DIGITAL COMMUNITIES

A **CENTER FOR DIGITAL GOVERNMENT** ISSUE BRIEF | Armis

ELECTION SYSTEMS REQUIRE UPGRADING AHEAD OF VOTING

How officials can act quickly to boost protection

When folded into a comprehensive cyber defense strategy, passive monitoring can help build trust in election systems.

To protect voting outcomes, every step of the election process must be secure. Election machines are particularly vulnerable to cyberattacks because they're network-connected and expand the attack surface of government entities.

The traditional approach to network endpoint security includes installing a software agent for monitoring, detection and response (MDR). Unfortunately, election machines are typically impossible to secure with agent-based MDR. Moreover, election authorities often rely on legacy security policies and procedures that need immediate updates to meet modern cybersecurity requirements.

One way to address these limitations is implementing passive monitoring software that tracks every asset in an election authority's network. When folded into a comprehensive cyber defense strategy, passive monitoring can help build trust in election systems.

ELECTION SECURITY CHALLENGES

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) warns the nation's elections systems are potential targets of phishing, malware, ransomware and distributed denial-of-service (DDoS) attacks. According to CISA, criminals could target electronic poll books and voter registration databases to sow chaos and delay counts.

"Visibility starts with understanding the full scope of a network's exposure to attack," says Michael Atkinson, principal sales engineer with Armis, an asset intelligence cybersecurity company. "This means identifying all network assets and making sure they are not being misused."

AGENTLESS MONITORING AND ELECTION SYSTEMS PROTECTION

Comprehensive network asset monitoring is a pillar of cyber defense because it tracks devices and ensures they're on task. Some cybersecurity software vendors provide monitoring by installing, on each network asset, a software agent that alerts authorities when something amiss happens.

However, software agents may degrade the performance of assets and networks. Election systems complicate the picture because voting machine manufacturers typically design them to prevent the installation of monitoring agents.

"They don't want you to change anything," Atkinson says. "And a security agent is a big change on a device."

Staying aware of cybersecurity and global politics news is one of the best ways to anticipate potential attacks.

Thus, comprehensive tracking of election network assets requires agentless monitoring. Software passively observes every asset on a network — and all its relevant data — with no software agent. Artificial intelligence (AI) and machine learning algorithms scan a database to interpret the meaning of network behavior in real time. The system is optimized to identify "good" asset behavior and send alerts when network assets' actions deviate from the norm.

"We are monitoring billions of customer devices in real time right now," Atkinson says. "We have tens of millions of unique device profiles, which gives us an unprecedented look into what devices are doing, what they should be doing and what they should not be doing."

PREPARING FOR THE 2024 ELECTION SEASON

Passive asset monitoring can help election officials secure their managed network assets. More importantly, it can protect unmanaged assets with configurations that cannot be changed.

But even the best passive monitoring is not a cure-all. Comprehensive election system security requires a robust cyber hygiene program, preferably built on Zero-Trust principles that limit intruders' ability to move laterally within your networks.

Staying aware of cybersecurity and global politics news is one of the best ways to anticipate potential attacks. Your adversaries won't limit their actions to breaching election management systems. They will launch disinformation campaigns to influence voter turnout.

"We anticipate the general election this November will be targeted by malicious actors — potentially the same players that attacked the last general election," Atkinson says. "Threat actors are opportunists. They time their actions to get the most out of their efforts, especially when it comes to geopolitics."

BEST PRACTICES FOR IMPLEMENTATION

- ✓ Identify vulnerabilities and prioritize most pressing needs for threat remediation.
- ✓ Deploy monitoring software before you need it. Don't wait for an attack.
- ✓ Give yourself enough time to analyze what you have learned from the software and take proper action when alerted.
- ✓ Make sure you have buy-in and cooperation from top management, cybersecurity teams and anyone else responsible for election security.

[1] www.cisa.gov/cybersecurity-toolkit-and-resources-protect-elections
[2] apnews.com/article/election-security-2024-cybersecurity-misinformation-cisa-b374e32925e1f9d14c9003a1a182d24b

This piece was written and produced by the Center for Digital Government Content Studio, with information and input from Armis.

ADOBESTOCK