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

MA 14, Prüfung der IKT-Sicherheit von ausgelagerten Bereichen

Tätigkeitsbericht 2015

KURZFASSUNG

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.

INHALTSVERZEICHNIS

1. Umfang der Prüfung 6
1.1 Prüfungsgegenstand....6
1.2 Definitionen zum Prüfungsgegenstand 6
1.3 Prüfungshandlungen....6
2. Grundlagen....7
2.1 Begriffsbestimmung des Kundinnen- bzw. Kundenbereiches der Magistratsabteilung 14....7
2.2 Leistungsumfang der Magistratsabteilung 14 7
2.3 Rechtliche Grundlagen 8
3. Kundinnen- bzw. Kundenbereich der Magistratsabteilung 14....9
3.1 IKT-Sicherheit der internen Kundinnen bzw. Kunden 9
3.2 Vereinbarungen über die IKT-Sicherheit von externen Kundinnen bzw. Kunden 10
3.3 Inhalte der Vereinbarungen über die IKT-Sicherheit der externen Kundinnen bzw. Kunden....15
4. Stichprobenweise Einschau bei einer externen Kundin....19
5. Zusammenfassung der Empfehlungen....20

ABKÜRZUNGSVERZEICHNIS

ADV	Automationsunterstützte Datenverarbeitung
AKH-DTI	Allgemeines Krankenhaus - Direktion der Teilunternehmung Technologie und Informatik
BOS	Behörden und Organisationen mit Sicherheitsaufgaben
bzw	beziehungsweise
CERT	Computer Emergency Response Team

ELAK	Elektronischer Akt
E-Mail	Elektronische Post
gem	gemäß
http	Hypertext Transfer Protocol
IKT	Informations- und Kommunikationstechnologie
IT	Informationstechnologie
KAVIT	Krankenanstaltenverbund Informationstechnologie
lt.	laut
MA	Magistratsabteilung
MD-OS	Magistratsdirektion - Geschäftsbereich Organisation und Sicherheit
Nr.	Nummer
PC	Personal Computer
Pkt.	Punkt
s.	siehe
u.a.	unter anderem
www	World Wide Web
z.B	zum Beispiel
z.T.	zum Teil

GLOSSAR

Account

Ein Account ist ein Benutzerkonto mit einer Zugangsberechtigung zu einem zugangsbeschränkten IT-System.

Computer Emergency Response Team

Ein Computer Emergency Response Team ist eine Gruppe von Fachleuten, die im Zusammenhang mit konkreten IKT-Sicherheitsvorfällen sowohl Warnungen bereitstellt als auch bei der operativen Koordination der Lösungsansätze bzw. bei den Lösungen selbst mitwirkt.

Fileservice
Zentrale Datenspeicher.

Hosting
Unter Hosting wird die Bereitstellung bzw. die Unterbringung von Inhalten auf Ressourcen bei einem IKT-Dienstleister verstanden (z.B. Webseiten auf einem Webserver).

Internet Service Provider Dienste
Unter Internet Service Provider Dienste werden Leistungen, die inhaltlicher und/oder technischer Art sind, die für die Benutzung oder den Betrieb von Inhalten und Diensten im Internet durch die jeweiligen Kundinnen bzw. Kunden benötigt werden, verstanden.

Portalverbund
Der Portalverbund ist ein gesamtheitlicher Ordnungsrahmen und eine technische Lösung für einen einheitlichen Zugriff sowie der Verwaltung und der Verwendung von einzelnen übergreifenden IKT-Anwendungen und den darin enthaltenen Daten der einzelnen öffentlichen Stellen des Bundes, der Bundesländer und der Gemeinden Österreichs sowie weiterer Stellen.

Thin Clients (Terminal)
Ein IKT-Endgerät zur Eingabe und Ausgabe (Anzeige) von Daten.

PRÜFUNGSERGEBNIS

Der Stadtrechnungshof Wien unterzog die Magistratsabteilung 14 hinsichtlich 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. Umfang der Prüfung

1.1 Prüfungsgegenstand

Die gegenständliche Prüfung des Stadtrechnungshofes Wien betraf die Prüfung der IT-Sicherheit von ausgelagerten Bereichen in der Magistratsabteilung 14. Die eigentlichen Prüfungshandlungen wurden im Zeitraum von September 2014 bis Februar 2015 vorgenommen.

1.2 Definitionen zum Prüfungsgegenstand

Unter der Bezeichnung "ausgelagerte Bereiche" waren aus Sicht des Stadtrechnungshofes Wien jene Kundinnen bzw. Kunden zu verstehen, die insbesondere nicht Teil des Magistrats der Stadt Wien waren. Diese Kundinnen bzw. Kunden unterlagen deshalb keinen internen Regelungen des Magistrats der Stadt Wien und wurden daher von der Magistratsabteilung 14 als "externe Kundinnen bzw. Kunden" ausgewiesen (s. dazu auch Pkt. 2 Grundlagen).

1.3 Prüfungshandlungen

Der Fokus der Prüfungshandlungen lag in der praktischen Umsetzung und der Gewährleistung der gesamtheitlichen IT-Sicherheit (auch als IKT-Sicherheit bezeichnet) bei der Stadt Wien im Zusammenhang mit den ausgelagerten Kundinnen bzw. Kunden (externe Kundinnen bzw. Kunden). Insbesondere wurden jene Kundinnen bzw. Kunden in die Prüfung einbezogen, die von der Magistratsabteilung 14 bereitgestellte Hardware- und

Softwareinfrastruktur, wie u.a. den Zugang zu der Netzwerkinfrastruktur der Stadt Wien, benutzten bzw. IKT-Leistungen erhielten.

Der Stadtrechnungshof Wien überprüfte hiebei die zugrundeliegenden Vereinbarungen und deren Umsetzung, wobei stichprobenweise und unter Berücksichtigung der Prüfungsbefugnisse des Stadtrechnungshofes Wien die entsprechenden de facto Umsetzungen in ausgewählten ausgelagerten Bereichen - respektive bei einer Kundin vor Ort - eingesehen wurde.

2. Grundlagen

2.1 Begriffsbestimmung des Kundinnen- bzw. Kundenbereiches der Magistratsabteilung 14

Von der Magistratsabteilung 14 wurden alle Kundinnen bzw. Kunden als "interne" verstanden,

- die gem. § 3 Geschäftsordnung für den Magistrat der Stadt Wien taxativ aufgezählt sind (u.a. als Dienststellen und Unternehmungen der Stadt Wien),
- die sich aufgrund der Organisation des Magistrats im Rahmen der durch die dem Magistratsdirektor zugeteilten Aufgabe der "Leitung des Inneres Dienstes" (u.a. auch die Organe der Wiener Gemeinde- und Landesverwaltung) ergeben sowie
- die aufgrund gesetzlicher Vorgaben die Bereitstellung der entsprechenden sachlichen Erfordernisse bzw. Ressourcen - u.a. wird darunter von der Magistratsabteilung 14 die Bereitstellung einer adäquaten IKT-Organisation mit den entsprechenden einzelnen IKT-Leistungen verstanden - durch das Amt der Wiener Landesregierung zur Verfügung gestellt wurden.

Alle anderen Kundinnen bzw. Kunden, bei denen diese Bedingungen nicht zutrafen, wurden von der Magistratsabteilung 14 in der Folge als "externe" angesehen.

2.2 Leistungsumfang der Magistratsabteilung 14

Von der Magistratsabteilung 14 wurden im Rahmen einer adäquaten IKT-Organisation für ihre Kundinnen bzw. Kunden im Wesentlichen folgende IKT-Leistungen erbracht:

- Bereitstellung bzw. Nutzung der Netzwerkinfrastruktur der Stadt Wien,
- Bereitstellung bzw. Nutzung von IKT-Hardware (u.a. Personal Computer, Thin Clients, Laptops, Multifunktionsgeräte, Drucker, Festnetztelefonie, Mobilfunktelefonie, Faxgeräte),
- Bereitstellung bzw. Nutzung von IKT-Software (u.a. Standardsoftware des ADV-Installers, ELAK, Fileservice, E-Mail Dienst),
- Bereitstellung bzw. Nutzung von Diensten für die Behörden und Organisationen mit Sicherheitsaufgaben (z.B. BOS Funkkommunikation),
- Bereitstellung bzw. Nutzung von Internet Service Provider Diensten und
- Bereitstellung bzw. Nutzung von Portalverbund Anwendungen und Zugängen.

2.3 Rechtliche Grundlagen

Im Zusammenhang mit der Bereitstellung einer adäquaten IKT-Organisation mit den IKT-Leistungen durch die Magistratsabteilung 14 war für die Kundinnen bzw. Kunden auch die notwendige IKT-Sicherheit impliziert und in einem dementsprechenden Umfang jedenfalls als Thema mitzubetrachten bzw. mitzuberücksichtigen.

2.3.1 Im Magistrat der Stadt Wien wird das Thema der IKT-Sicherheit durch den IKT-Erlass MD-OS 51600-2013-1, Sicherheit in der Informations- und Kommunikationstechnologie vom 28. Jänner 2013, geregelt.

Die Magistratsabteilung 14 ist als zentrale IKT-Dienststelle der Stadt Wien für die Gewährleistung der IKT-Sicherheit im eigenen Bereich sowie für die betriebene IKT-Infrastruktur erforderlichen organisatorischen, personellen, technischen und baulichen Maßnahmen verantwortlich.

Adressatinnen des angeführten IKT-Erlasses waren alle städtischen Dienststellen gemäß der Geschäftsordnung für den Magistrat der Stadt Wien, die entsprechend dieses Erlasses die Einhaltung der IKT-Sicherheit - als interne Kundinnen bzw. Kunden der Magistratsabteilung 14 - sicherzustellen haben.

Für die externen Kundinnen bzw. Kunden, die weder Dienststelle gem. § 3 Geschäftsordnung für den Magistrat der Stadt Wien noch Unternehmung gem. § 71 Wiener Stadtverfassung sind, ist die Einhaltung des IKT-Erlasses durch schriftlichen Vertrag sicherzustellen.

2.3.2 Weiters wurde im IKT-Erlass näher ausgeführt, dass für die Unternehmung Wiener Krankenanstaltenverbund auf Grundlage dieses Erlasses für die Sicherheit in der IKT von der Leitung die erforderlichen organisatorischen Anordnungen sinngemäß zu treffen sind.

Aus Sicht des Stadtrechnungshofes Wien war in diesem Zusammenhang nicht eindeutig klar, inwieweit für die anderen Unternehmungen der Stadt Wien (Stadt Wien - Wiener Wohnen und Wien Kanal) ebenso weitere explizite sinngemäße Anordnungen nach dem IKT-Erlass zu treffen wären.

Der Stadtrechnungshof Wien empfahl der Magistratsabteilung 14, 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.

3. Kundinnen- bzw. Kundenbereich der Magistratsabteilung 14

Von der Magistratsabteilung 14 wurde dem Stadtrechnungshof Wien für die Überprüfung mitgeteilt, dass ihr Kundenbereich insgesamt 192 Kundinnen bzw. Kunden umfasste (Stand: Oktober 2014).

Von den 192 Kundinnen bzw. Kunden wurden von der Magistratsabteilung 14 insgesamt 48 mit einer entsprechenden adäquaten IKT-Organisation mit der Bereitstellung bzw. Nutzung der einzelnen IKT-Leistungen in unterschiedlicher Ausprägung als externe Kundinnen bzw. Kunden ausgewiesen.

3.1 IKT-Sicherheit der internen Kundinnen bzw. Kunden

Bei der Durchsicht der von der Magistratsabteilung 14 bereitgestellten Liste aller Kundinnen bzw. Kunden war festzustellen, dass einige davon (z.B. das Verwaltungsgericht

Wien bzw. die Organe der Wiener Gemeinde- und Landesverwaltung) den internen Kundinnen bzw. Kunden zugeordnet wurden. Aus Sicht des Stadtrechnungshofes Wien war dabei nicht eindeutig klar, ob diese tatsächlich dem internen Kundinnen- bzw. Kundenbereich zuzuordnen sind und damit der IKT-Erlass anzuwenden wäre.

Der Stadtrechnungshof Wien empfahl der Magistratsabteilung 14, 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.

3.2 Vereinbarungen über die IKT-Sicherheit von externen Kundinnen bzw. Kunden

Die Magistratsabteilung 14 hat als IKT-Dienststelle gemäß dem IKT-Erlass mit den auftraggebenden Stellen abweichende Verantwortlichkeiten im Zusammenhang mit der IKT-Sicherheit entsprechend zu vereinbaren.

Die grundlegende Bedingung über den Abschluss einer entsprechenden Vereinbarung zur IKT-Sicherheit mit den externen Kundinnen bzw. Kunden ist die Bereitstellung und Nutzung der Netzwerkinfrastruktur des Magistrats der Stadt Wien. Von der Magistratsabteilung 14 sollten - lt. deren eigener Angabe - mit 14 externen Kundinnen bzw. Kunden, eigene Vereinbarungen über die IKT-Sicherheit abgeschlossen werden.

Zudem bezogen neun weitere externe Kundinnen bzw. Kunden IKT-Leistungen (u.a. Internet Service Provider Dienste und Portalverbund Anwendungen und Zugänge) von der Magistratsabteilung 14, in der die IKT-Sicherheit entsprechend zu berücksichtigen war.

3.2.1 Von den ausgewiesenen 14 externen Kundinnen bzw. Kunden, welche die IKT-Leistung der Bereitstellung bzw. Nutzung der Netzwerkinfrastruktur des Magistrats der Stadt Wien nutzten, lagen zum Prüfungszeitpunkt 11 Vereinbarungen vor.

Zwei Vereinbarungen wurden nach entsprechenden inhaltlichen Anpassungen einiger Punkte während der Prüfung unterfertigt. Eine Vereinbarung fehlte allerdings zur Gänze. Die Magistratsabteilung 14 begründete dies damit, dass einer bei einer externen Kundin beschäftigten Person der Stadt Wien ein vollständiger Standard-Arbeitsplatz mit entsprechender IKT-Ausstattung (PC) mit Anbindung an das Netzwerk der Stadt Wien bereitgestellt wurde. Eine eigene Vereinbarung hinsichtlich der IKT-Sicherheit war in diesem Fall nach Ansicht der Magistratsabteilung 14 nicht notwendig, da diese Person dem bereits angeführten IKT-Erlass unterlag.

3.2.2 Neben der IKT-Leistung der Bereitstellung bzw. Nutzung der Netzwerkinfrastruktur des Magistrats der Stadt Wien erbrachte die Magistratsabteilung 14 bei vier weiteren externen Kundinnen bzw. Kunden auch IKT-Leistungen hinsichtlich der Internet Service Provider Dienste.

Wie der Stadtrechnungshof Wien feststellte, lagen für diese erbrachten Leistungen Vereinbarungen vor.

Von einer Kundin wurde der Magistratsabteilung 14 in diesem Zusammenhang mitgeteilt, dass die von der Magistratsabteilung 14 in der Regel abgeschlossene Vereinbarung nicht für sie zutreffen würde.

Die Einschau des Stadtrechnungshofes Wien in den zugrundeliegenden Vertrag ergab, dass bei der Erbringung dieser IKT-Leistung vertraglich festgelegt wurde, dass hinsichtlich der Thematik der IKT-Sicherheit ein allgemeiner Vorbehalt über eine allfällige Sperre bei sicherheits- oder betriebsgefährdenden Internetdiensten im Anlassfall von der Magistratsabteilung 14 gesetzt werden könnte. Allfällig weitere Regelungen zur IKT-Sicherheit waren in diesem Vertrag vom Stadtrechnungshof Wien nicht erkennbar.

Der Stadtrechnungshof Wien empfahl der Magistratsabteilung 14, 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.

3.2.3 Eine weitere IKT-Leistung der Magistratsabteilung 14 lag im Zusammenhang mit der Erbringung der Bereitstellung bzw. der Nutzung von Portalverbund Anwendungen und Zugängen vor. Der Portalverbund ist eine Struktur mit einer großflächigen Vernetzung von verschiedensten Teilnehmerinnen bzw. Teilnehmern in Österreich.

Aufgrund der großflächigen Vernetzung war aus Sicht des Stadtrechnungshofes Wien in diesem Bereich entsprechendes Augenmerk hinsichtlich der IKT-Sicherheit und den damit in Verbindung stehenden Vereinbarungen bei der Magistratsabteilung 14 zu legen.

Die Nutzung des Portalverbundes wird grundsätzlich durch die Portalverbundvereinbarung, die auf die Einhaltung der Regelungen - und damit auch der entsprechenden Konventionen der IKT-Sicherheit - durch die Teilnehmerinnen bzw. Teilnehmer hinweist, geregelt. Entsprechend dieser Portalverbundvereinbarung waren u.a. folgende Konventionen von entsprechend hoher Sicherheitsrelevanz und im Zusammenhang zur IKT-Sicherheit durch die Teilnehmerinnen bzw. Teilnehmer am Portalverbund einzuhalten:

- Benutzer- und Rechteverwaltung,
- Datensicherheitsmaßnahmen,
- Einräumung von Zugriffsrechten im Portalverbund,
- Einräumung von Zugriffsrechten im Portalverbund über Dienstleisterinnen bzw. Dienstleister,
- Protokollformat,
- Revisionsabfrage,
- Sicherheitsklassen.

Aus den Aufzeichnungen der Magistratsabteilung 14 war zu erkennen, dass insgesamt vier Kundinnen bzw. Kunden entsprechende IKT-Leistungen im Zusammenhang mit dem Portalverbund durch die Magistratsabteilung 14 erhielten.

Von der Magistratsabteilung 14 wurde dabei für zwei externe Kundinnen bzw. Kunden eine jeweils eigene Anwendung über den Portalverbund selbst bereitgestellt. In diesen Fällen wurden von der Magistratsabteilung 14 entsprechende Vereinbarungen über die IKT-Dienstleistung der Bereitstellung (Hosting) von Anwendungen im Portalverbund abgeschlossen.

Für zwei weitere externe Kundinnen bzw. Kunden wurde ein technischer Zugang zu Anwendungen des Portalverbundes durch die Magistratsabteilung 14 erbracht. Auch bei diesen IKT-Leistungen lagen entsprechende Nutzungsvereinbarungen von der Magistratsabteilung 14 mit den beiden externen Kundinnen bzw. Kunden vor. In diesen Fällen waren neben diesen Vereinbarungen über den technischen Zugang in das Informationssystem auch organisatorische Vereinbarungen über die Einräumung von Zugriffsrechten durch die Magistratsabteilung 26 notwendig. Wie der Stadtrechnungshof Wien bei der Prüfung feststellte, lag die Vereinbarung über die Einräumung von Zugriffsrechten für eine der genannten externen Kundinnen vor. Für die zweite externe Kundin war ein diesbezügliches Ansuchen für die Einräumung von Zugriffsrechten nicht gestellt. Von der Magistratsabteilung 14 wurde zwar ein technischer Zugang eingerichtet, ein tatsächlicher Zugriff korrekterweise aber nicht ermöglicht.

3.2.4 In diesem Zusammenhang war bei der Einschau in die IKT-Leistungen des Portalverbundes anhand der Liste der externen Kundinnen bzw. Kunden festzustellen, dass eine Kundin über eine definierte Nahtstellenstruktur entsprechende Datenübermittlungen durch die Magistratsabteilung 14 erhielt. Für den Stadtrechnungshof Wien war bei der ersten Durchsicht nicht eindeutig erkennbar, ob diese IKT-Leistung direkt dem Portalverbund zuzuordnen und daher eine entsprechende Vereinbarung notwendig war.

Nach Angabe der Magistratsabteilung 14 handelte es sich bei dieser Kundin um eine ehemalige Magistratsdienststelle, die aus dem Magistrat ausgegliedert wurde und somit zu den externen Kundinnen zugeordnet werden musste. Wie sich herausstellte, konnte auch die Magistratsabteilung 14 die erbrachte IKT-Leistung der Datenübermittlungen nicht eindeutig dem Portalverbund zuordnen.

Eine notwendige Vereinbarung hinsichtlich der IKT-Sicherheit konnte von der Magistratsabteilung 14 dem Stadtrechnungshof Wien daher nicht vorgelegt werden.

Der Stadtrechnungshof Wien empfahl der Magistratsabteilung 14 zu evaluieren, ob die IKT-Sicherheit für die erbrachten IKT-Leistungen der Datenübermittlung an eine externe Kundin durch schriftliche Vereinbarungen sicherzustellen wäre.

3.2.5 Von den insgesamt 48 externen Stellen lagen bei 25 Kundinnen bzw. Kunden keine schriftlichen Vereinbarungen über die IKT-Sicherheit vor. Begründet wurde dies damit, dass aus Sicht der Magistratsabteilung 14 keine weiteren IKT-Leistungen angeboten wurden, die eine Gefahr für die IKT-Sicherheit darstellten, und daher keine Vereinbarungen abzuschließen waren.

Bei der Durchsicht der einzelnen Vereinbarungen zur IKT-Sicherheit entstand für den Stadtrechnungshof Wien der Eindruck, dass eine genaue Zuordnung zu den jeweiligen externen bzw. internen Kundinnen- bzw. Kundenbereichen nicht immer eindeutig war. Insofern war dadurch nicht immer gewährleistet, dass das Thema der IKT-Sicherheit tatsächlich durchgängig geregelt war.

Der Stadtrechnungshof Wien empfahl der Magistratsabteilung 14, 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.

3.2.6 Der Stadtrechnungshof Wien vertrat die Meinung, dass die Magistratsabteilung 14 als die zentrale IKT-Dienstleisterin der Stadt Wien für die IKT-Sicherheit gegenüber dem gesamten Kundinnen- bzw. Kundenbereich mitverantwortlich ist. Die Vereinbarung, dass die Verantwortung der IKT-Sicherheit zum überwiegenden Teil den Kundinnen bzw. Kunden übertragen wurde, war für den Stadtrechnungshof nur z.T. nachvollziehbar. Vor allem deswegen, da bei einem eintretenden IKT-Sicherheitsvorfall und seiner Bewältigung - egal mit welcher Kundin bzw. welchem Kunden - die Magistratsabtei-

lung 14 bzw. in weiterer Folge die Stadt Wien als Verantwortliche angesehen werden könnte. Aus Sicht des Stadtrechnungshofes Wien impliziert die Bereitstellung der jeweiligen IKT-Leistungen auch eine entsprechende Mitverantwortung bei der Aufrechterhaltung der maximal möglichen und vertretbaren IKT-Sicherheit bei den einzelnen IKT-Leistungen der Magistratsabteilung 14.

Der Stadtrechnungshof Wien empfahl der Magistratsabteilung 14, 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.

3.3 Inhalte der Vereinbarungen über die IKT-Sicherheit der externen Kundinnen bzw. Kunden

Der Stadtrechnungshof Wien nahm Einschau in die Inhalte der Vereinbarung "IKT-Sicherheitsrichtlinien für magistratsexterne KundInnen/AuftraggeberInnen der MA 14".

Nach Angabe der Magistratsabteilung 14 wurde mit dieser Vereinbarung die IKT-Sicherheit externer Kundinnen bzw. Kunden geregelt. Es handelte sich um ein allgemeines Regelwerk, das den Leistungsanforderungen der Kundinnen bzw. Kunden entsprechend angepasst wird.

Diese Vereinbarung legte dabei in den folgenden Bereichen u.a. die Kriterien für

- die Anforderungen an die Räumlichkeiten der IKT-Infrastruktur,
- die IKT-Komponenten,
- die Beauftragungen von weiteren Dienstleisterinnen bzw. Dienstleistern,
- den Anschluss von IKT-Geräten im Netzwerk der Stadt Wien,
- die Softwaresicherheit,
- das Management der Administratoren bzw. den Accounts und den Berechtigungen,
- das IKT-Sicherheitsbewusstsein,
- die Störungen und Unterbrechungen des Netzbetriebes,

- das Management von Sicherheitsvorfällen,
- die Anwendungsrichtlinien der Magistratsabteilung 14 und
- die Empfehlungen zur IKT-Sicherheit fest.

Festzustellen war, dass diese Vereinbarung hinsichtlich der im ersten Punkt aufgezeigten Anforderungen an die Räumlichkeiten der IKT-Infrastruktur auf weitere drei Dokumente verwies und inhaltlich
- als Planungsunterlage für neue Standorte bzw. Generalsanierungen die Ausstattungsbeschreibung der Objektinfrastruktur der IKT-Versorgung,
- eine Checkliste zur Basissicherheit für periodische Sicherheitsbegehungen sowie
- die Verhaltensregeln als Aushang für dezentrale IKT-Räumlichkeiten

vertiefend die Kriterien festlegten.

3.3.1 Bei einem dieser drei erwähnten Dokumente war vom Stadtrechnungshof Wien u.a. zu erkennen, dass der Bearbeitungsstand dieses Dokumentes mit März 2009 angegeben war.

Der Stadtrechnungshof Wien empfahl der Magistratsabteilung 14, ein Dokument der IKT-Sicherheitsrichtlinien auf Aktualität zu überprüfen.

3.3.2 Hinsichtlich der IKT-Sicherheit wurde von der Magistratsabteilung 14 mitgeteilt, dass eine jährliche Überprüfung der erwähnten Inhalte bei den jeweiligen Kundinnen bzw. Kunden vorgesehen war. Der Stadtrechnungshof Wien stellte fest, dass dabei nur wenige externe Kundinnen bzw. Kunden in einer Prioritätenliste hinsichtlich der IKT-Sicherheit aufgenommen waren. Begründet wurde dies damit, dass der IKT-Sicherheitserlass erst seit etwas mehr als einem Jahr in Kraft war und derartige Überprüfungen der externen Kundinnen bzw. Kunden in die letzte jährliche Planung noch nicht miteinbezogen worden waren.

Der Stadtrechnungshof Wien empfahl der Magistratsabteilung 14, die erstmalig aufgrund des IKT-Sicherheitserlasses unterzeichneten Vereinbarungen zum Anlass zu nehmen, einen ersten Schwerpunkt - im Sinn eines Beratungs- bzw. Qualitätssiche-

rungsgespräches zur IKT-Sicherheit - bei den externen Kundinnen bzw. Kunden zu setzen.

3.3.3 In der IKT-Sicherheitsrichtlinie war vom Stadtrechnungshof Wien zu erkennen, dass die Thematik des Einsatzes von neuen IKT-Komponenten durch externe Kundinnen bzw. Kunden behandelt wurde. Zudem wurde auch die Thematik der Beauftragung von weiteren anderen IKT-Dienstleisterinnen bzw. IKT-Dienstleistern als die Magistratsabteilung 14 dargelegt.

In beiden Themen war aus Sicht des Stadtrechnungshofes Wien die textliche Ausführung zu den diesbezüglichen Pflichten der externen Kundinnen bzw. Kunden nicht ausreichend klar dargelegt (u.a. Wortwahl, Controlling von vereinbarten Maßnahmen, Mitteilungspflicht, schriftliche Vereinbarungen).

Die Magistratsabteilung 14 teilte hiezu mit, dass bis zum Prüfungszeitraum noch keine Beauftragung von anderen IKT-Dienstleisterinnen bzw. IKT-Dienstleistern durch externe Kundinnen bzw. Kunden als die Magistratsabteilung 14 in Erwägung gezogen wurde.

Der Stadtrechnungshof Wien empfahl der Magistratsabteilung 14, 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.

3.3.4 Im Zusammenhang mit dem Themenpunkt des Anschlusses von IKT-Geräten im Netzwerk der Stadt Wien war vom Stadtrechnungshof Wien zu erkennen, dass auf "gültige Sicherheitsvorschriften" verwiesen wurde, diese Vorschriften aber nicht näher definiert waren.

In gleicher Weise wurde hinsichtlich der Geheimhaltung von Authentisierungsmerkmalen auf "die von der MA 14 bekannt gegebenen Anforderungen" sowie im Bereich der Empfehlungen zur IKT-Sicherheit auf "Empfehlungen oder Services der MA 14" verwiesen, diese aber ebenso nicht erläutert.

Der Stadtrechnungshof Wien empfahl der Magistratsabteilung 14, generell in Dokumenten enthaltene Verweise auf andere bzw. weitere Vorschriften bzw. Dokumente zu präzisieren.

3.3.5 Bezüglich eines weiteren Bereiches über Störungen und Unterbrechungen des Netzbetriebes "Im Störungsfall sind umgehend geeignete Gegenmaßnahmen zu setzen, um den störungsfreien Zustand wiederherzustellen" - war nach Meinung des Stadtrechnungshofes Wien die textliche Ausführung nicht ausreichend klar definiert, welche Pflichten hier die jeweiligen externen Kundinnen bzw. Kunden dabei insbesondere zu erfüllen haben.

Der Stadtrechnungshof Wien empfahl der Magistratsabteilung 14, 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.

3.3.6 Beim Bereich über das Management von Sicherheitsvorfällen war in der Vereinbarung zur IKT-Sicherheit zu erkennen, dass die externen Kundinnen bzw. Kunden derartige Vorfälle unter einer angegebenen Rufnummer des Helpdesks der Magistratsabteilung 14 zu melden haben. Eine Kontaktangabe zum Computer Emergency Response Team der Stadt Wien (WienCERT) war nicht zu erkennen.

Seitens der Magistratsabteilung 14 wurde diesbezüglich mitgeteilt, dass der Helpdesk des Magistrats der Stadt Wien als zentrale Anlaufstelle für die IKT-Sicherheit der externen Kundinnen bzw. Kunden diente.

Anhand der im Intranet der Stadt Wien verfügbaren Information zum Helpdesk und des WienCERT war bei der betrieblichen Abwicklung zum WienCERT zu erkennen, dass außerhalb der Betriebszeiten des WienCERT der Kontakt über den Helpdesk sichergestellt war. Es wurde auf der betreffenden Intranetseite hingewiesen, dass die Teammitglieder des WienCERT in dringenden Fällen außerhalb der Betriebszeiten des

WienCERT unter den entsprechenden Mobilfunknummern ohne eine garantierte Erreichbarkeit zu kontaktieren sind.

Vom Stadtrechnungshof Wien war diesbezüglich anzumerken, dass diese Kontaktmöglichkeit nur für die internen Kundinnen bzw. Kunden ersichtlich war.

Aufgrund der Mitteilung des Leiters des WienCERT wurde diese Serviceleistung freiwillig - und daher ohne garantierte Erreichbarkeit - von den Teammitgliedern des WienCERT für die internen Kundinnen bzw. Kunden erbracht.

Aus Sicht des Stadtrechnungshofes Wien erschien es notwendig, diese freiwillige Serviceleistung der Teammitglieder im betrieblichen Ablauf und einer entsprechenden gesicherten Erreichbarkeit zur kontinuierlichen Aufrechterhaltung der IKT-Sicherheit zu überdenken.

Der Stadtrechnungshof Wien empfahl der Magistratsabteilung 14, den betrieblichen Ablauf hinsichtlich der Einbindung des WienCERT zu evaluieren.

4. Stichprobenweise Einschau bei einer externen Kundin

Der Stadtrechnungshof Wien prüfte bei einer externen Kundin, welche die von der Magistratsabteilung 14 bereitgestellte Netzwerkinfrastruktur nützte, ob die festgelegten Kriterien hinsichtlich der IKT-Sicherheit vereinbarungsgemäß eingehalten wurden.

Von der externen Kundin wurde hiezu ausgeführt, dass mit der Magistratsabteilung 14 als IKT-Dienststelle eine gute Kooperation bestand. Im Fall von Sicherheitsvorkommnissen wurden von dieser über den Helpdesk entsprechende Mitteilungen übermittelt. Festzustellen war jedoch, dass eine routinemäßige Überprüfung der vereinbarten Kriterien über die IKT-Sicherheit durch die IKT-Dienststelle bis zum Stand Jänner 2015 noch nicht stattfand.

Der Stadtrechnungshof Wien verkannte nicht, dass die externen Kundinnen bzw. Kunden mit der Vereinbarung die Verantwortung für die Gewährleistung der IKT-Sicherheit

übernommen haben, jedoch erschien es dem Stadtrechnungshof Wien insbesondere zur Abwendung möglicher Schadensfälle für die Stadt Wien sinnvoll, im Rahmen der IKT-Sicherheitsvereinbarung zumindest regelmäßige Beratungs- bzw. Qualitätssicherungsgespräche durchzuführen.

Der Stadtrechnungshof Wien regte wie schon im Pkt. 3.2.6 an, regelmäßige Beratungs- und Qualitätssicherungsgespräche bei den externen Organisationseinheiten durchzuführen und diese entsprechend zu dokumentieren.

5. Zusammenfassung der Empfehlungen

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 (s. Pkt. 2.3.2).

Stellungnahme der Magistratsabteilung 14:
Die erforderlichen Maßnahmen und Termine werden ehestmöglich mit den dafür Verantwortlichen abgestimmt.

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 (s. Pkt. 3.1).

Stellungnahme der Magistratsabteilung 14:
Die erforderlichen Maßnahmen und Termine werden ehestmöglich mit den dafür Verantwortlichen abgestimmt.

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 (s. Pkt. 3.2.2).

Stellungnahme der Magistratsabteilung 14:
Die erforderlichen Maßnahmen und Termine werden ehestmöglich mit den dafür Verantwortlichen abgestimmt.

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 (s. Pkt. 3.2.4).

Stellungnahme der Magistratsabteilung 14:
Die erforderlichen Maßnahmen und Termine werden ehestmöglich mit den dafür Verantwortlichen abgestimmt.

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 (s. Pkt. 3.2.5).

Stellungnahme der Magistratsabteilung 14:
Die erforderlichen Maßnahmen und Termine werden ehestmöglich mit den dafür Verantwortlichen abgestimmt.

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 (s. Pkt. 3.2.6 sowie Pkt. 4).

Stellungnahme der Magistratsabteilung 14:
Die erforderlichen Maßnahmen und Termine werden ehestmöglich mit den dafür Verantwortlichen abgestimmt.

Empfehlung Nr. 7:
Der Stadtrechnungshof Wien empfahl, ein Dokument der IKT-Sicherheitsrichtlinien auf Aktualität zu überprüfen (s. Pkt. 3.3.1).

Stellungnahme der Magistratsabteilung 14:
Die erforderlichen Maßnahmen und Termine werden ehestmöglich mit den dafür Verantwortlichen abgestimmt.

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 (s. Pkt. 3.3.2).

Stellungnahme der Magistratsabteilung 14:
Die erforderlichen Maßnahmen und Termine werden ehestmöglich mit den dafür Verantwortlichen abgestimmt.

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 (s. Pkt. 3.3.3).

Stellungnahme der Magistratsabteilung 14:
Die erforderlichen Maßnahmen und Termine werden ehestmöglich mit den dafür Verantwortlichen abgestimmt.

Empfehlung Nr. 10:
Der Stadtrechnungshof Wien empfahl, generell in Dokumenten enthaltene Verweise auf andere bzw. weitere Vorschriften bzw. Dokumente zu präzisieren (s. Pkt. 3.3.4).

Stellungnahme der Magistratsabteilung 14:
Die erforderlichen Maßnahmen und Termine werden ehestmöglich mit den dafür Verantwortlichen abgestimmt.

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 (s. Pkt. 3.3.5).

Stellungnahme der Magistratsabteilung 14:
Die erforderlichen Maßnahmen und Termine werden ehestmöglich mit den dafür Verantwortlichen abgestimmt.

Empfehlung Nr. 12:
Der Stadtrechnungshof Wien empfahl, den betrieblichen Ablauf hinsichtlich der Einbindung des WienCERT zu evaluieren (s. Pkt. 3.3.6).

Stellungnahme der Magistratsabteilung 14:
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 (werk-

tags) 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.

Der Stadtrechnungshofdirektor:
Dr. Peter Pollak, MBA
Wien, im April 2015