NEW YORK STATE | Board of Elections

Cyber Security Update

State Board of Elections

September 19, 2017

Year in Review

Cyber Security & the 2016 Election Cycle

- Allegations of “rigged” elections
- Hacking of Democratic National Committee
- Confirmed intrusions into election systems of Arizona & Illinois
- Nearly two dozen other states reported that their systems had been scanned

Cyber Security & the 2016 Election Cycle

- Throughout the 2016 election cycle, the State Board established and cultivated relationships with various organizations, some of which listed below, who were able to provide useful information and/or resources to strengthen cyber security of election infrastructure.

  - Department of Homeland Security (DHS)
  - Federal Bureau of Investigations (FBI)
  - National Association of Secretaries of State (NASS)
  - NYS Office of Information Technology Services (OITS)
  - NYS Cyber Security Advisory Board
  - NYS Intelligence Center (NYSIC)
  - New York State Police
  - NYS Association of Counties (NYSAC)
  - NYS Local Government IT Directors Association (NYSGLITA)

Cyber Security Since the Election

- Designation of Election Systems as “Critical Infrastructure”
- January 2017 Intelligence Community Assessment
  - *“Russian intelligence obtained and maintained access to elements of multiple US state or local electoral boards. DHS assesses that the types of systems Russian actors targeted or compromised were not involved in vote tallying.”*
- Leaked NSA memo
  - VR Systems and New York

Targeted Systems

- The election infrastructure in New York State, much like the rest of the country, can be broken into three distinct parts:
  - Voter Registration Systems
  - Election Day Systems
  - Election Results Systems
- This segmented and decentralized design, along with the fact that voting machines are not networkable, make the successful hacking of an election extremely difficult.

Understanding Potential Threats & Their Impact

Understanding Potential Threats & Their Impact

- **Malware / Viruses / Ransomware**
  - Any computer that connects to any part of the election infrastructure is a target.
  - Can be activated by a user:
    - Visiting a website with malicious code
    - Accessing an email with a malicious attachment
    - Use of an infected USB device

Understanding Potential Threats & Their Impact

- **Server, Desktop & Software Vulnerabilities**
  - Unpatched operating systems and software
  - Use of weak or shared passwords
  - Excessive user privileges
  - Lack of backups

Understanding Potential Threats & Their Impact

- **Network Vulnerabilities**
  - Missing or poorly configured firewalls
  - Inability to monitor network activity or intrusion detection
  - Virtual Private Networks (VPNs) / Remote Access
  - Open WiFi

Understanding Potential Threats & Their Impact

- **Social Engineering**
  - Phishing - An attempt to obtain sensitive information such as usernames or passwords by disguising as a trustworthy entity in an electronic communication, usually email.
  - Spear Phishing - Phishing attempts directed at specific individuals or companies.
    - Attackers may gather personal information about their target to increase their probability of success.
    - This technique is by far the most successful on the internet today, accounting for 91% of attacks.

Understanding Potential Threats & Their Impact

- There are three main types of outside threats to be aware of and plan for:
  - Scanning of your systems by potential bad actors looking for vulnerabilities.
  - Attempted exploits of web applications or servers (often injection or scripting attacks)
  - Distributed Denial of Service (DDoS) attacks where targeted systems are flooded with traffic in an attempt to take down or disrupt access to a system.

Moving Forward

Moving Forward

- **National Level**
  - “Critical Infrastructure” Designation
    - Impact?
    - Coordinating Councils
    - Information Sharing and Analysis Centers
  - DHS, EAC, NASED & NASS

Moving Forward

- **State Level**
  - NYSBOE Elections Risk Assessment
    - Purpose
    - Initial survey responses due back July 7, 2017
    - Future follow up
    - Goals

Moving Forward

- **County Level**
  - Strengthen relationships with IT staff.
  - Advocate for the consideration and inclusion of your board's infrastructure in county IT security recommendations and plans.
  - Ensure the cyber security needs of your county's election infrastructure is included in your board's annual budget.

Questions?