Audit of System Vulnerabilities of City Datacenters

MARTIN MATSON
City Comptroller

AYCHA SIRVANCI, CPA
Audit Manager
City of Milwaukee, Wisconsin

September 2014

Martin Matson
Comptroller

John M. Egan, CPA
Deputy Comptroller

Glenn Steinbrecher, CPA
Special Deputy Comptroller

Toni Biscobing
Special Deputy Comptroller

Office of the Comptroller

September 26, 2014

Honorable Tom Barrett, Mayor
The Members of the Common Council
City of Milwaukee
Milwaukee, WI 53202

Dear Mayor Barrett and Council Members:

As a component of Internal Audit's comprehensive audit work plan, the consulting firm Experis was engaged to complete an Information Technology (IT) vulnerability audit of the City owned and operated datacenters. The focus of the audit was to identify system vulnerabilities and risks involving both the Internet-exposed City IT networks and selected devices available on the internal network. Internal Audit recently received the two enclosed final reports detailing the results of the vulnerability audit performed by Experis. One report covers the Internal Network environment while the other encompasses the external-facing IT environment. Basing its findings and recommendations on the June and July 2014 tests performed, the report advises the datacenters to increase certain security configurations for the City's IT assets.

The consultant, who performed this audit, has extensive experience and subject-matter expertise in all aspects of IT-vulnerability scanning and penetration testing. Thus, computer scans and non-aggressive ethical hacking techniques were utilized to achieve the outlined objectives. A vulnerability analysis was performed on both internal and external networks, including websites. Additionally, a risk assessment was performed on applications used throughout the City. A point system was developed and applied, ranking the risk of each application in an impartial manner. Consequently, the City's highest risk applications were identified and selected for supplemental in-depth vulnerability and penetration testing.

Overall, Experis concluded that for some system configurations, the deployed security controls should be increased, to enhance the control design or operational effectiveness and, thereby, reduce the overall level of risk to certain City IT assets. The Experis report identified technical IT recommendations aimed at augmenting system security. This report only provides summary information on datacenter activities, in order to protect the confidential and sensitive nature of City datacenter operations. Detailed findings and recommendations were sent to all datacenter managers and a written management response was received, indicating their action plan to heighten security. The potential vulnerabilities are currently undergoing review and assessment by datacenter management. Furthermore, the noted items are being addressed in a timely manner, in accordance with the recommended solutions that will minimize datacenter risks. Specific department follow-up to these recommendations will be managed and tracked by Internal Audit.

Appreciation is expressed for the cooperation extended to the auditors by the staff of the City's datacenters.

Sincerely,

Aycha Sirvanci, CPA
Audit Manager

AS:gjl

Information Security:

Internal Network

Vulnerability Assessment Summary

Prepared for:

City of Milwaukee

CONFIDENTIAL

August 26, 2014

Experis

www.experis.com

PRIVACY OF CONTENT

The information contained herein is considered privileged, confidential and the property of Experis and the client. This internal report, including any reproduction portions of this report, contains conclusions and analysis that reflect the information available to Experis prior to the completion date of the work. Upon delivery, Experis has not continued to monitor, nor does the report reflect, any later alterations that may have been relevant to the report contents.

1 Executive Summary

1.1 Objective

During June and July 2014, Experis was engaged by City of Milwaukee (The City) to perform an internal network vulnerability assessment. This review was conducted to verify that adequate controls are in place and access to City of Milwaukee's internal network environment does not compromise system confidentiality, integrity or availability. The goal of this engagement was to identify potential security risks, provide a foundation for improved risk-based decision-making, and prioritize investments.

1.2 Scope

The City of Milwaukee requested Experis perform a limited scope internal network vulnerability assessment. The agreed-upon objectives included the following:

- Perform an automated vulnerability scan of agreed-upon internal servers, workstations, and network devices (e.g., routers, switches)
- Perform an automated vulnerability scan of selected internally accessible applications.
- Provide security expertise to assist City of Milwaukee.

1.3 Vulnerability Assessment Approach

The general activities performed by Experis during the internal network vulnerability assessment portion of the engagement consisted of the following three major phases:

- **Phase I** – Perform a discovery and footprint analysis of the network. Specifically, determine and confirm where the internal network connectivity begins and ends (i.e., the in-scope network segments), and gain a basic understanding of the types of systems and services accessible from the internal network segments.
- **Phase II** – Perform automated vulnerability scans of all internal devices that were discovered in Phase I and considered in-scope by City of Milwaukee Internal Audit Department. The results provide an increased understanding of the accessible operating systems, ports, and services, where vulnerabilities may exist.
- **Phase III** – Produce a consistent and complete report covering the technical vulnerabilities, risks associated with the vulnerabilities, priorities for remediation, and potential root-cause discussions, to facilitate timely enhancements to the overall network security strategy.

The application vulnerability test consisted of the following activities:

- All in-scope application elements were scanned for a variety of potential vulnerabilities such as vulnerable ports and services, out-of-date software versions, and mis-configurations. Scans were conducted using log on credentials provided by the City.
- Based on the results of the initial scans, Experis identified potential attack vectors with higher probability of success (based on prior experiences and research).
- The applications were mapped and common security issues such as Cross-Site Scripting (XSS), SQL Injection (SQLi), and Command Injection (CMDi) were identified.

1.4 Report Content

This report only provides summary information on datacenter activities in order to protect the confidential and sensitive nature of City datacenter operations. Detailed findings and recommendations were sent to all datacenter managers and a written management response was received indicating their action plan to further enhance security. The vulnerabilities are currently undergoing review and assessment by datacenter management; and the noted items are being addressed with the appropriate solution to minimize risk.

Specific department follow-up to these recommendations will be managed, tracked and reported by Internal Audit.

1.5 Engagement Team

The assessment team consisted of the following Experis personnel:

- John Hainaut – Director, Information Security Center of Expertise (ISCOE)
- Peter Paul – Security Professional, ISCOE

Experis™
ManpowerGroup

Information Security:

External Facing Environment

Vulnerability Assessment and Penetration Test

Prepared for:

City of Milwaukee:

CONFIDENTIAL

August 26, 2014

Experis

www.experis.com

PRIVACY OF CONTENT

The information contained herein is considered privileged, confidential and the property of Experis and the client. This internal report, including any reproduction portions of this report, contains conclusions and analysis that reflect the information available to Experis prior to the completion date of the work. Upon delivery, Experis has not continued to monitor, nor does the report reflect, any later alterations that may have been relevant to the report contents.

1 Executive Summary

1.1 Objective

From May 2014 to July 2014 City of Milwaukee (The City) engaged Experis to perform external network vulnerability assessment and test. This review was conducted to verify that adequate controls are in place for the City external network environment so that system confidentiality, integrity or availability is protected. The goal of this engagement was to identify potential security risks, provide a foundation for improved risk-based decision-making, and prioritized investments.

1.2 Scope

Experis was engaged by the City to test the security of its external and internal networks by simulating a hostile attack. The activities performed within this type of activity are commonly performed in one of three ways – White-Box (detailed technical knowledge of network), Gray-Box (limited knowledge), or Black Box (no knowledge). Experis applied the Gray-Box technique utilizing only limited knowledge about the environment provided to Experis by The City. This approach simulates an attacker with some knowledge of the systems. It also allowed Experis to target the selected in-scope systems and produce more focused results in less time.

1.2.1 Network Penetration Testing Approach

The general activities performed by Experis during the External Network and Internal Network components of the engagement consisted of the following four major phases:

- **Phase I** – Perform a discovery and footprint analysis of the network. Specifically, determine and confirm where the external and internal network connectivity begins and ends (i.e., the in-scope network segments), and gain a basic understanding of the types of systems and services accessible from the Internet and from internal network segments.
- **Phase II** – Perform automated vulnerability scans of all externally facing devices and internal devices that were discovered in Phase I and considered in-scope by The City management. The results provide an increased understanding of the accessible operating systems, ports, and services, where vulnerabilities may exist.
- **Phase III** – Attempt to exploit the high and medium risk vulnerabilities discovered in Phase II. Determine if other vulnerabilities exist based on manual activities performed in this Phase. Determine the success or failure levels of the activities to exploit the vulnerabilities and produce adequate evidence to substantiate findings.
- **Phase IV** – Produce a consistent and complete report covering the technical vulnerabilities, risks associated with the vulnerabilities, priorities for remediation, and potential root-cause discussions, to facilitate timely enhancements to the overall network security strategy.

The web application security test consisted of the following activities:

- All in-scope application elements were scanned for a variety of potential vulnerabilities such as vulnerable ports and services, out-of-date software versions, and mis-configurations. Scans were conducted using log on credentials provided by the City.
- Based on the results of the initial scans, Experis identified potential attack vectors with higher probability of success (based on prior experiences and research).
- The applications were mapped and common security issues such as Cross-Site Scripting (XSS), SQL Injection (SQLi), and Command Injection (CMDi) were identified. Tests were then performed by

identifying available input fields, including form inputs, cookie values, URL parameters and HTTP headers. The web sites were ‘fed’ a variety of data in an attempt to expose opportunities that could may lead to further compromise.

- Manual testing of the external web application was also performed. These activities included validation of findings from the automated scans and further reviews of possible exploitation points. The nature of web application vulnerabilities is such that successful exploitation often requires that attacks be unique to each application. Manual testing involves crafting requests to the application, analyzing the returned values, and attempting to avoid or subvert security measures.

1.3 Report Content

This report only provides summary information on datacenter activities in order to protect the confidential and sensitive nature of City datacenter operations. Detailed findings and recommendations were sent to all datacenter managers and a written management response was received indicating their action plan to further enhance security. The vulnerabilities are currently undergoing review and assessment by datacenter management; and the noted items are being addressed with the appropriate solution to minimize risk.

Specific department follow-up to these recommendations will be managed, tracked and reported by Internal Audit.

1.4 Engagement Team

The assessment team consisted of the following Experis personnel:

- John Hainaut – Director, Information Security Center of Expertise (ISCOE)
- Peter Paul – Security Professional, ISCOE