TORONTO

REPORT FOR ACTION WITH CONFIDENTIAL ATTACHMENT

Information Technology Vulnerability Assessment and Penetration Testing - Wrap-up of Phase I and Phase II

Date: March 10, 2017
To: Audit Committee
From: Auditor General
Wards: All

REASON FOR CONFIDENTIAL INFORMATION

This report involves the security of property belonging to the City or one of its Agencies or Corporations.

SUMMARY

The alarming increase in cybercrimes and threats to critical information and infrastructure including the high cost of data breaches across industry led the Auditor General to perform vulnerability assessment and penetration testing at the City.

In early 2016, the Auditor General completed an external vulnerability assessment and penetration testing of the City's information technology (IT) network. The testing included the external facing applications and firewall to determine if unauthorized access to the City's corporate network and systems could be gained from the outside.

The Phase I report on External Penetration Testing (with confidential attachment) was tabled at the March 30, 2016 Council meeting.
http://www.toronto.ca/legdocs/mmis/2016/au/bgrd/backgroundfile-90751.pdf

Later in 2016, an internal vulnerability assessment and testing of the City's IT network, servers and systems was performed. The goal was to identify vulnerabilities that could be exploited by someone from within the City (contractors, employees, persons accessing City buildings) who may have access to the City's IT network, servers and systems.

The Phase II, Part 1 report on Internal Penetration Testing – Accessibility of Network and Servers (with confidential attachment) was tabled at the November 8, 2016 Council meeting.
http://www.toronto.ca/legdocs/mmis/2016/au/bgrd/backgroundfile-97617.pdf

As mentioned in our Phase II report, testing was divided into two parts. This current report includes results of Phase II, Part 2 - Application Vulnerability Assessment and Penetration Testing, as well as a wrap-up of all our penetration testing audits completed in 2016.

Additional information is included in the confidential attachment 1. The Auditor General will continue to perform these types of audits to ensure the City's critical information and infrastructure are adequately protected.

RECOMMENDATIONS

The Auditor General recommends that:

1. City Council request the City Manager to review how best to create and implement a Chief Information Security Officer's role reporting administratively to the Chief Information Officer and functionally to the City Manager. The Chief Information Security Officer should coordinate with the Chief Information Officer:

a. To develop information technology security baseline standards at the City, and report to the City Manager and Chief Information Officer on compliance to established baseline standards.
b. To work with City Agencies and Corporations to align baseline standards and leverage best practices.

2. City Council direct that Confidential Attachment 1 to the report (March 10, 2017) remain confidential in its entirety as it contains confidential information involving the security of property belonging to the City or one of its Agencies and Corporations.

FINANCIAL IMPACT

The implementation of the recommendation in this report will strengthen information technology controls at the City and its Agencies and Corporations. The extent of costs and resources needed to implement the recommendation is not determinable at this time. The investment to improve controls to manage and respond to cyber threats offsets the potentially significant costs that could result from security breaches.

DECISION HISTORY

The Auditor General's 2015 Audit Work Plan included a project related to the City's information technology vulnerability assessment and penetration testing. The Auditor General's 2015 Audit Work Plan is available at: http://www.toronto.ca/legdocs/mmis/2015/au/bgrd/backgroundfile-79980.pdf

The purpose of this audit was to assess whether the City's IT systems and assets are adequately protected from external and internal threats.

COMMENTS

Auditing IT vulnerabilities and penetration testing is a highly specialized area. This audit required the combined information technology skills of audit staff and the expertise of external consultants.

The audit tests were designed to simulate the approach and techniques that an attacker would use to find weaknesses in the City's IT networks, servers and systems.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Audit Scope and Methodology

The audit methodology included the following:

- Meetings with the external consultant and the Corporate Information & Technology Division to define the scope of testing, emergency contacts and notification protocols
- Identification of in-scope IT networks, servers, systems and applications, testing scenarios, risks and testing exclusions
- Performing the vulnerability assessment, scanning and analysis using specialized tools to execute automated and manual security testing
- Investigation and validation of findings

A sample of applications and systems was selected for vulnerability assessment and penetration testing. Detailed testing was performed on 50 network addresses (devices attached to the City's network), three web applications and five private City wireless networks.

The audit team used the industry standard Common Vulnerability Scoring System (CVSS) ratings and the Penetration Testing Execution Standard to align the defined severity to the vulnerabilities identified.

Table 1: Risk Category Definitions

Risk	Score	Description
Critical Severity	9.0-10	Exploitation of the vulnerability discovered on the system can directly lead to an attacker gaining privileged access to the machine over a remote connection. Exploitation is trivial or exploits exist and are easily carried out.
High Severity	7.0-8.9	Exploitation of the vulnerability discovered on the system can directly lead to an attacker gaining privileged access to the machine over a remote connection.
Medium Severity	4.0-6.9	Exploitation of the vulnerability discovered on the system can directly lead to an attacker gaining non-privileged access (e.g. standard user) to the machine over a remote connection. Exploitation of the vulnerability may also lead to a significant negative impact on system services.
Low Severity	0.1-3.9	The vulnerability discovered on the system, when combined with other vulnerabilities discovered, may lead to an attacker gaining non-privileged access (e.g. standard user) to the machine over a remote connection.

In September 2016, the Harvard Business Review noted that *the Biggest Cybersecurity Threats Are Inside Your Company,* this is referred to as the "Insider threat" https://hbr.org/2016/09/the-biggest-cybersecurity-threats-are-inside-your-company.

This article referred to the 2016 Cyber Security Intelligence Index, where IBM found that 60 per cent of all attacks were carried out by insiders. The average cost per breach as per a study sponsored by IBM in 2016 was US $4 million. This study involved 383 organizations. http://www-03.ibm.com/security/data-breach/

The Auditor General has recommended that information technology security baseline standards be developed and tested by the CISO to ensure organizational compliance with these standards.

The Auditor General has recommended the CISO report administratively to the CIO and functionally to the City Manager to align more with best practice.

Management Actions

Management's response to the recommendation in this report is attached as Appendix 2. Management has agreed with all 10 of the Auditor General's recommendations for Phases I and II and a plan is being developed to implement the recommendations.

CONTACT

Julian Lebowitz, Audit Manager, Auditor General's Office
Tel: 416-392-8473, Fax: 416-392-3754, E-mail: Julian.Lebowitz@toronto.ca

Syed Ali, Audit Director, IT & Strategy, Auditor General's Office
Tel: 416-392-8438, Fax: 416-392-3754, E-mail: Syed.Ali@toronto.ca

SIGNATURE

Beverly Romeo-Beehler
Auditor General

ATTACHMENTS

Confidential Attachment 1 - Results of the Vulnerability Assessment and Penetration Testing

Attachment 2 - Management's Response to the Auditor General's Review of Information Technology Vulnerability Assessment and Penetration Testing-Wrap-up of Phase I and Phase II