Wesentliche Ziele der elektronischen Kommunikation liegen darin, Verbesserungen in den Verwaltungsabläufen der Stadt Wien zu schaffen, den Bürgern den Kontakt mit der Verwaltung zu erleichtern sowie eine Vernetzung mit anderen Gebietskörperschaften und mit der Wirtschaft zu erreichen. Um die in diesem Zusammenhang besonders hohen Anforderungen an die Datensicherheit zu gewährleisten, sind umfangreiche Vorkehrungen - die sowohl auf externen als auch auf internen Regelungen beruhen - zu treffen.

Das in die Zuständigkeit der Magistratsabteilung 14 - Automatisationsunterstützte Datenverarbeitung, Informations- und Kommunikationstechnologie fallende Mail-Verbund-System der Stadt Wien erfüllt die Anforderungen an die Grundsätze der Vertraulichkeit, Zuordenbarkeit und Echtheit des Inhaltes des elektronischen Schriftverkehrs in hohem Maße, einige wenige Schwachstellen wurden noch während der Prüfung des Kontrollamtes beseitigt bzw. wurde an Verbesserungen gearbeitet.

Künftig wird eine noch intensivere Befassung mit der elektronischen Signatur und der Verschlüsselung von E-Mails erforderlich sein.

1. Allgemeines

Die Informations- und Kommunikationstechnik nimmt einen immer wichtigeren Platz in der Gesellschaft ein. Die Verwaltungsabläufe der Stadt Wien, der Kontakt mit den Bürgerinnen und Bürgern, die Vernetzung zu anderen Gebietskörperschaften und der Wirtschaft haben sich erheblich verändert. In der Vergangenheit zeigte sich, dass die rasche Erledigung von Verfahren eine gute Arbeitsorganisation voraussetzt, wobei die moderne Kommunikationstechnologie hilft, die Effizienz zu steigern. Deshalb sollte der Zugang zur elektronischen Kommunikation so einfach wie möglich gestaltet sein, wobei bei der Beurteilung des daraus entstehenden Nutzens die Anforderungen an die Vertrauenswürdigkeit und Sicherheit berücksichtigt werden müssen.

Der Einsatz dieses Mediums wurde daher vorrangig unter den Gesichtspunkten Servicefreundlichkeit, Geschwindigkeit, Leistungsfähigkeit und unter Berücksichtigung der Authentizität, der Verfügbarkeit sowie der Kosten überprüft.

Die Datensicherheit bei der elektronischen Kommunikation, bei der hohe Anforderungen an die Grundsätze der Vertraulichkeit, eindeutigen Zuordenbarkeit und Echtheit des Inhaltes der Schriftstücke zu erfüllen sind, ist seitens der zuständigen IT-Abteilung zu gewährleisten. Nach der geltenden Geschäftseinteilung für den Magistrat der Stadt Wien ist hiefür die Magistratsabteilung 14 zuständig, die strategischen Vorgaben und grundlegenden Regelungen fallen in den Zuständigkeitsbereich der Magistratsdirektion, Geschäftsbereich Organisation, Gruppe Informations- und Kommunikationstechnologie (MDO-IKT).

2. Formale Grundlagen

Für den Magistrat der Stadt Wien besteht ein umfangreiches Regelwerk, welches die formalen, organisatorischen und technischen Aspekte berücksichtigt: Hiebei handelt es sich sowohl um externe als auch interne Vorgaben, die die Rahmenbedingungen und deren Umsetzung definieren.

2.1 Externes Regelwerk

Mit dem E-Government-Gesetz, das am 1. April 2004 in Österreich in Kraft getreten ist, wurde die Basis geschaffen, Amtswege von der Antragstellung bis zur Zustellung und Hinterlegung der behördlichen Erledigung auf elektronischem Wege zu erledigen. Die Authentizität des elektronisch gestellten Anbringens, dem die Kontaktaufnahme eines Beteiligten oder einer Beteiligten mit einer Behörde aus eigenem Anlass zu Grunde liegt, soll mittels elektronischer Signatur nachgewiesen werden können. Die Grundlage für die Anerkennung elektronischer Signaturen im österreichischen Recht wurde durch das Bundesgesetz über elektronische Signaturen (Signaturgesetz - SigG), BGBl. I Nr. 190/99, geschaffen, womit die Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen umgesetzt wurde.

Die allgemeinen Rahmenbedingungen für den Datenschutz und Datensicherheit bei der elektronischen Kommunikation mittels E-Mail sieht die EU-Datenschutzrichtlinie (Richtlinie 2002/58/EG) vor. Die Umsetzung dieser Richtlinie wird in Österreich durch das Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 -

DSG 2000) bzw. für Wien durch die Wiener Datenschutzverordnung - WDSV geregelt.

2.2 Vereinbarung zwischen den Gebietskörperschaften

Der Begriff "E-Government" (Electronic Government) steht heute als Synonym für eine moderne und effiziente Verwaltung, die eine neue Form der Zusammenarbeit zwischen den öffentlichen Stellen erfordert. Grundlegende Veränderungen der Strukturen und Prozesse der Verwaltung wurden bereits eingeleitet bzw. sind noch zu erwarten. Dabei ist eine verstärkte Zusammenarbeit der Gebietskörperschaften zur erfolgreichen Umsetzung der Schnittstellen für eine einheitliche und gemeinsame Vorgangsweise entscheidend. Prozessabläufe müssen wesentlich detaillierter und technisch präziser gestaltet werden, als dies bei der Papier-Abwicklung der Fall ist. Weiters ist eine Vielzahl unterschiedlicher Verfahren einheitlich oder nach einem einheitlichen Muster zu gestalten, um einen effizienten Technikeinsatz mit hoher Qualität zu ermöglichen.

Dies betrifft auch die E-Government-Schnittstellen und Basisfunktionen, wofür bereits ein gemeinsames Bekenntnis von Bund, Ländern und Gemeinden vorliegt. Mittels eines Beschlusses der Landesamtsdirektorenkonferenz vom 8. November 2000 wurde eine E-Government-Arbeitsgruppe unter der Leitung Wiens eingerichtet, die sowohl Standards als auch Richtlinien erarbeiten soll. In dieser E-Government-Plattform, an der auch Bund, Österreichischer Städtebund und Österreichischer Gemeindebund mitarbeiten (Arbeitsgruppe "E-Government Bund-Länder-Gemeinden"), werden wesentliche rechtliche, technische und damit verbundene organisatorische Fragestellungen bearbeitet. Zu speziellen Themen wurden Arbeits- bzw. Projektgruppen vom IKT (Informations und Kommunikation Technologie)-Board des Bundes, von der E-Government-Länderarbeitsgruppe, vom Gemeinde- und Städtebund bzw. von einzelnen Organisationen der öffentlichen Verwaltung eingesetzt.

Die erarbeiteten Vorschläge für E-Government-Konventionen bilden die oberste Ebene der organisationsübergreifenden Regeln und sind eine grundlegende Voraussetzung für die bundesweit einheitliche Gliederung von Verwaltungsleistungen. Sie dienen auch gleichzeitig für die Vernetzung von elektronischen Verfahrensinformationen. Die an der Arbeitsgruppe beteiligten Gebietskörperschaften haben erklärt, dass Konventionen, so-

bald sie ihre Zustimmung erhalten haben, für den eigenen Bereich verbindlich sind und umgesetzt werden. Auch wenn keine Genehmigung vorliegt, können Vorschläge in E-Government-Systemen umgesetzt werden, wenn die Bereitschaft zur Nachbesserung auf einen später beschlossenen Standard besteht.

Die definierten Ziele und Standards der einzelnen Konventionen werden als Angelegenheiten, die den selbstständigen Wirkungsbereich der jeweiligen Gebietskörperschaften betreffen, in geltendes Recht transformiert. Für diesen Bericht wurde die beschlossene und für den Magistrat der Stadt Wien verbindliche "E-Mail-Policy - mailpol 2.0.2 " (http://reference.e-government.gv.at/Sicherheit_E-Mail-Policy_2_0.636.0.html) als Beurteilungskriterium herangezogen.

Diese Konvention wurde am 15. April 2005 zur Annahme vorgelegt, die Stadt Wien, vertreten durch die MDO-IKT, hat am 20. Mai 2005 zugestimmt.

2.3 Internes Regelwerk

Für die Umsetzung bei der elektronischen Kommunikation im Magistrat der Stadt Wien bestehen im wesentlichen folgende Dienstvorschriften, die von der Magistratsabteilung 14 und den beteiligten Dienststellen und Mitarbeitern zu berücksichtigen sind:

MDO-337-11/04	Internet und elektronische Kommunikation; Richtlinie
MD-771-9/02	Datenschutz im Magistrat der Stadt Wien
MDA-1598-1/02	Sicherheit in der Informations- und Kommunikationstechnologie (IKT); Richtlinie inkl. Beilage und Glossar
MDS-K-1564-3/04	Versendung von Erlässen mit elektronischer Post; offizielle Dienststellen-Postfächer
MDO-46/2004	Einschau in Mailboxen; Vorgehensweise
MD-1764-2/99	Kanzleiordnung für den Magistrat der Stadt Wien; Neufassung

Darüber hinaus gibt die E-Mail-Verhaltensempfehlung der MDO-IKT wesentliche Hinweise für eine ordnungsgemäße und zweckmäßige Nutzung des Mediums.

Mit der Richtlinie "Internet und elektronische Kommunikation" des Erlasses MDO-337-11/04 wurde mit 1. Februar 2005 geregelt, dass die elektronische Übermittlung und Abwicklung des Schriftverkehrs von Geschäftsstücken, Akten und Aktenteilen an andere Dienststellen als vorrangig gilt. Die Schriftlichkeit in herkömmlicher Papierform ist nur bei gesetzlichen oder sonstigen Vorschriften sowie aus Gründen der Zweckmäßigkeit im Sinn der Gebarungssicherheit bzw. Beweissicherung vorgesehen. Medienbrüche bzw. ein zusätzliches Verschicken auf Papier sollten unterlassen werden. Im Schriftverkehr mit anderen Dienststellen und den Bürgern der Stadt Wien wird den Dienststellen empfohlen, die elektronische Versendung mittels der offiziellen E-Mail-Postadressen im Sinn der elektronischen Kommunikation umzusetzen.

Der Erlass sieht weiters vor, dass der Empfänger von offiziellen Dienststellen-Postfächern einer Dienststelle davon ausgehen kann, dass die internen Unterschriftenregelungen der versendenden Dienststelle eingehalten werden.

Auch die elektronische Behandlung von Geschäftsstücken im Einsichtswege (Videnden) ist verstärkt umzusetzen.

Versendete Schriftstücke mit hoher Anforderung an Vertraulichkeit und Sicherheit sind mit einem einheitlichen zwischen MDO-IKT und Magistratsabteilung 14 abgestimmten Verschlüsselungsverfahren zu versehen. Weiters ist von den beiden Dienststellen ein Schlüsselverwaltungsverfahren umzusetzen, sodass im Fall eines Schlüsselverlustes unter Beachtung des Mehraugenprinzips die Schriftstücke entschlüsselt werden können. Die Verschlüsselungswerkzeuge und Schlüssel sind von der Magistratsabteilung 14 auf Anforderung der einzelnen Dienststellenleiter zur Verfügung zu stellen. Die Verwendung anderer Verschlüsselungswerkzeuge und Schlüssel ist untersagt.

3. Ergebnis der Prüfung des Kontrollamtes

Bei der vorliegenden Prüfung wurden wesentliche Punkte der angeführten Regelwerke unter dem Aspekt der Erfüllung der Mindestanforderungen im Umgang und beim Einsatz von E-Mails ausgewählt und anschließend deren Umsetzung beurteilt.

3.1 Arbeitsplatz

Die eingesetzten E-Mail-Programme (Clients) der Benutzer müssen durch die Magistratsabteilung 14 bzw. den lokalen Administrator so vorkonfiguriert sein, dass ohne weitere Mithilfe der Benutzer ausreichende Sicherheit erreicht wird. Die Benutzer sind darauf hinzuweisen, dass sie die Konfiguration nicht selbsttätig ändern dürfen bzw. können.

3.1.1 Passwortsicherheit

Das E-Mail-Passwort darf keinesfalls dauerhaft vom E-Mail-Programm gespeichert werden. Dabei wird das Passwort auf der Client-Festplatte abgelegt, u.U. sogar im Klartext oder nur schwach verschlüsselt.

Die Magistratsabteilung 14 erfüllte diese Forderung mittels des eingesetzten Mailverbundsystems Microsoft Exchange.

3.1.2 Adressen

Innerhalb einer Organisation sollten Adressbücher und Verteilerlisten gepflegt werden, um die Korrektheit der gebräuchlichsten Adressen sicherzustellen. Neben personenbezogenen E-Mail-Adressen können auch organisations- bzw. funktionsbezogene E-Mail-Adressen eingerichtet werden. Dies ist insbesondere bei zentralen Anlaufstellen wichtig.

Bei der Konfiguration der E-Mail-Clients muss die Adressierung von E-Mails eindeutig erfolgen, um eine fehlerhafte Zustellung zu vermeiden. Dabei ist die Korrektheit der durchgeführten Datenübertragungen zu überprüfen. Die Empfängerseite sollte den korrekten Empfang überprüfen und der Senderseite bestätigen.

Dies wurde im System der Magistratsabteilung 14 mit dem Microsoft Exchange-Verbund ebenfalls umgesetzt, sodass im internen Mailverkehr die Adressen eindeutig zuordenbar sind.

Die MDO-IKT sieht in ihrer E-Mail-Verhaltensempfehlung keine standardmäßige Aktivie-

rung der "Lese- bzw. Empfangsbestätigungen" Funktionen vor, da hiedurch ein starker E-Mail-Verkehr erzeugt wird.

Der eingesetzte Client (MS Outlook) hat jedoch für jeden Benutzer die auswählbare Einstellungsmöglichkeit, den Empfang bzw. den Lesevorgang quittieren zu können.

3.1.3 Absenderangaben

Zur Beschreibung des Absenders wird bei E-Mails eine so genannte Signatur - hiebei handelt es sich lediglich um eine Absenderangabe in Textform und keine elektronische Signatur - an das Ende der E-Mail angefügt. Der Inhalt einer Signatur sollte dem eines Briefkopfs ähnlich sein, also Name, Organisationsbezeichnung und Telefonnummer u.ä. enthalten. Eine Signatur sollte nicht zu umfangreich sein, da dies Übertragungszeit und Speicherplatz kostet. Es sollte ein vorgegebener Standard für die einheitliche Gestaltung von Signaturen vorgesehen sein.

Diese Forderung wurde mittels der E-Mail-Verhaltensempfehlung der MDO-IKT umgesetzt. Die eingefügte Signatur mit der Absenderangabe am Ende der E-Mails ist jedoch jederzeit leicht austauschbar und somit kein Garant für die Echtheit des Absenders.

Als Antwortadresse (Reply) ist die E-Mail-Adresse des Benutzers einzustellen, um sicherzustellen, dass keine internen E-Mail-Adressen weitergegeben werden. Die Betreffangabe (Subject) des Kommunikationssystems sollte immer ausgefüllt werden, z.B. entsprechend der Betreffangabe in einem Anschreiben. Eine aussagekräftige Betreffzeile ist nicht nur beim Einordnen der Relevanz der E-Mail hilfreich, sondern auch beim sofortigen bzw. automatischen Erkennen von "Spams" (unerwünscht zugesandte E-Mails, massenhafter Versand von Nachrichten).

Das Kontrollamt hat im Rahmen der Einschau die Möglichkeit der Veränderung der Absenderadresse einer Mail untersucht und dabei festgestellt, dass es bis zu der Einschau verwendete Standard SMTP (Simple Mail Transfer Protocol) erlaubte, eine beliebige Absenderadresse zu verwenden. Die Schnittstelle (SMTP) wird für den externen Mailverkehr verwendet und ist generell als nicht vertrauenswürdig und leicht manipulier-

bar eingestuft. Daher sollte darauf geachtet werden, dass diese Schnittstelle nur mit zusätzlichen Sicherheitsmaßnahmen verwendet wird. Aus diesem Grund werden E-Mails von der Magistratsabteilung 14, um eine missbräuchliche Verwendung interner Namen als Absender zu verhindern, an dieser Schnittstelle mit dem Vermerk *EXTERN* beim Absendernamen gekennzeichnet.

Das Kontrollamt hat jedoch festgestellt, dass es möglich war, auch interne E-Mails über diese Schnittstelle (SMTP) zu versenden. Derartige E-Mails wurden nicht mit der *EXTERN*-Markierung gekennzeichnet. Die Magistratsabteilung 14 reagierte nach Aufzeigen dieses Umstandes und stattete das E-Mail-System mit neuen Zugangsregelungen aus, sodass E-Mails erst nach erfolgreicher Identifizierung und Authentisierung des Stadt Wien E-Mail-Verbund-Benutzers gesendet werden können. Ursache für den Fehler war lt. Magistratsabteilung 14 die zu diesem Zeitpunkt laufende Vereinfachung und Umstrukturierung der Internet-Mailanbindung, die durch den Einsatz der neuen Exchange Version 2003 verursacht wurden. Die Umbauarbeiten selbst wurden Ende November abgeschlossen. Danach wurde das gesamte System sowohl vom Hersteller Microsoft als auch von der Magistratsabteilung 14 einer internen Sicherheitsüberprüfung unterzogen. Nach Aussage der Magistratsabteilung 14 sind E-Mails innerhalb des internen Mail-System-Verbunds sowohl vom Inhalt als auch von der Absenderadresse nunmehr fälschungssicher und in diesem Bereich keine zusätzlichen Sicherungsmaßnahmen erforderlich.

Die daraufhin vom Kontrollamt durchgeführten Tests haben gezeigt, dass die Absenderadresse (From) im aktuellen System der Magistratsabteilung 14 nicht mehr vom Benutzer verändert werden konnte, die Echtheit der Absenderangabe war damit gewährleistet. Dies galt jedoch nur für den Zeitpunkt der durchgeführten Tests, bei Veränderungen des Systems (Update, Upgrade, Tausch von Komponenten) können neuerlich sicherheitsrelevante Probleme auftreten. Daher war zu empfehlen, dass zusätzlich zu den technischen Vorkehrungen ein davon abgekoppeltes organisatorisches Instrument für ausreichende Sicherheit sorgen sollte. Hiefür käme der Einsatz einer elektronischen Signatur infrage, wie er auch in der E-Mail-Policy vorgesehen ist.

Stellungnahme der Magistratsabteilung 14:

Um die Echtheit von Absenderangaben und auch prinzipiell eine gesicherte Herkunft von internen Mails zu gewährleisten, werden zusätzliche Maßnahmen, die Fehler durch Veränderungen des Systems (Update, Upgrade, Tausch von Komponenten) abfangen sollen, empfohlen. Die Magistratsabteilung 14 hat daher eine tägliche automatische Überprüfung des Mailingsystems auf Fehlverhalten implementiert. Damit wird sichergestellt, dass keine unbeabsichtigten Änderungen in diesem Bereich erfolgen.

3.1.4 Elektronische Signatur

Die Verwendung von elektronischen Signaturen im E-Mail-Verkehr führt zur Hebung der Sicherheit, des Schutzes der Vertraulichkeit bzw. der Integrität von Daten sowie zur Authentisierung. Damit können E-Mails unabhängig von den eingesetzten technischen Einrichtungen eindeutig den Absenderadressen zugeordnet werden. Diese Maßnahme verbessert die Qualität des Kommunikationsmediums E-Mail.

Das Kontrollamt empfahl, bei der Zuteilung elektronischer Signaturen an Bedienstete der Stadt Wien selektiv vorzugehen. Der Aufwand sollte in Relation zu dem daraus zu erwartenden Effizienz- und Nutzengewinn stehen. Als Zuteilungsgrundlage sollte die organisatorische Stellung des Bediensteten (Umfang der Weisungsbefugnis) bzw. die Bedeutung der Funktion (Erfüllung behördlicher Aufgaben bzw. finanzielle Auswirkungen) herangezogen werden.

Die Verwendung elektronischer Signaturen bei E-Mails ist möglich. Die von den Anwendern dafür benötigten Zertifikate können bei der Magistratsabteilung 14 angefordert werden.

3.1.5 Verschlüsselte E-Mails

Mit zunehmender Bedeutung der elektronischen Kommunikation nimmt der Bedarf der öffentlichen Verwaltung an Verfahren zur Vertraulichkeit von E-Mails zu. Es ist Aufgabe der verantwortlichen Dienststelle festzulegen, ob bzw. unter welchen Bedingungen Ver-

schlüsselungsverfahren einzusetzen sind. Das Interesse an der Aufrechterhaltung des Betriebes sollte immer im Vordergrund stehen.

Die MDO-IKT hat in ihrem Kommunikationserlass MDO-337-11/04 die Entscheidung in der Form getroffen, dass bei elektronischer Kommunikation, bei der eine hohe Anforderung an Vertraulichkeit und Sicherheit des Absenders gegeben ist, die seitens der Magistratsabteilung 14 zur Verfügung gestellten Einrichtungen zu verwenden sind. Die Magistratsabteilung 14 hat einheitliche, mit der MDO-IKT abgestimmte Verschlüsselungsverfahren einzusetzen.

Verschlüsselte Nachrichten können im Allgemeinen nicht zentral auf Viren überprüft werden. Dazu wäre die zentrale Hinterlegung der notwendigen Schlüssel erforderlich, da alle verschlüsselten Mails für das Scannen nach Viren geöffnet werden müssten. Die Virenprüfung würde am Arbeitsplatz nach dem Entschlüsseln der Nachrichten stattfinden.

Bei einer Abwägung von Risiko und Nutzen sah das Kontrollamt im Einsatz von Verschlüsselungsverfahren eine Verbesserung des Schutzes vor unberechtigtem Zugriff und eine bessere Gewährleistung der Verbindlichkeit und der Vertrauenswürdigkeit von Geschäftsprozessen und Verwaltungsabläufen der Stadt Wien auf digitaler Basis. Deshalb sollte geregelt sein, wie und wann übertragene Dateien verschlüsselt werden müssen. Gleichermaßen ist festzulegen, in welcher Form kryptographische Mechanismen zur Überprüfung der Integrität von Daten wie z.B. MACs (Message Authentication Code), Digitale Signaturen usw. eingesetzt werden müssen.

Die Charakteristik von verschlüsselten E-Mails im internen E-Mail-Verkehr lässt die potenzielle Virengefahr auf ein sehr geringes Restrisiko sinken und es kann auch davon ausgegangen werden, dass verschlüsselte E-Mails keine Spams darstellen. Verschlüsselte E-Mails können nicht von Virenscannern und Spamfiltern von zentraler Stelle übergreifend geprüft werden, es müssten Gruppen-Verschlüsselungszertifikate zum Einsatz kommen.

Für die Magistratsabteilung 14 ergeben sich für die praktische magistratsweite Nutzung nicht zuletzt auf Grund des Kommunikationserlasses organisatorische Hindernisse in Bezug auf Verwendung der Dienststellen-Postfächer sowie genereller Stellvertreterregelungen, für die es zur Zeit der Einschau des Kontrollamtes kein organisatorisches Gesamtkonzept gab.

> In Abstimmung mit der Magistratsdirektion/Geschäftsbereich Organisation, Gruppe Informations- und Kommunikationstechnologie ergeht zur Empfehlung des Kontrollamtes folgende Stellungnahme:
>
> Wenngleich die zusätzliche Verschlüsselung einzelner interner Mails zweifellos einen gewissen zusätzlichen Vertraulichkeitsgewinn bedeuten würde, wären die dabei anfallenden Kosten und Aufwände sowie die im Bericht bereits erwähnten zu erwartenden Probleme (Stellvertreterregelung, Dienststellen-Postfächer, Empfänger muss Zertifikat besitzen, Wiederherstellung bei Schlüsselverlust) nicht unerheblich.

3.1.6 Dateianhänge der E-Mails

Erfolgt über eine E-Mail auch eine Dateiübertragung, so sollten die folgenden Informationen an den Empfänger zusätzlich übermittelt werden:

- Art der Datei (z.B. Dokumente, Tabellen, Präsentationen usw.),
- Kurzbeschreibung für den Inhalt der Datei,
- Hinweis, dass Dateien auf Viren überprüft sind,
- gegebenenfalls Art des verwendeten Packprogramms,
- gegebenenfalls Art der eingesetzten Software für Verschlüsselung.

Jedoch sollte nicht vermerkt werden,

- welches Passwort für die eventuell geschützten Informationen vergeben wurde,

- welche Schlüssel gegebenenfalls für eine Verschlüsselung der Informationen verwendet wurden.

E-Mails, deren Beilagen ausführbare Programme sind, sind im Allgemeinen abzuweisen. Potenziell gefährlicher Inhalt sollte geblockt werden, um bereits präventiv vom Virenscanner unerkannte Angriffe gar nicht zuzulassen. Zu den potenziell gefährlichen Inhalten zählen z.B.

- jeglicher ausführbarer Inhalt oder
- Inhalte mit Formatverletzungen (z.B. Archive mit falschen Inhaltsangaben).

Außerdem können jene Dateien abgewiesen werden, bei denen angenommen werden kann, dass sie nicht für dienstliche Zwecke bestimmt sind.

Die Magistratsabteilung 14 veröffentlicht jene Dateiformate, die aus Sicherheitsgründen eine Einschränkung bezüglich der Verwendung von beigefügten Dateien beim Mail-Verkehr erforderlich machen. Diese Restriktion soll die Verbreitung von Viren erschweren. Die Erkennung der Dateien erfolgt ausschließlich auf Grund ihrer Datei-Endung. Diese Dateianhänge können mit dem Client weder geöffnet noch gespeichert werden. Vor dem Versenden von solchen Dateianhängen wird der Benutzer mit einer Dialogbox gewarnt, wobei diese Warnung mit Mausklick bestätigt werden muss. Jedoch wird vor der Übertragung der E-Mail der Dateianhang entfernt und gelöscht; auf diese Art kann man keinen Zugriff auf den Dateianhang erhalten. Beim Weiterleiten (Forwarding) von solchen Mails wird der Dateianhang ebenfalls entfernt und gelöscht. Alle anderen Datei-Typen - insbesondere die Schriftstücke aus dem Microsoft Office-Bereich - werden ebenfalls auf Viren untersucht. Die Empfänger der Stadt Wien sind jedoch angehalten, diese Dateien nur mit gedrückter Shift-Taste zu öffnen, um das automatische Starten von Makros zu unterbinden.

Ausnahmen von der Filterung von Dateiformaten bzw. Dateiendungen sollten nach Möglichkeit nicht durch Umgehung (z.B. durch Komprimieren mit Passwort oder dgl.), sondern durch organisatorische Maßnahmen gelöst werden.

Bei der Einschau stellte das Kontrollamt fest, dass mit bzw. ohne Passwort geschützte Packprogramme - so genannte ZIP-Archive, welche Dateien mit gesperrten Dateiendungen beinhalteten, versendet werden konnten und in einem Fall, obwohl sie einen Virus beinhalteten, zugestellt wurden. Des Weiteren war es auch möglich, einzelne Dateien durch Ändern der gesperrten Dateiendungen auf gültige Dateiendungen zu versenden.

Das Kontrollamt empfahl der Magistratsabteilung 14, gemeinsam mit der MDO-IKT entsprechende Maßnahmen zu setzen, um den Schutz weiter zu verbessern.

Die aufgezeigte Möglichkeit, gesperrte Dateiendungen durch Verpacken in ZIP-Archive oder durch Umbenennen auf eine nicht gesperrte Dateiendung übertragen zu können, stellt kein erhöhtes Risiko dar und ist allgemein üblich. Die Sperre von Dateiendungen soll deren Übertragung nicht generell blockieren. Sie soll nur verhindern, dass Schadprogramme im funktionsfähigen Zustand übertragen werden und dadurch beim Empfänger unbeabsichtigt zur Ausführung kommen können.

Im dargestellten Einzelfall eines bis zum Arbeitsplatz durchgekommenen Virus geschah dies in der knappen Zeit zwischen dem Auftauchen des neuen Virus und der Verteilung der neuen Erkennungsdaten durch die Virenscannerhersteller. Der Virus wurde später durch den Virenschutz automatisch erkannt und deaktiviert.

Wie der Bericht des Kontrollamtes im Pkt. 4.1 ausführt, kann eine absolute Sicherheit nicht gewährleistet werden. Die umfangreichen Maßnahmen, die zur Abwehr unerwünschter oder schädlicher Inhalte getroffen wurden, werden regelmäßig überprüft und bei neuen Erkenntnissen bzw. neu auftauchenden Gefahren ergänzt und ausgeweitet.

3.1.7 Aufbewahrung von E-Mails

Für E-Mails, die nicht gelöscht werden, ist eine Archivierung und Sicherung vorzusehen.

Wie die Einschau ergab, gab es seitens der Magistratsabteilung 14 keine Regelungen, wie E-Mails archiviert werden konnten. Die Sicherung und Archivierung obliegt in diesen Fällen der Verantwortung des Benutzers selbst. E-Mails werden daher in Papierform archiviert oder nach eigenem Ermessen auf Datenträger gesichert und aufbewahrt. So verbleiben diese E-Mails auf dem Arbeitsplatzcomputer bzw. einem Netzlaufwerk.

Die Magistratsabteilung 14 arbeitete an einer Umsetzung eines Archivierungskonzeptes für E-Mails. Dieses wird in das bestehenden Exchange E-Mail-Verbund-System integriert werden. Damit sollte eine einheitliche, standardisierte Lösung der E-Mail-Archivierung im Sinn des Datenschutzes und der Datensicherheit geschaffen werden.

3.2 Serverseitige Aufgaben betreffend E-Mail

3.2.1 Eingesetztes Produktionssystem

Der sichere Betrieb eines Mailservers setzt voraus, dass sowohl die lokale Kommunikation als auch die Kommunikation auf Seiten des öffentlichen Netzes abgesichert wird. Der Mailserver nimmt von anderen Mailservern E-Mails entgegen und leitet sie an die angeschlossenen Benutzer oder Mailserver weiter. Ebenso reicht der Mailserver die gesendeten E-Mails lokaler Benutzer an externe Mailserver weiter. Der Mailserver muss hiebei sicherstellen, dass lokale E-Mails der angeschlossenen Benutzer nur intern weitergeleitet werden und nicht in das öffentliche Netz gelangen können. Die E-Mails werden vom Mailserver bis zur Weitergabe zwischengespeichert.

Damit Unbefugte nicht über den Mailserver auf Nachrichteninhalte zugreifen können, muss der Mailserver gegen unbefugten Zugriff gesichert sein (vgl. dazu § 126a StGB zu Datenbeschädigung, BGBl.Nr. 60/74 idgF). Dafür sollte er räumlich gesichert in einem Serverraum oder Serverschrank aufgestellt sein. Für den ordnungsgemäßen Betrieb sind Administrator und Stellvertreter zu benennen und zum Betrieb des Mailservers und des zu Grunde liegenden Betriebssystems zu schulen. Der Mailserver sollte ein abgeschlossenes, eigenes Produktionssystem darstellen, insbesondere sollten von der Ver-

fügbarkeit des Mailservers keine weiteren Dienste abhängig sein. Es sollte jederzeit kurzfristig möglich sein, ihn - z.B. bei Verdacht auf Manipulationen - abzuschalten.

Die Sicherung der Daten des E-Mail-Systems ist als Bestandteil einer IT-Sicherheitsrichtlinie zu sehen, die für das EDV-System selbst definiert wurde. In diesem Rahmen sind auch die Backup- und Restoreverfahren des E-Mail-Systems festzulegen.

Das eingesetzte System der Magistratsabteilung 14 ist der Exchange 2003 Server der Firma Microsoft und befindet sich räumlich getrennt an mehreren Orten. Zur Zeit der Einschau des Kontrollamtes bestand diese Rechenanlage aus neun einzelnen Servern, die von der Magistratsabteilung 14 betreut wurden. Der Exchange 2003 Server ist ein Managementsystem für Nachrichten und dazu gedacht, in mittleren bis großen Behörden bzw. Unternehmen den internen und externen E-Mail-Verkehr zu regeln. Ebenso werden Newsgroups, Kalender, Kontakte und Verteilerlisten verwaltet.

Outlook 2003 bzw. das auch noch während der Einschau im Einsatz befindliche Outlook 2000 sind Bestandteile des Office 2000- bzw. Office 2003-Pakets der Firma Microsoft. Es handelt sich hiebei um eine typische Client-Server-Anwendung, wobei Exchange 2003 die Server- und Outlook 2000/2003 die Client-Komponente darstellt.

Die Magistratsabteilung 14 geht nach einem intern festgelegten Sicherungskonzept vor, welches die Sicherungs-, Wiederherstellungs- und Archivierungsmaßnahmen der Exchange 2003 Server regelt.

Die Datensicherung erfolgt mit der Software Networker von der Firma Legato auf Magnetbandkassetten mittels Bandroboter in der Magistratsabteilung 14.

Täglich wird eine Vollsicherung der gesamten Exchange Datenbank erstellt. Tagessicherungen werden mindestens zwei Wochen aufbewahrt, bevor die Bänder wieder überschrieben werden. Wochensicherungen werden zwölf Wochen aufbewahrt.

Zwischen den einzelnen Servern an den einzelnen Standorten wird aus Sicherheits-

gründen wöchentlich wechselseitig gesichert. Damit sollte auch bei vollständigem Datenverlust in einem Computerraum - wie z.B. durch einen Brand - eine Sicherung vorhanden sein, die höchstens eine Woche alt ist.

Die Wiederherstellung (Restore) von E-Mails aus den Sicherungskassetten ist in einem Zeitraum von längstens drei Monaten möglich.

3.2.2 Benutzerkonten

Die Benutzernamen auf dem Mailserver sollten nicht aus den E-Mail-Adressen unmittelbar ableitbar sein, um mögliche Angriffe auf Benutzeraccounts zu erschweren.

Dies war im System der Magistratsabteilung 14 noch nicht umgesetzt.

> Es ist geplant, nach Vorliegen entsprechender Regelungen zur Unterscheidung von Personen mit Namensgleichheit, Adressen der Form Vorname.Nachname@... einzuführen.

3.2.3 Protokollierung und Logging

Grundsätzlich sollen unter Einhaltung der Datenschutzanforderungen nur jene Daten protokolliert werden, die für die Sicherung der Funktionsweise des Systems und für die Einhaltung der organisatorischen und gesetzlichen Vorgaben benötigt werden.

Die Magistratsabteilung 14 protokolliert und archiviert die Metadaten der E-Mails in Protokolldateien. Diese Dateien dienen dazu, um die Nachvollziehbarkeit im Sinn des Datenschutzgesetzes (DSG) 2000 und die Klärung von Problemfällen zu gewährleisten. Liegt ein begründeter Verdacht auf rechtswidriges oder von der Norm abweichendes Verhalten vor, so können in Abstimmung mit der Personalvertretung gemäß dem Erlass über die "Einschau in Mailboxen" vom 27. Oktober 2004, MDO-46/04, Auswertungen vorgenommen werden.

3.2.4 Transport der E-Mails durch das interne Netzwerk

Bei den eingesetzten E-Mail-Systemen können die Informationen unverschlüsselt über

offene Leitungen transportiert und auf diversen Zwischenrechnern gespeichert werden, bis sie schließlich ihren Empfänger erreichen. Auf diesem Weg können Informationen manipuliert werden. Die internen elektronischen Netzwerke der Stadt Wien sind als gesicherte Bereiche eingerichtet und vom externen Internet abgekoppelt.

Bei dem ursprünglich eingesetzten E-Mail-Client-Programm der Magistratsabteilung 14 (Microsoft Outlook 2000) bestand keine Verschlüsselung der Transportebene. Im neuen Exchange Mail-Verbund, bestehend aus den Outlook 2003 E-Mail-Clients und den Exchange 2003-Servern, wird nunmehr der Transport verschlüsselt. Das Abhören und Auswerten von Netzwerkpaketen wird durch den Einsatz dieses Produktes der Firma Microsoft unterbunden.

Zum Zeitpunkt der Prüfung befand sich das neue E-Mail-Client-Programm (Microsoft Outlook 2003) in der Roll Out-Phase und wurde bereits von nahezu 95 % der Bediensteten der Stadt Wien verwendet. Die vollständige Umstellung sollte bis Jänner 2006 abgeschlossen sein.

Es stehen auch angemietete Leitungen in Verwendung, die mit dem als sehr sicher geltenden Schutzmechanismus eines virtuellen privaten Netzwerks (VPN) betrieben werden. Die Verbindung über das öffentliche Netz wird hiebei verschlüsselt.

> Die Magistratsabteilung 14 hat den gesamten Transportweg der internen Mails bereits auf Verschlüsselung umgestellt. Lediglich die Speicherung der Mails am Server erfolgt unverschlüsselt. Die eingesetzten Serversysteme sind gegen unbefugten Zugriff gesichert. Nach der Ansicht der Magistratsabteilung 14 genügen diese Vorkehrungen für interne Mails sogar den strengen Anforderungen des Gesundheitstelematikgesetzes (GTelG).

3.2.5 E-Mail-Transferprotokolle

Das generelle Ziel der E-Government-Strategie sollte die Einrichtung der Kommunikation nach offenen international verfügbaren und anerkannten Standards sein. Nur so

können Interoperabilität, Kompatibilität und eine weite Verbreitung erreicht werden.

Daher wurde in der E-Mail-Policy für die Kommunikation zwischen Client und Server im E-Mail-Verkehr, sowie zwischen E-Mail-Servern nachstehende Protokolle festgelegt:

- SMTP Simple Mail Transfer Protocol,
- POP3 Post Office Protocol - Version 3,
- IMAP Internet Message Access Protocol.

Davon wird im Bereich der Magistratsabteilung 14 das SMTP-Protokoll eingesetzt.

Unter Einhaltung der genannten Kompatibilitätsanforderungen kann zur Erreichung einer höheren Funktionalität die Kommunikation zwischen Server und Client auch auf Basis von proprietären (herstellerspezifischen) Protokollen stattfinden. Der Einsatz von derartigen Protokollen (z.B. MAPI mit MS-Exchange, Abkürzung für "Messaging Application Programming Interface", eine Schnittstelle von Microsoft) setzt voraus, dass diese in die Sicherheitsrichtlinie eingebunden werden.

Das eingesetzte Mail-Verbund-System der Magistratsabteilung 14 unterstützt nicht nur die offenen Standards, wie POP3, SMTP und IMAP. Die volle Funktionalität kann das Mailprogramm der Firma Microsoft nur über das MAPI-Protokoll erreichen, wobei entsprechende Sicherheitsvorkehrungen seitens der Magistratsabteilung 14 getroffen worden sind.

Da E-Mails aus verschiedenen Inhalten bestehen, wie z.B. aus Texten, Bildern, Dateien, gelten für diese so genannten Bodyparts verschiedene Kodierungsalgorithmen, die sich nach folgenden Standards orientieren:

MIME ist die Abkürzung für Multipurpose Internet Mail Extensions. Hiebei handelt es sich um einen Kodierungsstandard, der die Struktur und den Aufbau von E-Mails festlegt.

Es gibt eine Erweiterung dieses Standards namens S/MIME (Secure MIME) bzw. CMS (Cryptographic Message Syntax), die für die digitale Unterzeichnung, Verarbeitung, Authentisierung und Verschlüsselung von rechtlich relevanten Nachrichten entwickelt wurde.

Es wurde seitens der Magistratsabteilung 14 darauf geachtet, dass die eingesetzten E-Mail-Server und Clients diese Standards unterstützen. Bei der internen Kommunikation wurden diese Protokolle bisher nicht eingesetzt.

4. Schutzmaßnahmen

Eingehende E-Mails sollten an der Firewall (d.i. jener Rechner, der das interne Netz gegenüber dem Internet absichert) oder am Mailserver auf Viren und andere schädliche Inhalte überprüft werden.

4.1 Schutz vor Viren

Vor dem Absenden bzw. vor dem Eingang der Dateiübermittlung sind die Daten explizit auf Viren zu überprüfen. Gegen Malware - ist die Abkürzung für "malicious software" und bedeutet in etwa "bösartige Software" - bei E-Mails können Gegenmaßnahmen auf mehreren Ebenen (Virenscannung am Client, am Server und im Netzwerk) gesetzt werden. Der Virenscan kann an verschiedenen Punkten der Informationsübermittlung geschehen. Danach richten sich auch die Möglichkeiten und die Art und Weise der Reaktion.

Im Idealfall kann der MTA (Mail Transfer Agent) der Organisation eine mit Malware infizierte E-Mail bereits bei der Entgegennahme erkennen. Dann besteht für den MTA die Möglichkeit, diese E-Mail schon während der Übermittlung über SMTP abzulehnen. Um Timing und Systemlastproblemen vorzubeugen, können Scanner nicht direkt am MTA die eingehenden E-Mails überprüfen. Ein zwischen MTA und Client eingefügter E-Mail-Proxy kann die Aufgabe übernehmen und ausschließlich für diesen Zweck vorgesehene E-Mails während der SMTP-Bearbeitung behandeln.

Eine weitere Untersuchung auf Viren kann am Client selbst erfolgen, nachdem die E-

Mail bereits im Postfach zugestellt wurde. Bei der Virenprüfung am E-Mail-Client (z.B. MS Outlook) wird der Benutzer vom Scanprogramm bei Virenbefall über das Ergebnis informiert.

Ein weiterer wesentlicher Aspekt zur Bekämpfung von derartigen Schädlingen ist die umfassende Aufklärung der Benutzer. Es ist daher zu achten, dass die Benutzer über die Gefahren aufgeklärt werden bzw. sich informieren können. Unter anderem gilt dies für Hoax E-Mails (Hoax: engl. Jux, Schabernack), die an sich keine Gefahr darstellen. Auswirkungen können sie jedoch dann haben, wenn die Benutzer den Anweisungen Folge leisten.

Wie die Einschau ergab, wurden der Stadt Wien im Monat durchschnittlich rd. 7,40 Mio. E-Mails zugestellt. An der Firewall der Magistratsabteilung 14 wurden davon durchschnittlich 5,70 Mio. Malware und Hoax E-Mails als nicht erwünscht erkannt und abgewiesen.

Auf den Exchange-Servern der Magistratsabteilung 14 wurde das Programm Antigen von der Firma Sybari eingesetzt. Dieses Programm prüft die eingehenden E-Mails mit fünf verschiedenen Antivirenprogrammen der Firmen Kaspersky, Sophos, Norman Data Defense, CA InoculateIT und CA VET auf Viren. Da diese Antivirenprogramme unabhängig voneinander suchen, steigt die Wahrscheinlichkeit der Virenerkennung.

Dateianhänge der E-Mails werden immer geprüft. Die Zahl der geblockten Dateianhänge betrug zur Zeit der Einschau des Kontrollamtes 43 Dateiformate.

Die Aktualisierung der Antivirenprogramme wird einmal pro Stunde durchlaufen, wobei zwischen den unterschiedlichen Antivirenprogrammen ein Intervall von zehn Minuten liegt. Zusätzlich läuft am Wochenende auf allen Exchange-Servern eine komplette Überprüfung aller Daten.

Auf der Client-Seite wird von der Magistratsabteilung 14 die Desktop Antivirenlösung der Firma McAfee zur zusätzlichen Virenabwehr eingesetzt.

Das Kontrollamt konnte sich davon überzeugen, dass umfangreiche Maßnahmen zur Abwehr von Schadprogrammen getroffen wurden. Eine absolute Sicherheit kann jedoch nicht gewährleistet werden, da das Bedrohungspotenzial sich permanent verändert. Wie bereits in Pkt. 3.1.6 erwähnt, ist es möglich, dass Schadprogramme als Beilagen zu E-Mails in die Postfächer der Benutzer gelangen. Dem Benutzer steht mit der Desktop Antivirenlösung der Firma McAfee ein leistungsfähiges Instrument zur Erkennung dieser Schadprogramme zur Verfügung. Die Information über derartiges Eindringen wird vom Antivirenprogramm per E-Mail an die Magistratsabteilung 14 übermittelt. Diese Informationen werden derzeit manuell ausgewertet. Auf Grund des zeitweise großen Volumens wäre eine automatisierte Analyse zweckmäßig und würde eine verbesserte Erkennung von derartigen Programmen unterstützen.

Eine Analyse, wie im Bericht angeregt, ist bereits im Einsatz. Die Antivirenlösung von McAfee sammelt automatisch die Informationen über erkannte Viren oder Schadprogramme in einer Datenbank. Daraus ist das aktuelle Virenaufkommen jederzeit ersichtlich. Bei Bedarf kann darüber hinaus ein Drill-down bis zu den betroffenen Arbeitsplätzen erfolgen. Berechtigte können sich auch per E-Mail über das Virenaufkommen informieren lassen.

4.2 Spams

Unerwünschte, massenweise verschickte E-Mail-Nachrichten werden als Spams bezeichnet. Um diesen entgegenzuwirken, bedarf es so genannter Spam-Filter, die sich sowohl auf Server- als auch auf Client-Seite befinden können.

4.2.1 Aktive Abwehrmaßnahmen

Spam-Filter ermöglichen die Analyse von Header (= Kopfzeilen) und Body (= Inhalt) einer E-Mail nach unterschiedlichen Kriterien und geben eine Einschätzung über die Wahrscheinlichkeit ab, ob die untersuchte Nachricht ein Spam darstellt oder nicht.

Da Spam-Versender in der Regel Ihre E-Mails nicht als UBE ("Unsolicited Broadcast Email") kennzeichnen, existieren zur Analyse eingehender Nachrichten keine objektiven

Kriterien. Aktuelle Spam-Filter arbeiten daher mit verschiedenen Bewertungsverfahren, um Spams hinreichend genau zu erkennen. Das Auftreten mehrerer Merkmale erhöht dabei die Wahrscheinlichkeit und durch das Überschreiten eines Schwellenwertes wird eine positive Erkennung indiziert. Wird eine E-Mail als Spam klassifiziert, kann die Nachricht auch in Quarantäne gestellt werden.

Hiebei sollte festgelegt werden, wie lange die E-Mail aufgehoben wird bzw. ob der Empfänger Zugriff zu den eingelangten E-Mails erhält.

An der Firewall können mit Filterregeln für bestimmte E-Mail-Adressen der Empfang oder die Weiterleitung von E-Mails gesperrt werden. Hiebei muss mit Bedacht vorgegangen werden, damit der Filterung keine erwünschten E-Mails zum Opfer fallen. Daher sollten entsprechende Filterregeln sehr genau definiert werden, indem beispielsweise aus jeder Spam-Mail eine neue dedizierte Filterregel abgeleitet wird. Entsprechende Filterlisten sind im Internet verfügbar bzw. können von verschiedenen Herstellern der Kommunikationssoftware bezogen werden. Es ist festzulegen, welche Protokolle und Dienste am Mailserver erlaubt sind.

Ein Mailserver sollte davor geschützt werden, als Spam-Relay verwendet zu werden. Dafür sollte ein Mailserver so konfiguriert werden, dass er E-Mails nur für die Organisation selber entgegennimmt und nur E-Mails verschickt, die von Mitarbeitern der Organisation stammen.

Entsprechende Maßnahmen wurden von der Magistratsabteilung 14 umgesetzt und laufend verbessert. Zusätzlich wurden auch Verbesserungen auf der Client-Seite vorgenommen, um Spams effizienter Einhalt zu bieten. Auf Grund des großen Umfangs und der großen Variation von derartigen E-Mails ist allerdings eine vollständige Erkennung mit dem derzeitigen Stand der Technik nicht durchführbar.

4.3 Information

Um den Bediensteten der Stadt Wien einen Überblick und die aktuellen Erkenntnisse über die neuesten Viren, über Malware und Spaming zugänglich zu machen, wird das

Intranet der Stadt Wien eingesetzt. Die Magistratsabteilung 14 hat dafür eine spezielle Seite innerhalb ihres Angebotes eingerichtet, auf der derartige Informationen veröffentlicht werden.

5. Bedienungshinweise

Die Benutzer müssen vor erstmaliger Nutzung von E-Mail in die Handhabung der relevanten Applikationen eingewiesen werden. Die organisationsinternen Benutzerregelungen zur Dateiübermittlung müssen ihnen bekannt sein.

Alle Regelungen und Bedienungshinweise zum Einsatz von E-Mail sind schriftlich zu fixieren und sollten den Mitarbeitern jederzeit zur Verfügung stehen.

Die Benutzer müssen vor dem Einsatz von Kommunikationsdiensten, wie E-Mail, geschult werden, um Fehlbedienungen zu vermeiden und die Einhaltung der organisationsinternen Richtlinien zu gewährleisten.

Hiefür eignet sich ein E-Learning-Konzept für die Basisdefinitionen der E-Mail-Richtlinien, das um Ergänzungen für den internen Betrieb erweitert werden kann. Dieses E-Learning-Konzept soll im Rahmen der Einrichtung von E-Mail-Zugängen eingesetzt werden. Für die bereits aktiven Benutzer sind Vorkehrungen zu treffen, die den Erwerb dieses Wissens sicherstellen.

Diese Anforderung wird in der Stadt Wien durch die "Sicherheit in der Informations- und Kommunikationstechnologie (IKT)"-Richtlinie inkl. Beilage und Glossar sowie die E-Mail-Verhaltensempfehlung der MDO-IKT umgesetzt.

Erweiterungen und Ergänzungen finden sich in der virtuellen Verwaltungsakademie (ViVA), dem E-Learning-Angebot der Stadt Wien der Magistratsdirektion - Geschäftsbereich Personal und Revision, Gruppe Verwaltungsakademie und Personalentwicklung (MVA).

Auch steht in der Stadt Wien ein umfangreiches Kurs- und Schulungsprogramm für den

Umgang mit diesem elektronischen Medium zur Verfügung. Aktualisierungen finden sich im Online-Skriptenangebot der MVA.

6. Private Nutzung der E-Mails

Es ist festzulegen, ob und gegebenenfalls in welchem Rahmen eine private Nutzung von E-Mail-Diensten zulässig ist. Diese Festlegung sollten in schriftlicher Form getroffen werden. Weiters sind auch die zulässigen Kontrollmaßnahmen des Arbeitgebers (Protokollierung, Auswertung ...) und die möglichen Sanktionen bei Verstößen gegen die getroffenen Vereinbarungen zu regeln.

In den einschlägigen Bestimmungen für den Umgang mit E-Mails wie der Geschäftsordnung für den Magistrat der Stadt Wien (§ 57 GOM - Private Nutzung von dienstlichen Kommunikationseinrichtungen) und der Dienstanweisung "Internet und elektronische Kommunikation Richtlinie" werden mögliche Gefährdungen und einzuhaltende Sicherheitsmaßnahmen beim Versenden bzw. Empfangen von E-Mail geregelt.

Die private Nutzung von E-Mail für private Zwecke sind den Mitarbeitern im unumgänglich notwendigen Ausmaß gestattet. Weitere wesentliche Punkte dieser internen Richtlinie umfassen die Belehrung zur Vermeidung von Überlastung des E-Mail-Systems durch potenzielles Fehlverhalten. Ebenso wird vor der Teilnahme an E-Mail-Kettenbriefen, vor Spams, der unnötigen Weiterverbreitung von Virenwarnungen sowie vor der Abonnierung umfangreicher Mailinglisten gewarnt.

Anwender werden darauf hingewiesen, dass Dateien, deren Inhalt pornografischer, rassistischer, sexistischer oder ähnlicher Natur ist, weder verschickt, noch auf Informationsservern eingestellt, noch nachgefragt werden dürfen.

Außerdem haben die Benutzer darauf zu achten, dass bei der Nutzung von Kommunikationsdiensten die fahrlässige oder gar vorsätzliche Unterbrechung des laufenden Betriebes unter allen Umständen vermieden werden muss (vgl. dazu § 126a StGB zu Datenbeschädigung, BGBl.Nr. 60/74 idgF). Zu unterlassen sind insbesondere Versuche, ohne Autorisierung Zugang zu Netzdiensten - welcher Art auch immer - zu erhalten

bzw. Informationen, die über die Netze verfügbar sind, zu verändern, in die individuelle Arbeitsumgebung eines Netznutzers einzugreifen oder unabsichtlich erhaltene Angaben über Rechner und Personen weiterzugeben.

Diese Vorgabe wird, wie sich das Kontrollamt überzeugen konnte, bereits beim Dienstantritt von neuen Bediensteten in der Stadt Wien durch den Geschäftsbereich Personal und Revision (MD-PR) im Rahmen der so genannten "Newcomer-Schulung" zur Kenntnis gebracht.

7. Verfügbarkeit

Generell ist zu beachten, dass bei der Nutzung von Internetdiensten bezüglich deren Verfügbarkeit keine verbindliche Aussage getroffen werden kann. Der Transport von E-Mails ist von einer Summe von Netzwerkdiensten abhängig, deren Funktionalitäten üblicherweise nicht durch den Sender oder Empfänger beeinflussbar sind. Eine Aussage über die Transportdauer kann ebenso wenig getroffen werden. Die von der öffentlichen Verwaltung betriebenen Posteingangsserver-Systeme sollten im Regelfall 24 Stunden am Tag zur Verfügung stehen und zum Empfangen und Versenden von E-Mails bereit sein.

Innerhalb des Exchange Mail-Verbund-Systems ist nach Aussage der Magistratsabteilung 14 die Zustellung der E-Mails garantiert. Die Verfügbarkeit der Exchange-Server liegt nach den Berechnungen während der üblichen Bürodienstzeit in der Regel bei 100 %. Wartungsarbeiten und notwendige Updates werden in vordefinierten Wartungsfenstern immer an Wochenenden erledigt. Zur Zeit der Einschau waren zwölf Wartungsfenster pro Jahr vorgesehen, wobei der Betrieb während dieser Zeit nicht immer eingestellt werden musste.