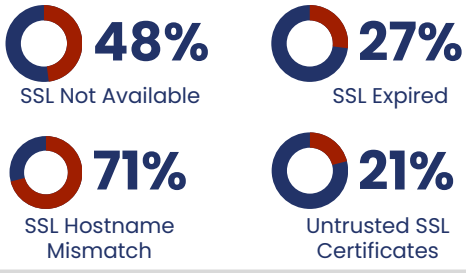
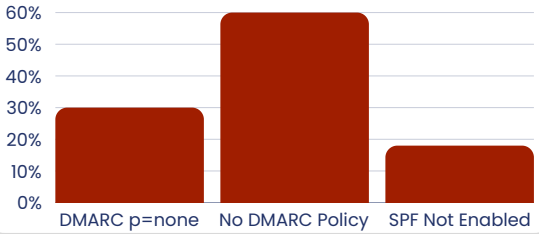
Municipal Attack Surface

This document provides practical guidance for identifying and addressing the most common vulnerabilities discovered amongst municipalities in the Northeast Homeland Security Region of Massachusetts.

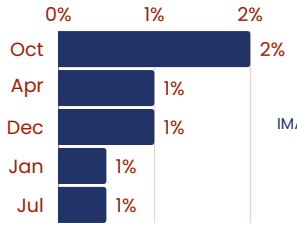
SSL Security Findings



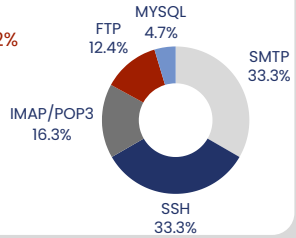
Email Security Configuration Findings



Quarterly Average Score of fixed vulnerabilities



Unnecessary Open Ports



The average score of the region improved most during Cybersecurity Month (October), indicating the collective efforts of cyber advocates throughout Massachusetts culminate in the fall.

CRMWG Cyber Resilient Massachusetts Working Group

MassCyberCenter.org

Email Security (DMARC/SPF/DKIM)

Why is this important?

The simplest way for an attacker to compromise a municipality is to impersonate ("spoof") a trusted employee, vendor, or other external user via email. Without a DMARC policy (along with SPF and DKIM protocols), this is easy to do – there are even online services that will do it for you for about $25. Whether it is to trick users into downloading malware or, as has been seen more recently, into transferring large sums of money to fraudulent bank accounts, a missing or incorrectly configured DMARC policy puts your entire municipal organization at risk.

What do these vulnerabilities mean?

- **No DMARC Policy:** This is the simplest of the three, it simply means that there is no gatekeeper, and your organization is at risk for email compromise.
- **DMARC p=none:** A DMARC policy has three options for what to do with a message that fails the two checks – reject (return to sender), quarantine (put in spam), and nothing (aka "none"). The organization must define which option they want to use. In this case, the organization has a DMARC policy, but it is not doing anything.
- **SPF Not Enabled:** Your guest list is not enabled, and anyone is allowed in! Emails that look legitimate, but might have a non-obvious misspelling, or a foreign character inserted can easily come through to your users' inboxes.

Key Terms Defined

- **Domain-based Message Authentication, Reporting, and Conformance (DMARC)** is an email security policy that acts like a gatekeeper, checking whether incoming emails are really coming from the domain that is shown (e.g. @anytownma.gov). It checks incoming emails against two records, an SPF and DKIM, and one of the two must pass. If a message fails both, the policy dictates what should happen to the message.
- **Sender Policy Framework (SPF)** is an email security protocol that acts like a bouncer at a nightclub checking a guestlist. In this case, the guestlist is a list of IP addresses that are allowed to send emails to your domain (e.g., @anytownma.gov). If an email arrives at the "door" from an IP address not on the list, it is rejected.
- **Domain Keys Identified Mail (DKIM)** is an email security protocol that acts like a watermark on a check or currency, allowing the recipient to confirm its presence to ensure that an email message has not been tampered with in transit.

How can I fix them?

If you understand what DNS, DMARC, SPF, and DKIM are without any explainers like we have here, type "how to set up a DMARC policy" into your favorite search engine and follow the instructions. The journey to a fully implemented DMARC policy is not hard and does not have to cost you anything. However, it does take time and attention to ensure that you will not affect your email deliverability, so start today! There are also numerous vendors who can manage this journey for a fee if you need help. Reach out to your area IT Directors for recommendations.

If you do not understand these terms, reach out to your IT Director, or Managed IT Service provider today to ask whether you have a fully implemented DMARC policy. If the answer is no, find out what stands in the way, and begin the planning process to ensure that whatever resources are needed to complete this journey are available. The average cost of a business email compromise is $125,000 and can easily run much higher if internal IT systems are compromised.

Rev - April 3, 2025

SSL & Open Ports

Why does this matter?

SSL certificates are like secure locks on your website, making sure that any information exchanged between your municipality's servers and users is protected from eavesdropping and tampering. If these secure locks (SSL certificates) are expired, mismatched, untrusted, or missing, your municipality's security could be at risk. Similarly, open ports on your network are like unlocked doors, inviting unauthorized access and potential breaches.

What do these vulnerabilities mean?

- **Expired Certificates:** These show users that the website might not be secure anymore, which can lead to data breaches.
- **Mismatched Certificates:** If the name on the certificate doesn't match the website's name, browsers will flag the site as insecure, making it easier for data to be intercepted.
- **Untrusted or Self-Signed Certificates:** These lack validation from a Certificate Authority, making them easier to fake and leaving the website vulnerable to attacks.
- **Missing Certificates:** This means the data exchanged is not encrypted, making it easy for attackers to steal information.

Key Terms Defined

- **Secure Sockets Layer** (SSL) is a security protocol that provides privacy, authentication, and integrity to Internet communications.
- **SSL Certificate:** A digital certificate that authenticates (verifies) the identity of a website and allows encrypted (secure) communication between the server and the user.
- **Certificate Authority (CA):** A trusted organization that issues SSL certificates after verifying the identity of the applicant.
- **Open Ports:** Network ports that are open and listening for incoming connections. While necessary for certain services, open ports can be exploited if not properly secured.
- **Firewall:** A network security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules, helping to secure open ports.
- **Intrusion Detection System (IDS)**: A device or software application that monitors network traffic for suspicious activity and alerts administrators of potential security breaches.

How do I fix them?

SSL Certificates:

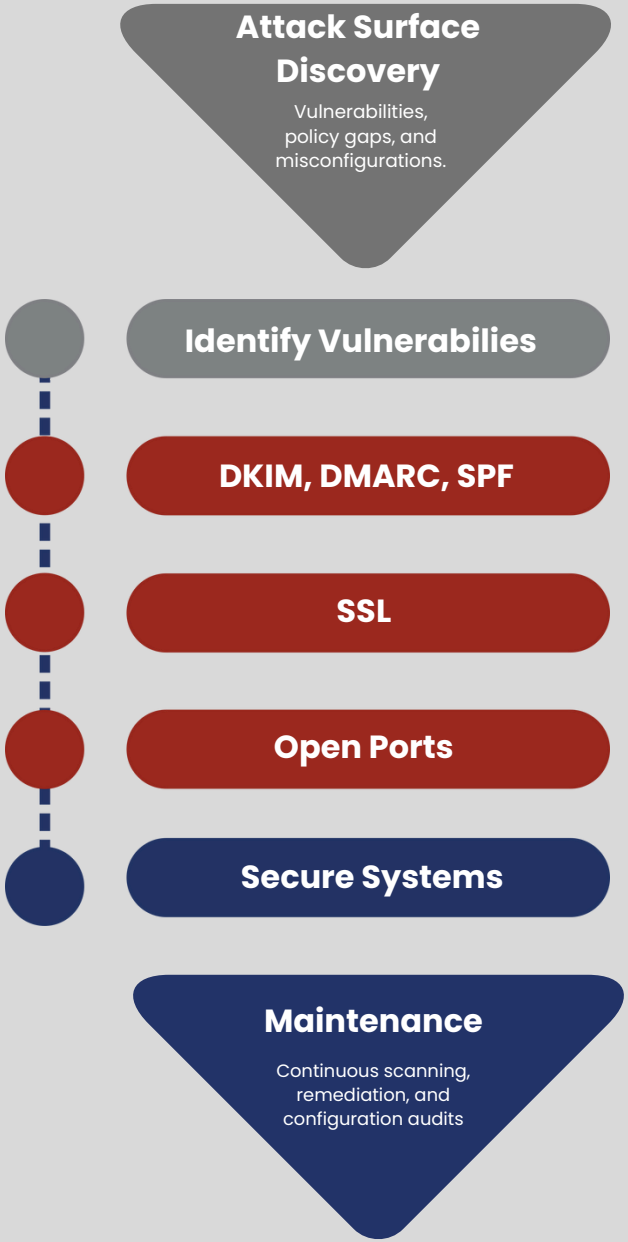
- **Monitor and Renew Certificates:** Regularly check the expiration dates of your SSL certificates and renew them before they expire. Set up automatic reminders to help with this.
- **Verify Certificate Matching:** Make sure the name on your SSL certificate matches your website's name. Use tools to find and fix any mismatched certificates.
- **Use Trusted Certificates:** Get SSL certificates from trusted sources. Avoid using self-signed certificates, especially for public-facing websites, to ensure proper security.
- **Enforce SSL Everywhere:** Use SSL for your entire website, not just for login or payment pages. This ensures all data exchanged is encrypted.

Open Ports:

- **Regular Scans**: Regularly scan your network to find open ports. Close any unnecessary ports and secure the ones you need with firewalls and intrusion detection systems.
- **Patch Vulnerabilities:** Keep your network services and devices updated with the latest security patches to protect against known vulnerabilities.

Rev - April 3, 2025

Municipal Attack Surface



CRMWG
Cyber Resilient Massachusetts Working Group
MassCyberCenter.org