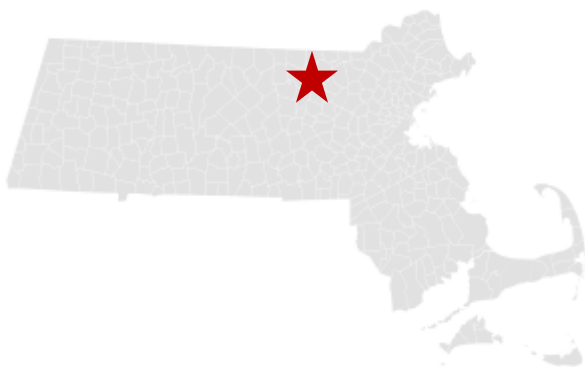


TOWN OF GROTON

CYBER SECURITY BEST PRACTICE | APRIL 2017

EXECUTIVE SUMMARY

The Town of Groton, Massachusetts adopted the Cyber Security best practice as part of a Community Compact agreement signed with the Baker-Polito Administration in October of 2015. The Town retained the services of Compass IT Compliance of North Providence, Rhode Island – a security, audit, and compliance services company - to perform penetration testing of Groton’s municipal network. In January of 2017, Compass completed their testing and delivered a report to the Town outlining their findings and recommendations. Groton’s IT Director found the report to be incredibly helpful in validating that the network is correctly configured and protected against external threats.



COMMUNITY PROFILE

The Town of Groton is located in the eastern part of Massachusetts in Middlesex County. Groton was the site of several important pre-revolution battles between British, French, and Native American forces. Today, Groton is known for having over 100 miles of walking and biking trails. 30% of all land in Groton is protected open space.

Population is 10,646 residents*
Annual Budget is \$36.4M (FY 2017)
Median Household Income is \$44,756*

**As of 2010 census*

In partnership with:



THE CHALLENGE

Municipalities of all sizes are facing the growing threat of malicious actors attempting to breach internal networks in search of personal information. Oftentimes, officials are busy running their cities and towns and don't have the time for intensive review of security.

Even a well-configured network protection appliance, like a firewall, can be inadvertently misconfigured and sometimes these errors cannot be easily determined until it's too late and a breach has already occurred.

THE SOLUTION

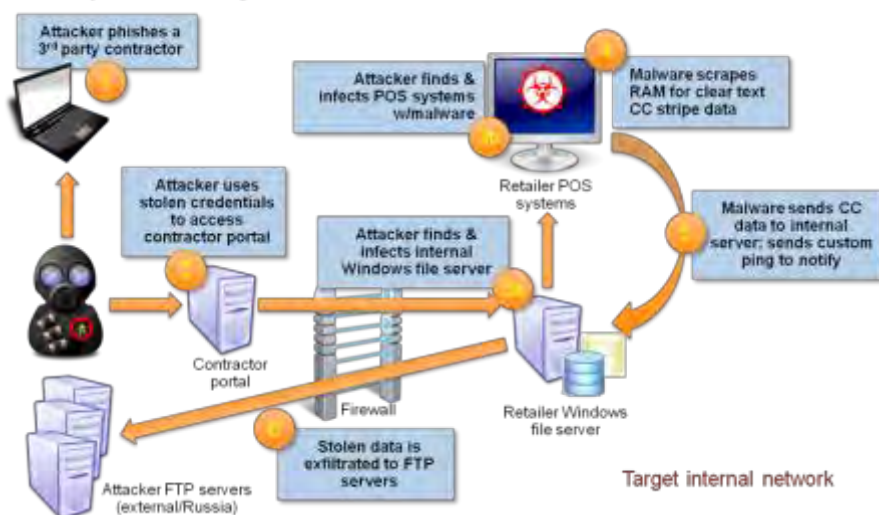
A grant was provided to Groton through a Community Compact to engage an outside firm for penetration testing of the Town's network. The goal of penetration testing is to verify that unauthorized access cannot be accomplished and that the network as a whole is up-to-date and secure against threats.

THE RESULTS

The results of the testing were provided to Groton in a confidential report. The report allows Groton to address any issues identified by the report and also provides validation by a third party that the internal network's configuration is modern, secure, and safe for municipal use.

DATA BREACH PROFILE

Anatomy of the Target Retailer Breach



In 2013, retailer Target experienced a data breach. 110 million customers were impacted by the eleven gigabytes of personal data that was stolen.

How did this breach occur? A third party HVAC contractor was phished and their stolen credentials were used to access Target's internal network.

Municipalities and retailers like Target are highly visible, attractive targets for cyber criminals. Penetration tests can help find areas of risk before they can be exploited.

Source: Security Intelligence - <https://securityintelligence.com>

"The services they performed were incredibly helpful in verifying our firewall practices were configured properly as expected for our primary site."

-Michael Chiasson, Information Technology Director

Photo Credit: Flickr – Doug Kerr in Groton, Massachusetts