National Cyber Awareness System:

ST19-001: Best Practices for Securing Election Systems

05/21/2019 12:46 PM EDT

Original release date: May 21, 2019

By adhering to cybersecurity best practices, election organizations—including state, local, tribal, and territorial (SLTT) governments—can improve the security of their election systems. The Cybersecurity and Infrastructure Security Agency (CISA) Hunt and Incident Response Team (HIRT) developed the best practices in this tip from lessons learned through engagements with SLTT governments, election stakeholders, and others. Organizations can implement these best practices, which harden enterprise networks and strengthen election infrastructure, at little or no cost. CISA's election systems best practices cover the following topics:

Software and Patch Management

Implementing an enterprise-wide software and patch management program reduces the likelihood of an organization experiencing significant cybersecurity incidents. A software and patch management program includes the establishment of an enterprise-wide inventory list, which provides an organization with greater insight into the software running on its networks and associated vulnerabilities. The organization can then use the inventory list to help identify and mitigate the risks to its election-related information technology (IT) infrastructure. Mitigations often include implementing application whitelisting, a best practice. (See Implementing Application Whitelisting.)

CISA has observed a correlation between the absence of a patch management program and the partial or complete compromise of an enterprise network due to the presence of commodity malware. Commodity malware is widely available, has minimal or no customization, and used by a wide range of threat actors. A partial or complete compromise could lead to additional impacts, including ransomware infection and the theft of sensitive data, which may include personally identifiable information.

Failure to deploy patches in a timely manner can make an organization a target of opportunity, even for less sophisticated actors, increasing the risk of compromise. If an enterprise-wide patch management solution is too costly, an organization should consider enabling automatic updates. CISA recommends organizations subscribe to the National Cybersecurity Awareness System for alerts about security updates, threats, and vulnerabilities. This will assist organizations in maintaining situational awareness of critical vulnerabilities present in software widely used throughout their enterprise environments. It is vital to act quickly to apply patches, especially if there is an associated vulnerability being exploited.

Log Management

Retaining and adequately securing logs from both network devices and local hosts supports triage and remediation of cybersecurity events. An organization can analyze the logs to determine the impact of cybersecurity events and ascertain whether an incident has occurred.

Centralized Log Management

Organizations should set up centralized log management:

- Forward logs from local hosts to a centralized log management server—often referred to as a security information and event management (SIEM) tool. CISA has observed threat actors attempting to delete local logs to remove on-site evidence of their activities. By sending logs to a SIEM tool, an organization can reduce the likelihood of malicious log deletion.
- Correlate logs from both network and host security devices. By reviewing logs from multiple sources, an organization can better triage an individual event and determine its impact to the organization as a whole.
- Review both centralized and local log management policies to maximize efficiency and retain historical data. CISA recommends that organizations retain critical logs for a minimum of one year, if possible.

Update PowerShell and Enable Advanced Logging

In addition to setting up centralized logging, organizations should ensure that instances of PowerShell are logging activity. PowerShell is a cross-platform command-line shell and scripting language that is a component of Microsoft Windows. CISA has observed threat actors, including APT actors, using PowerShell to hide their malicious activities.

- Update PowerShell instances to version 5.0 or later and uninstall all earlier PowerShell versions. Logs from PowerShell prior to version 5.0 are either non-existent or do not record enough detail to aid in enterprise monitoring and incident response activities.
- Ensure PowerShell 5.0 instances have module, script block, and transcription logging enabled.

Network Segmentation

Organizations can limit the impact of a cybersecurity incident by enforcing network segmentation. Proper network segmentation is an effective security mechanism to prevent an intruder from propagating exploits or laterally moving around an internal network. On a poorly segmented network, intruders are able to extend their impact to control critical devices or gain access to sensitive data and intellectual property. Segregation separates network segments based on role and functionality. A securely segregated network can contain malicious occurrences, reducing the impact from intruders in the event that they have gained a foothold somewhere inside the network. (See Securing Network Infrastructure Devices.) During on-site engagements, CISA has observed organizations without effective network segmentation suffer commodity malware compromises of all Windows hosts in their environments.

Organizations should define their distinct organizational components (e.g., human resources, IT administration, demilitarized zone, elections) and create a separate Virtual Local Area Network (VLAN) for each component. Alternatively, if feasible, organizations should implement physical network segmentation for

each component. CISA recommends that organizations restrict traffic between VLANs following the principle of least privilege. See below for additional guidance for protecting elections-specific VLANs.

Segment Elections-Related Hosts from the General User Network

- Use dedicated servers and workstations for elections-related tasks. Organizations should never allow workstations with elections-related roles—such as submitting election results to a reporting server—to be used for general purpose computing, such as browsing the internet. Organizations should ensure up-to-date patching of workstations and servers dedicated to elections-related tasks.
- Follow the principle of least privilege. Organizations should only allow elections-related VLANs to communicate with machines unrelated to elections on an as-needed basis. Other network traffic should be explicitly denied (e.g., by using a `DENY/DENY` ruleset).
- Apply the appropriate technical controls (e.g., implement Group Policy Object [GPO] and firewall rules) to restrict general internet browsing from elections-related workstations and servers.

Block Suspicious Activity

Many organizations set their security devices to alert on suspicious activity instead of blocking it. When an organization does not block suspicious activity by default, it increases the likelihood of adverse events that allow an adversary to compromise IT resources. Organizations should follow best practices in disabling network protocols known to spread malware, such as Server Message Block version 1 (SMB v1). (See SMB Security Best Practices.)

Prevent Malware and Malicious Traffic

Organizations should perform the following actions to block malicious traffic and malware:

- Enable security features. Many network appliances, cloud services, and security software (e.g., host intrusion prevention systems) have features—not enabled by default—that block malicious traffic. CISA recommends that organizations enable these features. Note: organizations should thoroughly test changes before implementing them in production environments.
- Scan all incoming emails for malicious attachments and links prior to delivery, and quarantine emails, as necessary.
- Train employees to recognize phishing attempts and ensure a process exists for reporting and triaging phishing emails.
- Block macros from running in documents throughout enterprise. (See Who Needs to Exploit Vulnerabilities When You Have Macros? for more information.)
    - Before restricting macro-enabled documents, determine if any users need macro-enabled documents to perform their work functions. If macros are not used, disable them by GPO.
    - If blocking macro-enabled documents across an organization is too restrictive, consider alternative solutions, such as only allowing macro-enabled documents for specific users or blocking macros from running when received as email attachments from external users.

Disable SMB v1

In the course of recent engagements, CISA has observed threat actors using SMB v1 to spread malware across organizations. Based on this specific threat, CISA recommends organizations consider the following actions to protect their networks:

- Disable SMB v1 internally on their network.
- Block all versions of SMB at the network boundary by blocking Transmission Control Protocol (TCP) port 445 with related protocols on User Datagram Protocol ports 137–138 and TCP port 139.

Credential Management

Managing passwords and using strong passwords are important steps in preventing unauthorized access to databases, applications, and other election infrastructure assets. Multi-factor authentication (MFA), in particular, can help prevent adversaries from gaining access to an organization's assets even if passwords are compromised through phishing attacks or other means. Threat actors have the capability to defeat single-factor authentication, especially when passwords are weak (e.g., common or trivial passwords) or—taking into account credential reuse—have been exposed in unrelated third-party breaches. CISA has published the following guidance to assist organization in achieving the goal of fully preventing unauthorized access:

- Implement MFA to prevent unauthorized access, particularly by external users, including APT actors. (See Using Rigorous Credential Control to Mitigate Trusted Network Exploitation and Supplementing Passwords.) MFA requires users to present two or more credentials (e.g., a password and the use of a hardware token) at login to verify their identity before being granted access to a given system. Organizations should consider implementing MFA for voter registration, election night reporting, and associated enterprise IT systems.
- Enforce password best practices, including the use of unique and complex passwords to access different systems and accounts. Accounts with additional privileges (e.g., administrator accounts) should have password requirements that are more stringent than those for standard users. (See Choosing and Protecting Passwords.)
- If possible, use a local administration password solution. (See Local Administrator Password Solution.)

Establish a Baseline for Host and Network Activity

An organization's IT personnel are critical in determining what is and is not normal and expected host or network activity. With the appropriate tools, IT personnel are well positioned to determine whether observed anomalous activity warrants further investigation. During on-site engagements, CISA uses the following metrics to establish a baseline for expected network- and host-based activity:

Network Baseline

- Specific metrics should include expected bandwidth usage for
    - The organization,
    - Each user (if possible),
    - Remote access,
    - Ports,
    - Protocols, and
    - File types.

- Organizations should consider variables such as the time of day traffic occurs, i.e., remote access is more suspicious occurring at 1 a.m. than during standard business hours.
- Including additional metrics—such as the destination of network traffic and the destination Internet Protocol (IP) address's geographic location—establishes a more detailed baseline.
- Once a baseline is established, an organization should review the results to determine if they align with industry best practices. (See Handbook for Elections Infrastructure Security.)
- Organizations should compare their baseline traffic with the rules from their boundary firewalls to ensure that the rules are acting as intended and align with industry best practices.

Host Baseline

- Organizations can establish a baseline by creating a "gold image" for workstations and servers. A gold image contains an organization's standard set of necessary, trusted applications installed for the set of systems for which it is designed. Once created, the organization should document the gold image's configuration. Organizations should also document approved variations from the gold image, such as tools used by the organization's network or security teams. Examples of configuration information that may be useful in identifying anomalous activity include
    - Hashes of critical operating system files;
    - Software used for remote host access (e.g., a Virtual Private Network client);
    - An organization-wide approved software list, which can help determine if detected software is not approved for the organization; and Information on configurations and settings that can be used to automatically launch software after a reboot, including services, scheduled tasks, and autorun programs.
- In addition to reviewing files on a system, organizations should review the location of file installation and the validity of the files' digital certificate, if possible.

Organization-Wide IT Guidance and Policies

Developing and maintaining guidance and policies targeted to specific situations and that assist in implementing best practices throughout the organization benefits an organization's IT ecosystem. Guidance and policies that can significantly benefit an organization's cyber hygiene include

- A cybersecurity incident response plan and corresponding communications plan (see Incident Handling Overview for Election Officials, Handbook for Elections Infrastructure Security, and Election Cyber Incident Communications Plan Template);
    - At a minimum, include
        - Roles and responsibilities of the parties in regard to the plans;
        - 24/7 contact information for the parties with critical roles;
        - Incident severity thresholds and associated role-based actions taken at those thresholds;
        - A policy establishing a user's responsibility to notify IT personnel of an IT security event; and
        - Guidance that helps determine when the organization should notify external parties, such as CISA, the Federal Bureau of Investigation, or the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC) (see Election Infrastructure Subsector Communications Protocol, EI-ISAC Formalized Notification Process, both available from CISA upon request, and Cyber Incident Reporting Unified Message).
- Patch management policies;
- Password management policies; and

- An approved software list.

Guidance and policies like these help formalize expectations for users and IT personnel. Organizations should formally document any exceptions to official guidance and policies.

CISA On-Site Engagement Preparation

CISA provides expert intrusion analysis and mitigation guidance to clients who lack in-house capability or require additional assistance with responding to a cyber incident. CISA supports federal departments and agencies, state and local governments, the private sector (industry and critical infrastructure asset owners and operators), academia, and international organizations.

Before CISA can approve an organization's Request for Technical Assistance (RTA) to provide on-network assistance to SLTT government agencies as part of a hunt or incident response, CISA requires proof that the organization has implemented login consent banners that appear on the screens of all servers and workstations accessed by the organization's staff and within the scope of the assistance. This login consent banner cannot conflict with other IT resource policies, procedures, or trainings. In many situations, CISA has successfully helped government organizations update their banners in a way that allows CISA assistance. CISA cannot approve deployment to an on-site SLTT engagement involving on-network assistance unless the RTA and login consent banners are approved. For more information regarding consent banners, see the Election Infrastructure Questionnaire.

CISA also strongly recommends that organizations maintain current internal documentation related to the Election Infrastructure Questionnaire. CISA developed the questionnaire to assist organizational documentation of election infrastructure cybersecurity posture and to identify key interdependencies.

Notice and Consent Banners for Computer Systems

This section identifies recommended elements in computing system notice and consent banners and provides an example banner. This section does not include legal advice, and the information it contains is not guaranteed to be accurate or complete. Anyone reviewing or developing a notice and consent banner should consider consulting an attorney and should note that laws can change rapidly, differ from jurisdiction to jurisdiction, and can be subject to various interpretations by various entities. Further, notice and consent banners can require tailoring based on the specific circumstances and legal jurisdiction at issue. The elements or the examples may be inadvisable depending on the entity or situation. Applicable laws may include the Fourth Amendment to the U.S. Constitution, any similar provisions in State Constitutions, and relevant federal- and state-level statutes.

Notice and Consent Banner Elements

1. The banner expressly covers monitoring of data and communications in transit rather than just accessing data at rest.
    - Example: "You consent to the unrestricted monitoring, interception, recording, and searching of all communications and data transiting, traveling to or from, or stored on this system."
2. The banner provides that information in transit or stored on the system may be disclosed to any entity, including to government entities.
    - Example: "You consent, without restriction, to all communications and data transiting, traveling to or from, or stored on this system being disclosed to any entity, including to government entities."

3. The banner states that monitoring will be for any purpose.
    - Example: "…at any time and for any purpose."
4. The banner states that monitoring may be done by the entity or any person or entity authorized by the entity.
    - Example: "…monitoring or disclosure to any entity authorized by [ENTITY]."
5. The banner explains to users that they have "no reasonable expectation of privacy" regarding communications or data in transit or stored on the system.
    - Example: "You are acknowledging that you have no reasonable expectation of privacy regarding your use of this system."
6. The banner clarifies that the given consent covers personal use of the system (such as personal emails or websites, or use on breaks or after hours) as well as official or work-related use.
    - Example: "…including work-related use and personal use without exception…."
7. The banner is definitive about the fact of monitoring, rather than being conditional or speculative.
    - Example: "…will be monitored…"
8. The banner expressly obtains consent from the user and does not merely provide notification.
    - Note: click-through banners can be best because they force the user to interact with the language.
    - Note: supporting processes should generally also preserve/provide evidence of the user's agreement to the terms.
    - Example: "By using this system, you are acknowledging and consenting to…"
    - Example: "By clicking [ACCEPT] below…you consent to…"
9. Nothing in the remainder of the banner or associated policies, agreements, training, etc., is inconsistent with, or otherwise undercuts, the elements of the banner.

Example Banner

By clicking [ACCEPT] below you acknowledge and consent to the following:

All communications and data transiting, traveling to or from, or stored on this system will be monitored. You consent to the unrestricted monitoring, interception, recording, and searching of all communications and data transiting, traveling to or from, or stored on this system at any time and for any purpose by [the ENTITY] and by any person or entity, including government entities, authorized by [the ENTITY]. You also consent to the unrestricted disclosure of all communications and data transiting, traveling to or from, or stored on this system at any time and for any purpose to any person or entity, including government entities, authorized by [the ENTITY]. You are acknowledging that you have no reasonable expectation of privacy regarding your use of this system. These acknowledgments and consents cover all use of the system, including work-related use and personal use without exception.

Additional Resources

Elections-Specific Guidance

CISA Election Security Information:
https://www.dhs.gov/cisa/election-security

Incident Handling for Elections:
https://www.dhs.gov/sites/default/files/publications/Incident%20Handling%20Elections%20Final%20508.pdf

Election Cyber Incident Communications Plan Template for State and Local Officials:
https://www.belfercenter.org/publication/election-cyber-incident-communications-plan-template

Election Infrastructure Questionnaire:
https://www.us-cert.gov/sites/default/files/publications/Elections%20Infrastructure%20Questionnaire.pdf

Securing Voter Registration Data:
https://www.us-cert.gov/ncas/tips/ST16-001

Center for Internet Security (CIS) Handbook for Elections Infrastructure Security:
https://www.cisecurity.org/elections-resources-best-practices/

Patch Management Best Practices

Understanding Patches and Software Updates:
https://www.us-cert.gov/ncas/tips/ST04-006

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-40 Rev. 3: Guide to Enterprise Patch Management Technologies:
https://csrc.nist.gov/publications/detail/sp/800-40/rev-3/final

CIS Top 20 Security Controls:
https://www.cisecurity.org/controls/

Ransomware Best Practices

Protecting Against Ransomware:
https://www.us-cert.gov/ncas/tips/ST19-001

Password Best Practices

Choosing and Protecting Passwords:
https://www.us-cert.gov/ncas/tips/ST04-002

Supplementing Passwords:
https://www.us-cert.gov/ncas/tips/ST05-012

NIST SP 800-63B Digital Identity Guidelines Authentication and Lifecycle Management:
https://pages.nist.gov/800-63-3/sp800-63b.html

Enterprise Best Practices

Securing Enterprise Wireless Networks:
https://www.us-cert.gov/ncas/tips/ST18-247

Website Security:
https://www.us-cert.gov/ncas/tips/ST18-006

Note: due to variances among enterprise networks and associated election infrastructure, organizations should not consider these best practices a prescriptive solution for all cybersecurity risks.

References

- Election Infrastructure Questionnaire