Elections Infrastructure ISAC

Essential Guide to Election Security

Search

INTRODUCTION

The Essential Guide to Election Security

MATURITY

Maturities

Determining Your Maturity Level

Prioritizing Best Practices for the Level 1 maturity

Prioritizing Best Practices for the Level 2 and Level 3 maturities

BEST PRACTICES

Index of Best Practices

Addressing Physical Threats

Join the EI-ISAC

Asset Management

Encrypt Data at Rest

Encrypt Data in Transit

Managing Infrastructure with Secure Configurations

User Management

Backups

Incident Response Planning

Building and Managing Staff

Patching and Vulnerability Management

Remediate Penetration Test Findings

Perform Internal Penetration Test

v: latest

Managing Wireless Networks

Wireless networks are a critical piece of modern connectivity. In the election environment, some systems, like voting machines, are never connected to a wireless network. Others, like e-pollbooks, often have to be to on a wireless network to properly update voter rolls. Some jurisdictions use wireless networks to transmit election results on election night.

There's also the day-to-day administration of the elections that occur on regular workstations used by employees throughout an election office. These may use wired or wireless connections and have access to private networks or the internet.

Good cybersecurity outcomes require proper management of the wireless networks and connections in offices and polling places.

Goals

1. Protect all wireless networks with basic wireless security practices (Level 1 maturity)
2. Deploy additional tools and measures to limit risk (Level 2 maturity)
3. Deploy mutual MFA for wireless access (Level 3 maturity)

Actions

For Managing Wireless Networks, the necessary actions vary by maturity as detailed below.

Level 1 Maturity

For those organizations operating at a Level 1 maturity, the important thing is to keep it simple. Avoid using wireless in risky scenarios, such as transmitting election results without the technical support of a state agency or other technical body providing guidance.

1. Use the advanced encryption standard (AES) to encrypt wireless data.
2. Create a separate wireless network (a guest network) for personal and untrusted devices.
3. Change administrator passwords on routers and other wireless access points to a secure passphrase.
4. Change the default access passphrase for wireless networks regularly, or enable user level authentication for private networks.
5. Don't permit visitors to use your primary wireless network. Instead set up a guest network.
6. Carefully decide whether a new device will be allowed on the network; you don't need to permit every new device onto the network.
7. Keep firmware and software up to date by including your router and other access points in your patching schedule.
8. Track what's on your network.
9. Use secure network management and communication protocols (e.g., 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise or greater). All wireless access points owned and operated by the jurisdiction should use either WPA2 or WPA3 with a strong password.

Level 2 Maturity

Organizations operating at a Level 2 maturity should take additional actions, including:

1. Maintain an inventory of authorized wireless access points to ensure rogue ones are not introduced.
2. Disable wireless access on devices if the device does not strict require wireless connectivity.
3. Disable peer-to-peer wireless network capabilities on wireless clients to prevent communication between devices that is not visible on the wireless network.

Level 3 Maturity

Organizations operating at a Level 3 maturity should take additional actions, including:

1. Use wireless authentication protocols that require mutual, multi-factor authentication.
2. Detect wireless access points connected to the wired network.

Cost-Effective Tools

- Aircrack-ng: Wireless security suite
- Kismet: Wireless security and investigation
- Wireshark: Packet capture analysis

Learn More

- CIS's Mobile Security Companion Guide
- NIST Special Publication 800-153: Guidelines for Securing Wireless Local Area Networks (WLANs)
- NIST Special Publication 800-94: Guide to Intrusion Detection and Prevention Systems (IDPS)

Mapping to CIS Controls and Safeguards

- 12.1: Ensure Network Infrastructure is Up-to-Date (Level 1 maturity)
- 3.10: Encrypt Sensitive Data in Transit (Level 2 maturity)
- 12.3: Securely Manage Network Infrastructure (Level 2 maturity)
- 12.6 Use of Secure Network Management and Communication Protocols (Level 2 maturity)

Mapping to CIS Handbook Best Practices

- 5, 56

Previous
Network Monitoring and Intrusion Detection

Next
Public-Facing Network Scanning

Made with Sphinx and @pradyunsg's Furo
Last updated on Mar 13, 2024