insgesamt auf eine Verbesserung der IKT-Sicherheit, rechtliche Klarstellungen und besseren Support der Magistratsabteilung 14 ab.

Bericht der Magistratsabteilung 14 zum Stand der Umsetzung der Empfehlungen

Im Rahmen der Äußerung der geprüften Stelle wurde folgender Umsetzungsstand in Bezug auf die ergangenen 12 Empfehlungen bekannt gegeben:

Stand der Umsetzung der Empfehlungen	Anzahl	Anteil in %
Umgesetzt	7	58,3
In Umsetzung	5	41,7
Geplant	-	-
Nicht geplant	-	-

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

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.

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, notwendigen 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.

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 Geschäftsbe-

dingungen 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.

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 Wege einer definierten Nahtstellenstruktur (Zentrales Melderegister) erging eine Anfrage an die Magistratsabteilung 26 als auftraggebende Stelle im Sinne 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.

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.

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.

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.

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.

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.

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.

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.

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, KAVIT oder AKH-DTI) 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).

Für den Stadtrechnungshofdirektor:
Mag. Manfred Jordan
Wien, im Februar 2016