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

April 5, 2012

To the Honorable Common Council
City of Milwaukee

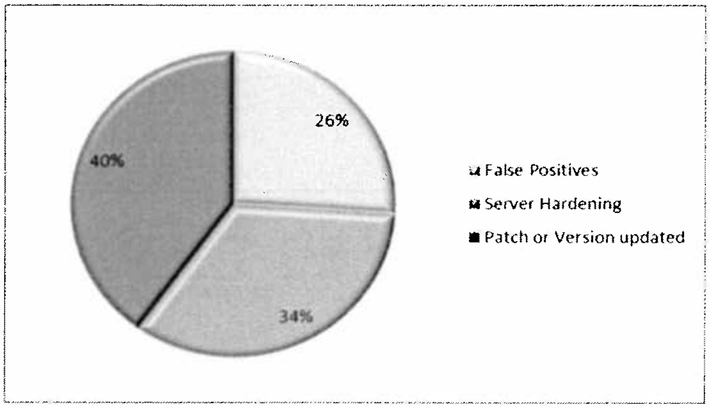
Dear Council Members:

As a component of the Comptroller's comprehensive information systems audit work plan, Securance Consulting was engaged to complete the internal network security test of the City's computer network. The Comptroller's Office recently received the enclosed final report detailing the results of the internal network security assessment performed by Securance in September 2011. The report contains 491 unique vulnerabilities that break down into 1453 types of possible threats with Securance's recommendations and City management responses to each of them. The 491 vulnerabilities were identified across 12 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 internal exploits. This Securance audit provided the City with a targeted and focused analysis of its internally facing network environment. Using a series of industry standard "hacking" tools and manual hacking techniques, Securance attempted to access from within the City networks any servers, routers or other internal network devices that exist within 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 491 unique vulnerabilities identified during the audit, 263 were rated "Medium Risk," 109 were rated "High" and 119 were rated "Critical" and none were rated "Urgent." The Penetration test results represent a strong internal security posture and the City's information technology leadership should be commended for their ongoing commitment to strengthening internal facing security.

The Comptroller's Senior IS Auditor, Isaak Lerner followed up on all 1453 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 26% of the vulnerabilities are agreed upon false positives that do not require remediation. The second, which constitutes 34% 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, 97% of the vulnerabilities and recommendations have been acknowledged and an acceptable management response or remediation plan was presented for these vulnerabilities. Three percent of the overall recommendations have not been addressed and are currently being assessed by the Library IS staff for remediation.

As a result of this audit, the Comptroller's Office recommends:

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 more timely and more efficient resolution of IS security vulnerabilities.

The City's action in resolving these vulnerabilities has made internal 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 the City's network security.

Sincerely,

Michael J. Daun

Michael J. Daun
Deputy Comptroller

CC: Nancy Olson, CIO

Provided for:

September 19, 2011

City
of
Milwaukee

CITY OF MILWAUKEE
Internal Network
Vulnerability Assessment Report

Securance

Risk Intelligence

[EXECUTIVE SUMMARY]

INTRODUCTION AND SCOPE

During September 2011, Securance Consulting conducted an internal 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 internal network security posture for select divisions. The scope of the engagement was limited to the internal IP networks of the department's listed in the conclusion starting on page 4.

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 internal IP network for the divisions in scope. The approach included the use of commercial and proprietary security tools designed to identify technical vulnerabilities in the City's internal network. Our procedures included:

- Network Understanding – Gaining an overall understanding of the internal network structure for the division in scope.

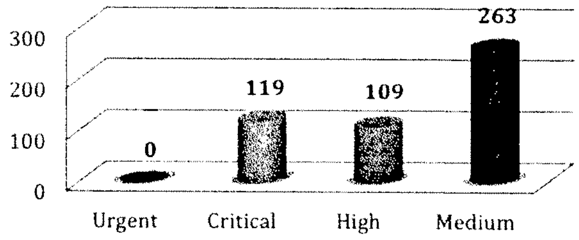
- Scanning - Utilizing automated tools to identity specific systems and services, software and operating system version levels, hardware devices, and other information; and

- Enumeration - Identifying specific vulnerabilities and avenues of attack through both automated and manual means.

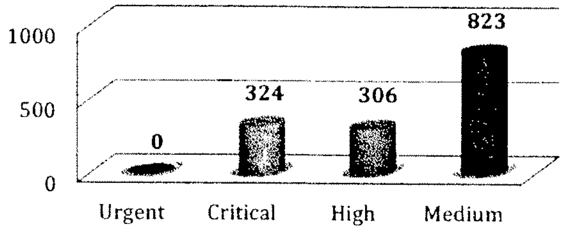
The tools utilized and our procedures, including the timing of our fieldwork, were configured and conducted to eliminate the possibility of any disruption to the City's Information Technology (IT) infrastructure.

The following charts provide a graphical analysis of the total and unique vulnerabilities identified that are considered critical, high or medium risk to the City's internal IP network. Department specific charts are provided in the management section of this report beginning on page 9.

CITY OF MILWAUKEE
Internal Systems Unique Vulnerabilities



CITY OF MILWAUKEE
Internal Systems Total Vulnerabilities



CONCLUSION

Based on the procedures we performed and our IT security experience, it is our opinion, as of the point-in-time of this review that the security posture relative to technical vulnerability management of the internal network for the in scope departments is as follows:

- Water Department – adequate.
- Department Community Development | RACM – needs improvement, moderate risk of breach.
- Department Neighborhood Services (DNS) – adequate.
- Department of Public Works – adequate.
- Fire Department – needs improvement, high risk of breach.
- HACM Department – adequate.

- Department of Health – needs improvement, moderate risk of breach.
- ITMD – needs improvement, high risk of breach.
- Library Department – needs improvement, high risk of breach.
- Police Department – needs improvement, high risk of breach.
- Department of Treasury – adequate.

We recommend the review and implementation of the solutions referenced in appendix A for each technical vulnerability to improve the internal network security of each department. 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 page left blank intentionally.

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:

INTERNAL NETWORK:

We performed an initial scan of all systems and network devices connected to the internal networks of the in scope departments to identify active systems and running services. Our methodology dictates performing multiple detailed vulnerability scans against each active system to identify all technical vulnerabilities. The scans were configured to enable "Safe Checks" in an effort to minimize disruption to any internal systems and network devices. In addition to vulnerability identification we attempted to remove false positives based on a review of the results and our IT security experience.

FINDINGS AND RECOMMENDATIONS

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

R No. 1: Internal Departments Network Vulnerabilities

We performed a detailed scan against the City's internal network(s) and identified several vulnerabilities. The results revealed technical vulnerabilities that increase the likelihood of an internally originated network breach for select departments.

The charts on the following page provide a snapshot of the vulnerabilities identified by department, 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. Appendix A provides a detailed summary, by department, of each unique vulnerability, the affected systems, and the recommended solutions. In many cases the recommended solution requires a system security patch.

Risk:

Select departments within the City's internal network are at a high to moderate risk of being compromised by an attacker. If a department's internal 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 the attack could be used to breach other internal systems.

Recommendation:

We strongly recommend that the City address all critical, 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.

Finding & technical vulnerability legend provided on page 15.

Management's Response:

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.

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!