CISA
CYBER+INFRASTRUCTURE

DEFEND TODAY. SECURE TOMORROW.

Ransomware

Ransomware is malicious software designed to deny access to computer systems or data. In a ransomware attack, systems and/or data are encrypted and a payment is requested to decrypt. Paying the ransom does not guarantee a user will regain access to their systems or data and this information can be permanently lost. For elections, a ransomware attack could deny access to voter registration data, election results, and other sensitive information. It could also inhibit access to important election systems during critical operational periods such as registration and candidate filing deadlines.

Protect Your Systems and Data Against Ransomware

Committing organizational resources which emphasize cyber hygiene and cybersecurity best practices are the best defenses against ransomware attacks. CISA recommends the following precautions and best practices to protect users against the threat of ransomware:

- **Update software and operating systems with the latest patches.** Outdated applications and unpatched operating systems are the most frequent targets of ransomware attacks.
- **Apply the principle of least privilege to all systems and services.** Restricting user and third-party permissions to install and run software applications can help prevent malware from executing and spreading. Application whitelisting—specifying an index of approved software applications that are permitted to be present and active on a system—can be effective in preventing unauthorized programs from running on a network.
- **Authenticate inbound email** to prevent receipt of spoofed emails. CISA recommends implementing Domain-Based Message Authentication, Reporting, and Conformance (DMARC) and adopting a policy to, at least, quarantine emails that fail the DMARC check. DMARC can reduce the likelihood of your domain being spoofed and enable you to reduce the likelihood of clicking on a spoofed email. For more information, see CISA's DMARC fact sheet.
- **Scan incoming and outgoing emails** to detect threats and filter executable files from reaching end users. Enable strong spam filters to prevent phishing emails from reaching end users.
- **Consider leveraging network security devices** to provide defense in depth. For example, an intrusion detection system (IDS) can identify infections before they cause too much damage. Ensure any solutions you implement monitor your entire election infrastructure.
- **Secure end users against phishing and social engineering** via ongoing awareness campaigns and assessments. Ensure staff members are aware of the risks associated with opening suspicious emails, clicking links, or opening unsolicited attachments. Advise them to report any abnormal or suspicious system behavior to your IT or security teams immediately. Implement multi-factor authentication where possible.

Plan for a Ransomware Incident

Ransomware infections typically occur through user-initiated actions like clicking on malicious email links, visiting infected websites, or opening files with embedded macros or scripts. Some types of ransomware may spread to shared storage drives and other systems on the same network. To prepare for a potential ransomware incident:

- **Develop an incident response plan** that details mitigation steps for business continuity and recovery should a ransomware event occur. In addition to addressing events that affect your systems and assets directly, the plan should account for ransomware infections on other state or local government systems that may indirectly affect your jurisdiction's election infrastructure.
- **Confirm you have up-to-date points of contact on file** if the EI-ISAC or a commercial security provider monitors your networks or email. Know how to notify responders as quickly as possible.

- **Conduct a business impact analysis to understand your backup and recovery needs.** Understanding how much data your organization can afford to lose will help you establish an appropriate backup schedule. A lower tolerance for lost data may necessitate a more frequent backup schedule. Also understand what supporting applications or structures you would need to restore voter registration or election management systems to full operational capability. Simply backing up voter registration data may not be sufficient to restore operations after a ransomware attack.
- **Develop a comprehensive plan for regular backups.** Backups should be stored offline, segmented from your network, and stored on multiple types of storage media. Validate your backups and practice your restoration plan to ensure you are prepared for implementation. If possible, include a physical restore in your exercise of the plan.

Recover from Ransomware

Certain resilience mechanisms already employed in the Election Infrastructure Subsector, such as provisional ballots or paper backups for e-pollbooks, can limit the negative effects of ransomware even during critical periods in the election cycle. In addition to built-in measures like these, your organization should be prepared to implement its incident response plan quickly in the event of a ransomware attack. If you do experience a ransomware attack:

- Identify, disconnect, and shut down infected and non-infected systems to isolate them from the network and prevent propagation.
- Report the incident to the appropriate parties identified in your incident response plan, including DHS and the EI-ISAC.
    - To report an incident to DHS, call 888-282-0870 or email nccicustomerservice@hq.dhs.gov.
    - To report an incident to the EI-ISAC, contact its Security Operations Center at 866-787-4722 or SOC@cisecurity.org.
- Determine what systems or data are affected.

After initial identification and response, your organization may implement additional mitigations such as identifying the root cause of the incident, determining whether data can be unencrypted, changing account and network passwords, and restoring data and systems using backups.

The U.S. Government does not recommend paying a ransom. There are serious risks to consider before doing so. Paying a ransom does not guarantee your organization will regain access to its data. Victims who do pay may be targeted again, or the malicious actor may demand additional payments to get the promised decryption key.

CISA Services and Support

The Cybersecurity and Infrastructure Security Agency (CISA) offers a suite of free, voluntary services state and local election officials can leverage to minimize risks associated with cybersecurity threats, including ransomware. The following services can help prevent or mitigate the effects of ransomware:

- A **Phishing Campaign Assessment** evaluates the organization's susceptibility and reaction to phishing emails. After the assessment, the organization receives a report on click rates for varying types of phishing emails, summarizing the organization's tendency to fall victim to phishing attacks.
- **Vulnerability Scanning** monitors internet-accessible systems for known vulnerabilities on a persistent and continual basis. As CISA identifies potential vulnerabilities, it notifies the organization so it can implement preemptive risk mitigation efforts to avert exploitation.
- **Remote Penetration Testing** uses a dedicated remote team to assess, identify, and mitigate vulnerabilities in externally-accessible networks or election systems. Participants receive a report that includes recommendations, specific findings, potential mitigations, and technical attack path details.

Election officials interested in taking advantage of these or other free CISA services should contact cisacustomerservice@cisa.dhs.gov. Additional information on products and services are available from CISA's Election Security Resource Library.