City of Milwaukee

W. Martin Morics, C.P.A.
Comptroller

Michael J. Daun
Deputy Comptroller

John M. Egan, C.P.A.
Special Deputy Comptroller

Craig D. Kammholz
Special Deputy Comptroller

Office of the Comptroller

November 9, 2010

To the Honorable Common Council
City of Milwaukee

Dear Council Members:

As a component of the Comptroller's comprehensive information systems audit work plan, KMPG was engaged to complete the external network security and wireless vulnerability test of the City's computer network. The Comptroller's Office recently received the enclosed final report detailing the results of the external network security assessment and wireless review performed by KPMG in 2009. The report contains 22 specific vulnerabilities with KPMG's recommendations and City management responses to each of them. The 22 vulnerabilities were identified across six divisions.

Vulnerabilities are commonly identified through penetration testing and allow the system owners to better configure technical security controls in order to strengthen the organization's protection against external exploits. This KPMG audit provided the City with a targeted and focused analysis of its externally facing network environment. Using a series of industry standard "hacking" tools and manual hacking techniques, KPMG attempted to access from the Internet any firewalls, border gateways, VPN concentrators, servers, routers, and any other network perimeter devices protecting the City's internal network.

KPMG rated the identified vulnerabilities on a three tier scale based on the significance of risk to the business unit. A level one rating represents vulnerabilities that are causing a disruption to operations. A level two rating represents a vulnerability that could have an adverse affect on operations. A level three rating represents a process improvement opportunity or minor control weakness. Of the 22 vulnerabilities identified during the audit, 3 were rated tier one, 10 were rated tier two and 9 were rated tier three.

The Comptroller's Senior IS Auditor, Isaak Lerner followed up on all 6 vulnerabilities that were still unresolved per management's responses to a draft of the report. Through inquiry with City management, it was determined that only 2 of the original 22 items remain unresolved. All of the highest risk vulnerabilities (Level one, as identified by KPMG) have been resolved. The first unresolved item was rated as a level two and will be addressed through a planned hardware upgrade in December 2010 and the second unresolved item rated as a level three will be addressed through the replacement of an outdated server in January 2011.

Several meetings were held with representatives of the Department of Public Works and the Information Technology Management Division throughout the last year to resolve the identified vulnerabilities through management actions. The City's action in resolving these vulnerabilities has made external network security stronger. The Department of Public Works and the Information Technology Management Division should be commended for their diligence in resolving identified security weaknesses and the Comptroller thanks all parties involved in this audit for their enthusiastic cooperation in strengthening our network security.

Sincerely,

W. MARTIN MORICS
Comptroller

CC: Jeffrey Mantes, DPW Commissioner
Nancy Olson, CIO

KPMG LLP
303 East Wacker Drive
Chicago, IL 60601-5212

November 8, 2010

Mr. James Michalski
City Hall,
200 East Wells Street,
Milwaukee, WI 53202

Dear Jim:

We have completed the IT External Penetration Test and Wireless Review engagement for the City of Milwaukee, as outlined in our engagement letter dated July 1, 2009. This letter signifies the completion of the services agreed to be provided by KPMG LLP ("KPMG") as described in the engagement letter.

The data included in this report was obtained from you, on or before August 28th, 2009. We have no obligation to update our report or to revise the information contained therein to reflect events and transactions occurring subsequent to August 28th, 2009. This report is solely for your information and is not to be referred to in communications with or distributed for any other purpose to anyone who is not a member of management.

Please contact Phil Lageschulte at (312) 665-5380 if you have any questions or comments. We look forward to continuing to provide service to your company in the future.

KPMG LLP

City of Milwaukee – External Network Security Assessment & Wireless Review

Table of Contents

Overview	3
Project Scope	3
Classification of Internal Audit Findings	4
Internal Audit Observations	
- Level One Observations	5
- Level Two Observations	8
- Level Three Observations	18

Overview

An External Network Vulnerability and Wireless Assessment was performed at the City of Milwaukee ("City") between July 27th, 2009 and August 28th, 2009. This internal audit provided the City with a targeted and focused analysis of its externally facing Internet-based network environment. The purpose of this audit was to assist the City in identifying vulnerabilities and recommending appropriate safeguards within its external network security architecture.

Project Scope

The scope of the audit procedures included the following:

- Internal Audit validated that proper externally facing Internet based security controls exist through an assessment of the appropriate technologies at the City. Using a series of industry standard "hacking" tools and manual hacking techniques, Internal Audit attempted to access from the Internet any firewalls, border gateways, VPN concentrators, servers, routers, and any other network perimeter devices protecting the City's internal network.
- The External Network Vulnerability Assessment was limited to testing specific security controls on the City's externally facing network devices. City Information Technology personnel provided the IP addresses and ranges.
- The City's wireless architecture in four specified locations was monitored and assessed for access vulnerabilities.

In addition, testing procedures were performed during non-peak hours to minimize potential disruption to the production environment. This assessment did not include Denial Of Service (DOS) attacks where network connections are flooded with data packets to temporarily disable the City's external network connections.

Sensitive technical information related to this assessment was shared with the appropriate City IT staff but has been omitted from this report.

Classification of internal audit findings

Control weakness observations in IT Audit reports are rated based on the significance of the risk posed by the observation identified to the business unit covered by the specific internal audit. Significance of internal control weaknesses noted in IT Audit reports are rated on a three-tier scale as follows:

Ranking	Definition of Ranking	Number of Observations
Level 1	Observation represents a control weakness, which is causing disruption of the process or adversely affecting the ability to achieve process objectives. Requires immediate management attention. Observations with at least one of the following attributes will be ranked as Level 1: • Technical vulnerability which could directly lead to system compromise • Technical vulnerability which could directly lead to disclosure of sensitive information.	**3**
Level 2	Observation represents a control weakness, which could have an adverse affect on the ability to achieve process objectives. Requires near-term management attention. Observations with at least one of the following attributes will be ranked as Level 2: • Technical vulnerability which could indirectly lead to system compromise or disclosure of sensitive information • Lack of documented process or procedures which could indirectly lead to system compromise or disclosure of sensitive information	**10**
Level 3	Observation represents a process improvement opportunity or minor control weakness, which could have an unfavorable affect on the ability to achieve process objectives. Observations with at least one of the following attributes will be ranked as Level 3: • Technical vulnerability which could provide unauthorized persons information which would aid in launching further attacks • Technical setting or configuration item that is unnecessary, or is not providing network services and could lead to information disclosure or other vulnerabilities	**9**

Internal Audit Observations

1. MySQL – Multiple Vulnerabilities		Ranking: Level 1
Observation	**Recommendation**	**Agreed Management action**
While performing the external penetration test, Internal Audit noted multiple vulnerabilities in the MySQL service on several systems.	As a general best-practice, MySQL ports should not be open through the firewall. Block MySQL at the perimeter. MySQL should be security configured, and upgraded to the latest version.	External MySQL access has been disabled on these systems.

Responsibility	David Henke, Telecommunications Analyst
Target date	12-7-2009

2. Multiple SSH Vulnerabilities		Ranking: Level 1
Observation	**Recommendation**	**Agreed Management action**
While performing the external penetration test, Internal Audit noted multiple vulnerabilities in the SSH service **Impact:** A successful attack would allow remote attackers to gain access to system resources granted as a legitimate user, capture sensitive information, compromise the system, or cause a denial of service.	Upgrade the version of OpenSSH, available from the OpenSSH Web site http://www.openssh.org/ Furthermore, disable SSH1 support, and do not enable SSH Version 1 Fallback. Systems with upgraded versions of SSH and with Fallback Version 1 enabled are still vulnerable.	External SSH access has been disabled.

Responsibility	David Henke, Telecommunications Analyst, Roger Rick, Business Systems Supervisor
Target date	12-07-2009

3. Apache Web Server Multiple Vulnerabilities		Ranking: Level 1
Observation	**Recommendation**	**Agreed Management action**
While performing the external penetration test, Internal Audit noted multiple vulnerabilities exist in the Apache HTTP service on several devices. **Impact:** The vulnerabilities listed above could lead to system compromise, denial of service, and information disclosure, as well as attacks on users of these systems.	Determine if the vulnerable Apache modules are required. Modules not required should be disabled. Apache configurations should be hardened as well. Lastly, upgrade to the latest version, which is available from the Apache Web site. http://www.apache.org/	Apache has been upgraded to the latest version, unneeded modules disabled, SSL disabled, and/or the latest HTTP patches applied. Four server configurations are maintained by CDC/John Hopkins University for specialized applications. Per the vendor, these servers have been updated to the latest version.

Responsibility	David Henke, Telecommunications Analyst
Target date	11-06-2009

4. Apache Tomcat Multiple Vulnerabilities		Ranking: Level 2
Observation	**Recommendation**	**Agreed Management action**
While performing the external penetration test, Internal Audit noted multiple vulnerabilities exist in the Apache Tomcat service on the following IP addresses: **Impact:** The vulnerabilities listed above could lead to sensitive information disclosures as well as attacks on users of these systems.	Apache Tomcat configurations should be hardened, and Tomcat software should be upgraded to the latest version. Refer to the Apache Tomcat Web site http://tomcat.apache.org/ for details.	Matter referred to website manager for review. Hardware and software scheduled to be upgraded/replaced by the end of 2010.

Responsibility	Eldon Gartzke, Network Manager
Target date	9-15-2009

5. PHP - Multiple Vulnerabilities		Ranking: Level 2
Observation	**Recommendation**	**Agreed Management action**
Internal Audit noted that Multiple PHP Buffer Overflow Vulnerabilities exist on multiple IP addresses due to an outdated version of PHP. **Impact:** Exploiting some of these issues depends on the configuration of the application employing the vulnerable PHP version. To exploit some of these issues, an attacker may need to have local access; for other issues, the attacker can use a browser. Exploitation can lead to a denial of service condition. These issues can be exploited by malicious people to disclose potentially sensitive information, bypass certain security restrictions, cause a denial of service, and potentially compromise a vulnerable system.	Upgrade to the latest version of PHP which is available for download from php's Web site http://www.php.net/downloads.php (PHP version 5.3.0 as of this writing)	PHP has been disabled on this device.

Responsibility	David Henke, Telecommunications Analyst
Target date	11-6-2009

6. Cisco VPN – Multiple Vulnerabilities		Ranking: Level 2
Observation	**Recommendation**	**Agreed Management action**
Internal Audit noted a VPN vulnerability on several hosts. **Impact:** A successful attack may lead to denial of service to legitimate users. A malicious user with access to the VPN data stream may be able to recover the session key of a VPN connection. This would then provide access to all data sent across the VPN connection, which may include passwords and sensitive files.	Internal Audit noted many hosts with PPTP, SSH, and RDP open. The Cisco 3000 VPN connector should be used as the remote access method of choice, rather than maintaining all of these individual services. Cisco has information on a mitigation technique only for Cisco IOS software affected by this issue. Refer to Cisco Security Response 70810 for further details. http://www.cisco.com/warp/public/707/cisco-sr-20060726-ike.shtml	Followed Cisco's recommended update of CAR on endpoint VPN devices to limit the traffic to mitigate vulnerability.

Responsibility	Peter Gnas, Network Manager
Target date	12-2-2009

7. PPTP VPN Weak Authentication Vulnerability		Ranking: Level 2
Observation	**Recommendation**	**Agreed Management action**
Internal Audit noted that a PPTP VPN Configuration Allows Weak MS-CHAPv1 Authentication on several servers. **Impact:** An attacker with access to the data stream between client and server may be able to decrypt the data stream, thus negating the effects of data encryption. This may lead to further attacks, such as session hijacking or password theft.	Disable MS-CHAPv1 support on the VPN server, and only allow the stronger CHAP or MS-CHAPv2 protocols instead. Instructions on enabling the MS-CHAPv2 protocol are available at the MS-CHAP version 2 Web page on Microsoft's site. http://www.microsoft.com/windows/windows2000/en/advanced/help/sag_RASS_MSCHAPv2.htm For machines running Windows NT 4.0, Windows 95, or Windows 98, this may require applying the latest security patch. Refer to this document for details. http://www.schneier.com/paper-pptp.html	MSCHAP-v1 authentication has been disabled of PPTP has been disabled on endpoint device.

Responsibility	Larry Sullivan, Management Civil Engineer – Senior, Peter Gnas, Network Manager
Target date	12-2-2009

8. Webmin Multiple Vulnerabilities		Ranking: Level 2
Observation	**Recommendation**	**Agreed Management action**
While connected via SSID"*CWL*", Internal Audit noted that the Webmin application, which is used to manage Linux servers, is configured on one system and was accessible without SSLencryption. Webmin was also externally accessible on two other systems. **Impact:** A successful attack could allow access to change City of Milwaukee Webmin settings, gain access as any known username without requiring the password for that account, inject JavaScript code, which will execute within the context of the Webmin domain, and obtain potentially sensitive information. One environment variable, HTTP_AUTHORIZATION, contains Webmin's administrator login ID and password in MIME 64-encoded form. An attacker may read and decode this information, and use it for further exploits (along with other data, including host path and configuration information), potentially obtaining root privileges.	Configure Webmin so that SSL encryption is required to access the configuration page and disable HTTP access to Webmin. See http://www.webmin.com/ssl.html for information on configuring SSL in Webmin. Upgrade to the latest version of Webmin. Ideally, administrators should only access management portals from inside the trusted network.	External Webmin access has been disabled to these systems.

Responsibility	David Henke, Telecommunications Analyst
Target date	12-7-2009

9. FTP Services – Multiple Vulnerabilities		Ranking: Level 2
Observation	**Recommendation**	**Agreed Management action**
Internal Audit noted that FTP was detected on several systems. **Impact:** 1. Since credentials are not encrypted before being sent, an attacker could intercept the FTP credentials and access the FTP server. 2. If this vulnerability is successfully exploited, it allows attackers to manipulate SQL queries and modify data or steal sensitive information from the underlying database or run arbitrary FTP commands on the server in the context of an unsuspecting user's session.	Remove FTP services from the City of Milwaukee network. Utilize SFTP where file transfers are necessary. Upgrade to the latest version of ProFTPD.	External FTP services have either been disabled or updated with the latest security patches.

Responsibility	Jane Tabaska, Network Manager, David Henke, Telecommunications Analyst, Roger Rick, Business Systems Supervisor
Target date	12-4-2009

10. Dropbear SSH Vulnerability		Ranking: Level 2
Observation	**Recommendation**	**Agreed Management action**
While performing the external penetration test, Internal Audit noted a vulnerability exists in the SSH service on the several systems. These systems appear to be running Dropbear SSH Server version [illegible]. The SSH service provides encrypted remote access to hosts. **Impact:** A successful attack may allow arbitrary code execution and can allow an attacker to gain superuser access.	The vendor released Dropbear [illegible] address this issue. Download the upgrade from http://matt.ucc.asn.au/dropbear/dropbear.html. Consider upgrading to the latest version of Dropbear (version [illegible] as of 8/11/2009).	External SSH access has been disabled to this system.

Responsibility	David Henke, Telecommunications Analyst
Target date	9-25-2009

11. Multiple OpenSSL Vulnerabilities		Ranking: Level 2
Observation	**Recommendation**	**Agreed Management action**
Internal Audit noted multiple OpenSSL vulnerabilities on the several servers. **Impact:** Successful exploitation of these vulnerabilities could result in the execution of arbitrary code or a service crash.	Upgrade to the latest version of OpenSSL (0.9.8k as of this writing). OpenSSL released the following advisories to address these issues. http://www.openssl.org/news/secadv_20060928.txt http://www.openssl.org/news/secadv_20071012.txt	Four server configurations are maintained by CDC/John Hopkins University for specialized applications. Per the vendor, these servers have been updated to the latest version.

Responsibility	Jeff Hussinger, Telecommunications Analyst
Target date	3-31-2010

12. Windows TCP/IP Remote Code Execution and Denial of Service Vulnerabilities		Ranking: Level 2
Observation	**Recommendation**	**Agreed Management action**
Internal Audit noted that a Windows TCP/IP Remote Code Execution and Denial of Service Vulnerabilities exists on the multiple IP addresses **Impact:** An attacker who successfully exploits the most severe of these vulnerabilities could take complete control of an affected system. The attacker could then install programs, view/edit sensitive data, and create new accounts with full user rights. An attacker who successfully exploits the most severe of these vulnerabilities would most likely cause the affected system to stop responding.	Install Microsoft Security Update MS05-019	All security patches have been applied, and/or ports not in use by applications have been disabled, One server is running Windows NT4 for which there is no applicable patch related to this vulnerability. This server is scheduled for removal from the environment by the end of 2010. Four server configurations are maintained by CDC/John Hopkins University for specialized applications. Per the vendor, these servers have been updated to the latest version.

Responsibility	Jana Tabaska, Network Manager, Peter Gnas, Network Manager, Roger Rick, Business Systems Supervisor, Jeff Hussinger, Telecommunications Analyst
Target date	3-31-2010

13. SSL Weak and Insecure Ciphers		Ranking: Level 2
Observation	**Recommendation**	**Agreed Management action**
Internal Audit noted multiple web servers supporting weak cryptographic ciphers. The following weak ciphers were supported: **Impact:** A successful attack on these vulnerabilities would allow an attacker to obtain sensitive information.	Web servers using SSL encryption should be configured to only use strong encryption.	Devices have been taken offline until updated with stronger encryption, are running SSLv3 certificates, SSL is unneeded and has been disabled, external HTTP access has been disabled, and/or HTTP patches have been applied. Four server configurations are maintained by CDC/John Hopkins University for specialized applications. Per the vendor, these servers have been updated to the latest version.

Responsibility	Eldon Gartzke, Network Manager, Peter Gnas, Network Manager, David Henke, Telecommunications Analyst, Jeff Hussinger, Telecommunications Analyst
Target date	3-31-2010

14. Web Server HTTP Trace/Track Method Support Vulnerability	Ranking: Level 3

Observation	Recommendation	Agreed Management action
While performing the external penetration test, Internal Audit noted that the Trace/Track HTTP Method is enabled on several web servers: **Impact:** If this vulnerability is successfully exploited, users of the Web server may lose their authentication credentials for the server and/or for the Web applications hosted by the server to an attacker. This may be the case even if the Web applications are not vulnerable to cross site scripting attacks due to input validation errors.	Disable the Trace method on production web servers.	External HTTP access has been disabled to these systems.

Responsibility	David Henke, Telecommunications Analyst
Target date	11-6-2009

15. Multiple DNS Vulnerabilities		Ranking: Level 3
Observation	**Recommendation**	**Agreed Management action**
While performing the external penetration test, Internal Audit noted vulnerabilities in the DNS services on several servers. **Impact:** A successful attack could lead to a denial of service, sensitive information disclosure, or possible system compromise.	DNS servers should be securely configured such that recursive searches and other types of queries are not allowed for untrusted clients. DNS server software should also be updated to the latest versions.	Latest DNS patches were applied to devices,

Responsibility	David Henke, Telecommunications Analyst
Target date	11-6-2009

16. Wordtrans PhpInfo Information Disclosure		Ranking: Level 3
Observation	**Recommendation**	**Agreed Management action**
While performing the external penetration test, Internal Audit noted a vulnerability exists in the wordtrans service on the several systems. **Impact:** By exploiting this vulnerability, malicious users can gather sensitive system information, which may be used in more serious future attacks.	There does not seem to be a legitimate business purpose for this service. Disable the Wordtrans service.	External HTTP access has been disabled to these systems.

Responsibility	David Henke, Telecommunications Analyst
Target date	11-6-2009

17. Web Application Information Disclosure - Listing of Employees and Cost Centers		Ranking: Level 3
Observation	**Recommendation**	**Agreed Management action**
Internal Audit noted that a listing of 2,874 employees/buildings was easily obtained and available for public access. By clicking "Search" without filling in any of the search parameters, the following information was available: : Last Name, First Name, Extension, Cost Center Code, Building, Address, and Room Number. **Impact:** An attacker could use the list for social engineering purposes or information gathering for further attacks such as social engineering or phishing.	The listing of employees should be controlled. A Web Application Vulnerability assessment should be performed for the City of Milwaukee to discover additional security vulnerabilities.	Information listed is subject to public records disclosure. However, access to this information has been restricted from external sources.

Responsibility	David Henke, Telecommunications Analyst
Target date	11-16-2009

18. Milwaukee Water Works – Payment and Bill Vulnerabilities		Ranking: Level 3
Observation	**Recommendation**	**Agreed Management action**
Internal Audit noted that there is an inadequate protection of public data on Milwaukee Water Works website. **Impact:** An attacker could write an automated script to pull data about the usage statistics and 'Bill To' addresses of any Milwaukee Water Works customer or property.	Control the ability to access and modify billing information from the Milwaukee Water Works web page through strong authentication. A Web Application Vulnerability assessment should be performed for the City of Milwaukee to discover security vulnerabilities.	There is no sensitive or private information contained on these web pages. All Milwaukee Water Works payment, bill, and water usage data are public records, not private information. (This is similar to accessing property and owner information through the Assessor's website.) Specifically as regards the "Change 'Bill To' Address", entries on this screen are not directly updated on our files; a report is produced and reviewed by MWW staff before the change is made on our records. Therefore, we are unconcerned about this item and will be taking no current action to change our website.

Responsibility	Eldon Gartzke
Target date	9-15-2009

19. Default Web Pages		Ranking: Level 3
Observation	**Recommendation**	**Agreed Management action**
Internal Audit noted a number of default web pages on several servers. **Threat:** While having a default web page enabled is not an immediate threat, it is not good practice. Web Publishing Services should be disabled on servers that are not being used to host websites. **Impact:** This could also indicate that a server has been installed on the network unknown to the City of Milwaukee.	Remove unneeded web services and remove default web pages.	External HTTP access has been disabled and/or default web pages removed where default web pages were inappropriate.

Responsibility	Eldon Gartzke, Network Manager, David Henke, Telecommunications Analyst, Jane Tabaska, Network Manager, Peter Gnas, Network Manager, Jeff Hussinger, Telecommunications Analyst
Target date	12-31-2010

20. Expired, Self-Signed, and Misconfigured SSL Certificates		Ranking: Level 3
Observation	**Recommendation**	**Agreed Management action**
Internal Audit noted web servers with expired, self-signed, and otherwise misconfigured SSL certificates on multiple servers. **Impact:** Unmaintained web servers can leave unpatched software that can lead to system compromise.	If these are legitimate web servers that are being used, properly configured SSL certificates should be installed. Either a private internal CA, or a public CA should be used to validate the certificates.	Self signed certificates are adequate for several devices or the external HTTP access has been disabled.

Responsibility	Peter Gnas, Network Manager, Roger Rick, Business Systems Supervisor, David Henke, Telecommunications Analyst, Jeff Hussinger, Telecommunications Analyst
Target date	12-31-2009

21. Windows NT PPTP DoS Vulnerability		Ranking: Level 3
Observation	**Recommendation**	**Agreed Management action**
Internal Audit noted a Microsoft NT PPTP vulnerability on a Windows NT server. **Impact:** By exploiting this vulnerability, a malicious user can cause a denial of service on the server running Windows NT with PPTP enabled. If this occurs, a restart of the server is required to regain normal functionality. Additionally, the successful exploitation of this vulnerability could assist in further attacks against the victim.	Microsoft released several patches to fix this problem. For information on which patch is relevant to your particular configuration, read Microsoft Security Bulletin MS01-009 http://www.microsoft.com/technet/security/bulletin/MS01-009.mspx Windows NT is no longer a Microsoft supported platform, and should be removed from the environment.	The relevant patch has been applied to the Windows NT 4.0 server. In addition, it should be noted that the server is slated for removal from the environment by the end of 2010.

Responsibility	Jane Tabaska, Network Manager
Target date	9-18-2009

22. Policy and Procedures		Ranking: Level 3
Observation	**Recommendation**	**Agreed Management action**
Internal Audit noted that a wireless policy and procedure document does not exist for the City of Milwaukee.	Create a wireless policy and procedure document. This document should describe the wireless network architecture and display where current wireless devices are deployed. They should also provide baseline documentation for the secure configuration, maintenance, and monitoring of these devices.	Wireless service is provided as a best-effort service, primarily for public usage. It is logically segregated from the internal City network. All wireless system documentation is maintained as part of the wireless controller configuration.

Responsibility	David Henke, Telecommunications Analyst
Target date	12-8-2010