City of Melrose

Cyber Security Best Practice

Prepared By: The Office of Municipal & School Technology

EOTSS | Executive Office of Technology Services & Security

Image: Melrose City Hall[1]

Introduction

Located just 7 miles from Boston, the City of Melrose has the benefits of a bustling metropolis and a quaint community. With a population of 26,983 and median household income of $87,712[2], the City is home to lush parks, historical Victorian homes, Ell Pond, and more. Melrose has a thriving business community, excellent school system, a local hospital, and a wide variety of cultural and recreational activities, making it an ideal place to live and visit. City officials are proud of their historic and cultural gems and seek to preserve and protect them by ensuring proper equipment and procedures are in place to do so. In alignment with this goal, the City joined the Community Compact Best Practice program in December of 2017 and received grant funding to perform a comprehensive cyber security assessment. Melrose worked with ePlus Technology, Inc. to identify gaps in their IT environment and provide recommendations for remediation. Due to the sensitive data contained in their final assessment report, it is not available for public consumption. This document provides a high-level overview of the work that was completed with Melrose, as it was described in the assessment report.

[1] Cmh2315fl. "Melrose City Hall (Melrose, Massachusetts)". *Flickr.com.* https://www.flickr.com/photos/21953562@N07/12507455623/in/photolist-k4eYNB-k4eT2g-k4e8oX-k4ePMk

[2] "Community Facts". United States Census Bureau. *American FactFinder*. https://factfinder.census.gov/faces/nav/jsf/pages/community_facts.xhtml

Project Process

For their Community Compact, the City of Melrose had ePlus conduct a cyber security assessment and penetration test of their network infrastructure to expose any vulnerabilities that would lead to the loss of sensitive data. ePlus reviewed the City's security infrastructure with the following goals in mind:

- Identify if a remote attacker could compromise any of their systems or obtain information about the City of Melrose that could aid in malicious activities.
- Identify if an attacker inside the network could compromise any of their systems and obtain sensitive or confidential information. This engagement takes the perspective of a disgruntled employee or an attacker that has already breached the perimeter of the network, etc.
- Identify any security weaknesses in the City's wireless network

Attack efforts were focused on identifying and exploiting any security weaknesses that could allow an attacker to gain unauthorized access to organizational data. The following 5 phases represent the services that were performed.

PHASE 1 – OPEN SOURCE INTELLIGENCE (OSINT) RECONNAISSANCE AND INFORMATION GATHERING

During this phase, ePlus's main goal was to find sensitive data that could be used to access the City of Melrose's network. This phase identified what an attacker could see and target, and how critical the information is. ePlus aimed to find any IP Assesses, Email Addresses, Sensitive Information, and Disclosed information online that could potentially harm the City. As a general best practice, ePlus suggests that all communities be aware of information attackers can find on the web and employ additional monitoring methods to protecting those assets. Web-based information is likely what an attacker will target first.

PHASE 2 – EXTERNAL VULNERABILITY & PENETRATION TEST

ePlus conducted external testing of Melrose's network and compared their practices to other communities of a similar size. They performed heavy scanning on some of the external hosts and web services, as well as advanced comprehensive enumeration. After the tests were completed, ePlus summarized their findings and provided recommendations.

PHASE 3 – INTERNAL VULNERABILITY & PENETRATION TEST

In addition to external testing, ePlus also conducted tests to identify any internal vulnerabilities. They used two approaches to achieve this objective.

- *Non-Credential* – The first approach was from the perspective of a user who did not have authenticated access to the City's network and aimed to penetrate the Police Department's systems. After scanning their infrastructure, ePlus communicated any gaps that were found and provided recommendations.
- *Credential* – The second approach was done on the entire network from the perspective of a user with credentials. ePlus looked for items such as missing third-party software and library patches, as well as enumerated active directory to determine if best practices were being followed. As with the non-credential scanning, ePlus communicated any gaps that were found and provided recommendations for remediation.

PHASE 4 – WIRELESS SECURITY ASSESSMENT

In this phase, ePlus used standard techniques and exploits in an attempt to gain access to Melrose's wireless network. Upon completion, ePlus provided recommendations and general best practices to the City for securing wireless connections.

PHASE 5 – SOCIAL ENGINEERING ASSESSMENT

ePlus performed a spear phishing assessment against all employees that were identified by Melrose's technical staff. Spear phishing is one of the leading attack vectors and is the leading contributor to network breaches. Phishing tests are a great way to gauge employee awareness around cyber threats. From this exercise, ePlus concluded that employee awareness around phishing and other malicious threat vectors is above industry average. They were unable to gather credentials from any employees that were phished.

COMPARATIVE RESULTS

After completing phases 1-5, ePlus analyzed their collected data and ranked the City's results in two matrices. Descriptions of the matrices and color-coded rankings can be seen below:

Assessed Area	Comparison Rating
External Security Assessment	
Internal Security Assessment	
Wireless Security Assessment	
Spear Phishing Assessment	

Image: Matrix Format

The first matrix is a comparison matrix that is based on what ePlus observes from other organizations they assess and where Melrose stands with respect to those observations.

- *Green* – indicated that the information security posture and effort of the information security team at the customer location is above industry average
- *Yellow* – indicates that the information security posture is average. There are some areas that need improvement
- *Red* – indicates that information security posture is below average and there are considerable amounts of areas that need improvement

In the second matrix, ePlus uses a vulnerability and exploitation-based criteria to depict the severity of findings and the amount of vulnerabilities found in each area assessed.

- *Red* – indicates numerous (more than 10 unique) exploitable vulnerabilities found that could potentially take a considerable amount of effort to patch. Efforts lead to system compromise and/or domain compromise
- *Yellow* – indicates the presence of exploitable vulnerabilities which lead to system and/or domain compromise. The effort needed to remediate said vulnerabilities is feasible within a reasonable time period
- *Green* – indicates minimal or no exploitable vulnerabilities were found and minor and no configuration changes should be made

Conclusion

The successful completion of this Cyber Security project through the Community Compact program has left the City of Melrose better equipped to mitigate future security risk. While this project was able to highlight many strengths in the City, such as employee awareness of phishing tactics, it also provided the documentation, findings and recommendations the City can use to address identified gaps.