NEW YORK STATE | Board of Elections

Cyber Security

A Risk We All Share

State Board of Elections

January 13, 2017

Cyber Security & the 2016 Election Cycle

NEW YORK STATE Board of Elections

Cyber Security & the 2016 Election Cycle

- Allegations of “rigged” elections
- Hacking of Democratic National Committee
- Confirmed intrusions into election systems of Arizona & Illinois
  - In Arizona, a county election official’s login credentials for the statewide system were compromised when they opened an email attachment, although no successful intrusion into that system occurred
  - In Illinois, there was a successful exfiltration of data of up to 200,000 voters from the statewide database, though no records were reportedly altered
- Nearly two dozen other states reported that their systems had been scanned

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

Targeted Systems

- However, an attack on any single part of our election infrastructure is a more real risk, one which should be understood and planned for as a failure of any part undermines confidence in the elections system.

- Although we recognize that there is a disparity statewide with the IT resources available to Boards of Elections, it is incumbent upon us to advocate for the needed protections to ensure the integrity of the electoral process.

- The State Board and other partners are here to help you understand the risks and mitigation strategies, along with the resources that are available to you to help implement those strategies.

- The next few slides will address some of the more common threats as well as how they could be used to target the election infrastructure.

NEW YORK STATE | Board of Elections

Common Threats and Potential Impacts

Malware and Viruses

- Most of you are familiar with these types of threats, but any computer that connects to any part of the election infrastructure can be made a carrier to affect the election infrastructure.

- Desktops that are used by election staff for voter registration or election tasks could be susceptible to viruses or malware activated by a user accessing an email with a malicious attachment, or the plugging in of an infected USB device.

- You should ensure that you have proper security protections (antivirus software, firewall, etc.) and any necessary procedures in place to avoid the potential infection of a computer that interacts with the election infrastructure.

Server, Desktop & Software Vulnerabilities

- Most of you likely piggyback off of county servers for certain tasks, like email. You may share servers with other agencies for file storage, and/or you might have a dedicated server for your voter registration database.

- All of these machines should be properly configured and kept up to date to ensure that they do not fall prey to any potential exploit.

- The same goes for your desktops. Many operating systems, browsers, email clients and other programs often require updating on a frequent basis to keep them safe.

- Although keeping servers, desktops and software up to date is a good practice across all functions, it is of particular importance with any systems that interact with or are part of the election infrastructure.

Threats from the Outside

- 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.
- The next slides will discuss ways to identify and protect yourselves from these threats.

Threats from the Outside

- Scanning of your systems:
  - You should keep logs that identify all traffic to and from the network infrastructure your systems are kept on.
  - You should review these logs regularly to identify if any known bad actors have been attempting to access your systems. In addition, frequent or repeated attempts by single sources should be reviewed for potential malicious activity.
  - Firewalls can be configured to deny traffic from specific sources, as identified by their IP address.

Threats from the Outside

- Attempted exploits of web applications or systems:
  - If you have any public facing applications (poll site lookup, registration lookup, contact forms, etc.), they could potentially be susceptible to injection or scripting attacks.
  - These attacks target applications where a bad actor could submit malicious code which could affect the application or allow access to the backend of those applications or to the data used by those applications.
  - It should be pointed out that if you share infrastructure with other county agencies, any of their applications could potentially be exploited and provide access to your systems and/or data.

Threats from the Outside

- Attempted exploits of web applications or systems (continued):
  - One example of how one system can provide access to another is the Target hack, where bad actors were able to leverage the credentials of an HVAC vendor to get into Target's systems and access sensitive data on consumers.
  - Code for any web applications should be reviewed to ensure that they are not susceptible to code injection attacks or scripting vulnerabilities.

Threats from the Outside

- Distributed Denial of Service (DDoS) Attacks:
  - This type of brute force attack looks to overwhelm a server by having a large number of traffic sources attempt to simultaneously and continually access a system.
  - Poor server and network configuration can make systems more vulnerable to being overwhelmed and taken down.
  - There are load balancing and caching systems that can be put in place to mitigate increased traffic when it happens.

Threats from the Outside

- Distributed Denial of Service (DDoS) Attacks (continued):
  - DDoS attacks could be used against web sites or web applications that provide registration, poll site and/or election results information.
  - Contingency plans for having redundant systems available to be brought online in case of failure is highly advisable.

Partners in Security

- Throughout the recent election cycle, the State Board has established and cultivated relationships with various organizations, some of which listed below, who are 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)

Partners in Security

- Despite these external organizations and resources that could potentially help counties in implementing cyber security measures, it is the responsibility of each County Board of Elections and their IT resources to be the first line of defense.

- Advocating for the consideration and inclusion of their county board's infrastructure in county IT security recommendations and plans is incumbent upon each county Election Commissioner.

- Ensuring the cyber security of election infrastructure should also be included in your board's annual budget.

Best Practices in Cyber Security

- A commitment to good cyber security and best practices is critical to protecting networks and systems. Here are a few places to start:
  - Backups:
    Do we backup all critical information? Are the backups stored offline?
    Have we tested our ability to revert to backups during an incident?
  - Risk Analysis:
    Have we conducted a cyber security risk analysis of the organization?
  - Staff Training:
    Have we trained staff on cyber security best practices?

Best Practices in Cyber Security (continued)

- Application Whitelisting:
  Do we allow only approved programs to run on our networks?

- Permissions, Privileges, and Access Controls:
  Manage permissions on user accounts wisely, especially those with administrative rights. Are we sharing passwords? Are we removing old employee accounts?

- Incident Response:
  Do we have an incident response plan and have we practiced it?

- Business Continuity: Are we able to sustain business operations without access to certain systems? For how long? Have we tested this?

Best Practices in Cyber Security (continued)

- Penetration Testing:
  Have we attempted to hack into our own systems to test the security of our systems and our ability to defend against attacks?

- Vulnerability Scanning & Patching:
  Have we implemented regular scans of our network and systems and appropriate patching of known system vulnerabilities?

Questions?