City of Milwaukee

Office of the Comptroller

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

January 5, 2012

To the Honorable Common Council
City of Milwaukee

External Network Security Audit

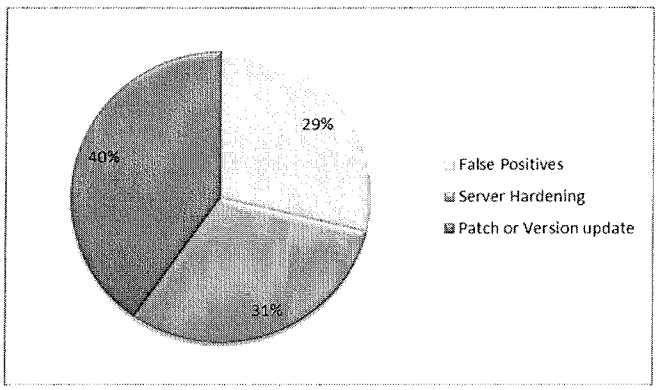
Dear Council Members:

As a component of the Comptroller's comprehensive information systems audit work plan, Securance Consulting was engaged to complete the external network security 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 performed by Securance in August 2011. The report contains 31 unique vulnerabilities that break down into 148 types of possible threats with Securance's recommendations and City management responses to each of them. The 31 vulnerabilities were identified across 8 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 Securance 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, Securance 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.

Securance rated the identified vulnerabilities on a four tier scale based on the significance of risk to the business unit. A "Medium Risk" rating represents vulnerabilities that expose some sensitive information from the host. A "High" rating represents a vulnerability that provide possible hackers with access to specific security related information about the host. A "Critical" rating represents a vulnerability that provides possible hackers with remote user access but not remote administrator access. An "Urgent" rating represents a vulnerability that provides possible hackers with remote root or administrator access. Of the 31 vulnerabilities identified during the audit, 22 were rated "Medium Risk," 9 were rated "High" and 0 were rated "Critical" or "Urgent."
The Penetration test results represent a very strong external security posture and the City's information technology leadership should be commended for their ongoing commitment to strengthening external facing security.

The Comptroller's Senior IS Auditor, Isaak Lerner followed up on all 148 possible vulnerabilities within the Securance report with a requested management response from the various server owners. All of the Vulnerabilities fell in two major categories; The first, which constitutes 29% of the vulnerabilities are agreed upon false positives that do not require remediation. The second, which constitutes 31% of the vulnerabilities are issues related to server hardening, like closing various ports and turning off risky services. The third category, which constitutes 40% of the vulnerabilities are issues related to un-updated patches and outdated software versions.



After compiling all the management responses, 100% of the vulnerabilities and recommendations have been acknowledged and an acceptable management response or remediation plan was presented for all vulnerabilities. As of January 1, 2012

24 of the 31 unique vulnerabilities have already been resolved and the outstanding 7 unique vulnerabilities have been scheduled for remediation in 2012 through various software and hardware updates.

As a result of this audit, the Comptroller's Office is recommending;

1) ITMD should engage with the CIMC and IS security professionals to write and adopt a City wide policy regarding patch management for software and hardware.

2) City wide IT security governance should be centralized under one DOA/ITMD Information Security Officer position for timelier and more efficient resolution of IS security vulnerabilities.

The City's action in resolving these vulnerabilities has made external network security stronger. All City divisions that participated in this audit 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,

Michael J. Daun
Deputy Comptroller

Attachment
CC: Nancy Olson, CIO

Provided for:

August 15, 2011

City of Milwaukee

CITY OF MILWAUKEE

External Network

Vulnerability Assessment Report

Securance

Risk Intelligence

City of Milwaukee

[EXECUTIVE SUMMARY]

INTRODUCTION AND SCOPE

During August 2011, Securance Consulting conducted an external network security vulnerability analysis for the City of Milwaukee. The overall objective of the engagement was to perform a controlled vulnerability assessment to determine the current state of the City's external network security posture. The scope of the engagement was limited to the external Internet-facing Internet Protocol (IP) network.

The review was limited to those areas specifically defined by the City's Internal Audit department and was not intended to be a comprehensive examination of the City's entire information systems function.

We designed an approach and applied our Vulnerability Assessment | Penetration methodology which ensured a comprehensive capture and review of the technical vulnerabilities that exist within the City's IP network. The approach included the use of commercial and proprietary security tools designed to identify vulnerabilities in the City's external Internet-facing network. Our procedures included:

- Network Foot-printing - Researching public information on the target, including technical listings (e.g., ARIN, WHOIS, DNS Lookup, etc.) and public information (newsgroups, search engines, Weblogs, etc.);
- Scanning - Utilizing automated tools to identity specific systems and services, software and operating system version levels, hardware devices, and other information; and
- Enumeration - Identifying specific vulnerabilities and avenues of attack through both automated and manual means.

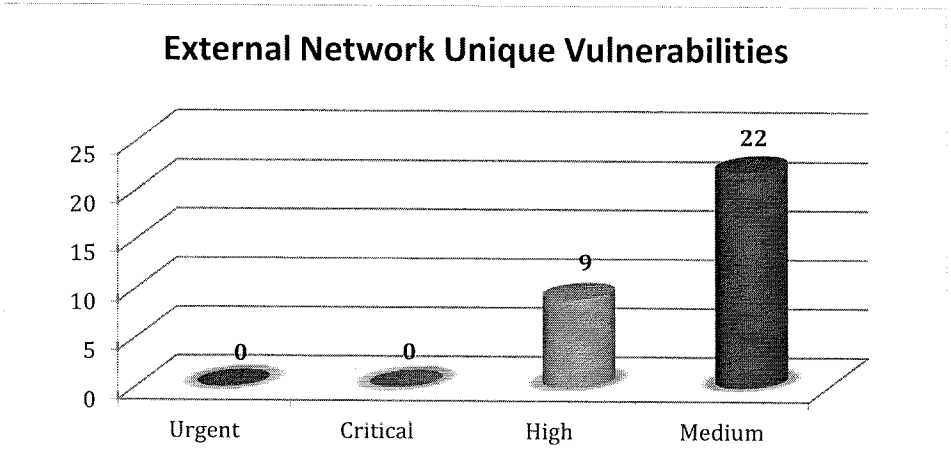
The tools utilized and our procedures, including the timing of our fieldwork, were configured and conducted to eliminate the possibility of any disruption to the City's Information Technology (IT) infrastructure.

City of Milwaukee

The following section provides a summary and graphical analysis of the vulnerabilities identified that are considered urgent, critical, or high risk to the City's IP network; and, our conclusion of the overall security posture of the external Internet-facing network.

External Unique System Vulnerabilities

- *Identified 9 high risk vulnerabilities that fall into these categories:*
  - There are various specialty application and web servers that do not have the latest patch applied;
  - There are various web servers that are configured with select default settings that should be adjusted; and
  - There is an obsolete web server running that the vendor is no longer supporting.



City of Milwaukee

CONCLUSION

Based on the procedures we performed, our knowledge of the City's external Internet-facing network and our IT security experience, it is our opinion, as of the point-in-time of this review, that the external network is adequately controlled to prevent and/or detect an externally-originated breach. We recommend the review and implementation of the solutions referenced on pages 8 - 21 to improve external network security. As with all recommendations that may affect a computer system or network device, changes should be tested in a non-production environment prior to implementation in production.

The remainder of this report provides a detailed analysis of our approach and methodology and specific vulnerabilities identified.

Remainder of this page left blank intentionally.

City of Milwaukee

[EXTERNAL NETWORK SECURITY REPORT]

BACKGROUND

During August 2011, the City's Internal Audit department contracted with Securance Consulting to perform a vulnerability assessment of their entire external Internet-facing Internet Protocol (IP) network.

SPECIFIC OBJECTIVES AND SCOPE

The objective of the review was to identify technical vulnerabilities within the City's external Internet-facing network and to analyze them in an effort to eliminate any false positives.

Review tasks included system discovery analysis, system port discovery, and system vulnerability identification and assessment. The review was limited to the areas we considered necessary to complete this engagement and was not intended to be a comprehensive examination of the City's entire information systems function.

APPROACH AND METHODOLOGY

To achieve the objectives of this engagement, within the defined scope, we performed our diagnostic and vulnerability assessment activities utilizing our proven methodology. The following describes the high-level tasks performed for each component of the project:

City of Milwaukee

EXTERNAL NETWORK:

During this phase, we performed step-by-step discovery and vulnerability assessment procedures aimed at identifying weaknesses in Internet Protocol (IP) network services. The following activities were performed:

- *Internet Discovery* – we created a profile of computer addresses and other information related to the City's Internet-connected network using public tools, manual tasks, publicly available information, and information from the City's IT personnel.

- *External IP Scan* – we performed a vulnerability scan against the approved range of external IP addresses noted above. The primary tools used were nmap and nessus host vulnerability scanner. We configured a scan policy that minimized disruption to the City's Internet facing systems and network devices. This included disabling denial of service and brute force attack attempts.

- *False Positive Identification* – analyzed the results of the activities and based on our knowledge and information retrieved during the scanning attempted to identify and remove all false positive vulnerabilities.

- *Exploitation Analysis* – analyzed which systems to attempt to breach by exploiting the remaining high-risk vulnerabilities based on our experience and expertise.

City of Milwaukee

FINDINGS AND RECOMMENDATIONS

The following recommendations, which resulted from the external network vulnerability assessment and are submitted to assist in improving the security posture of the City's external network:

No. 1: External Network Vulnerabilities

We performed a detailed scan against the City's external network(s) and identified the following vulnerabilities. The scan results revealed technical vulnerabilities that increase the likelihood of an externally originated network breach.

The charts on the following page provide a snapshot of the vulnerabilities identified, prioritized by level of severity as defined by the Common Vulnerability Scoring System (CVSS) version 2, the globally recognized standard for assigning a severity level to each vulnerability. The pages that follow summarize unique vulnerabilities, the affected systems, and the recommended solutions. In many cases the recommended solution requires a system security patch.

Risk:
The City's external network is at a relative low to moderate risk of being compromised by an attacker. If the City's external network is attacked, depending upon the type of attack and if the attack is successful, systems could be rendered unresponsive, data could be compromised, or segments of the network could be used to breach internal systems.

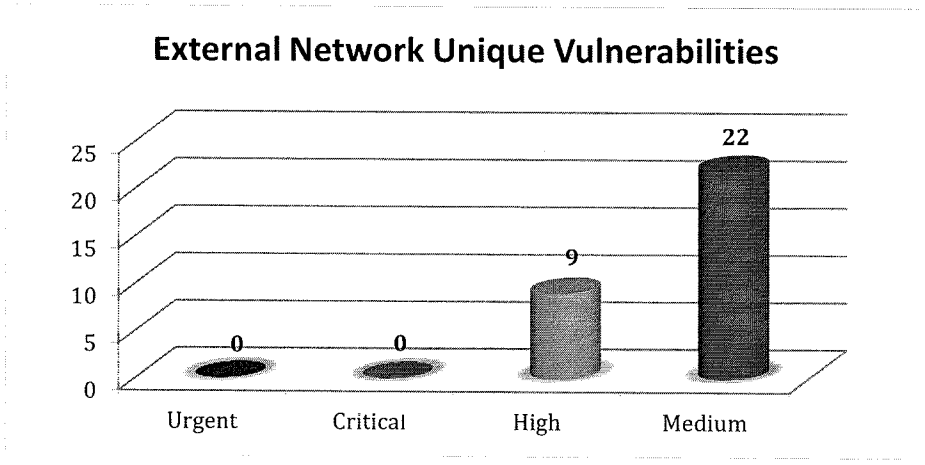
Recommendation:
We strongly recommend that the City address all high, and medium-risk vulnerabilities. As with all recommendations that may affect a computer system or network device, changes should be tested in a non-production environment prior to implementation in production.

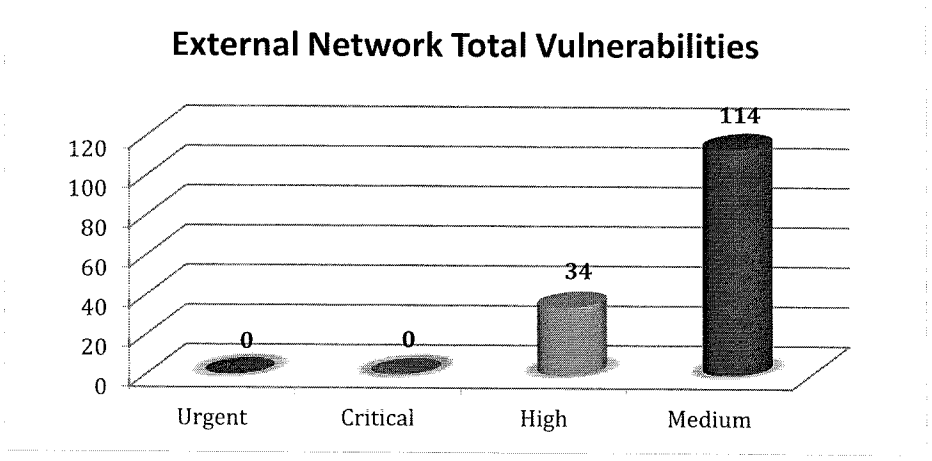
Vulnerability details are provided in the Technician's Report – Appendix B. All low risk vulnerabilities and informational disclosures are only provided in the technician's report.

City of Milwaukee

Finding & technical vulnerability legend provided on page 22.

Management's Response:





City of Milwaukee

FINDING RISK PRIORITY LEGEND:

R Immediate action recommended.

Y Recommend action within the coming year…minimal risk to the organization.

G Effective control…no changes recommended.

ADVISORY Advisory comment…action suggested at the discretion of management.

SECURITY THREAT LEVEL LEGEND:

Urgent	Urgent Risk (Level 5) vulnerabilities provide remote intruders with remote root or remote administrator capabilities.
Critical	Critical Risk (Level 4) vulnerabilities provide intruders with remote user, but not remote administrator or root user capabilities.
High	High Risk (Level 3) vulnerabilities provide hackers with access to specific information stored on the host, including security settings. This level of vulnerabilities could result in potential misuse of the host by intruders.
Medium	Medium Risk (Level 2) vulnerabilities expose some sensitive information from the host, such as precise versions of services. With this information, hackers could research potential attacks to try against a host.

Securance

City of Milwaukee

Securance Consulting would like to **THANK YOU** for your business. Aside from benefiting from the highest level of service possible, you also received unique advantages that only Securance Consulting delivers. Our hands-on approach is tailored to fit both the needs of the compliance and information technology departments. Our technical expertise, outstanding reputation, and personalized attention ensure you a level of service surpassed by no other technology risk management firm in the market.

As a Securance customer, you can be confident in your sound decision to manage your technology risk with a co-sourced relationship with Securance!

Securance