ARMIS®

WHITE PAPER

Securing U.S. State and Local Entities:

Top 4 Cybersecurity Trends in Election Security

Introduction

Cybersecurity has emerged as a paramount concern for both public and private entities, requiring robust measures to safeguard assets and environments from bad actors. In recent years, significant strides have been made in bolstering cybersecurity within the U.S. public sector, specifically the state and local entity level, due to previous cyber attacks such as the Solar Winds Supply Chain Attack, ongoing attacks on the Pentagon, and the Colonial Pipeline Ransomware Attack. While cybersecurity investments at the state and local entity level demonstrate positive progression in protecting assets, the threat landscape evolves during an election year, and entities must understand upcoming market trends to proactively anticipate emerging challenges.

Government/public sector

30% report over two breaches annually.

The 2024 Armis Cyberwarfare Report

State and Local Entities are Investing in Cybersecurity

> New York State debuted its first $90 million cybersecurity strategy to fund schools

> Biden-Harris administration's national cybersecurity strategy

> CISA's State and Local Cybersecurity Grant Program

U.S. public sector emerging trends include:

01 | **Defend Voting Machine Breaches**

02 | **Enhance Use of AI**

03 | **Initiate FedRAMP Policies**

04 | **Fund Critical infrastructure**

Defend Voting Machine Breaches

Start with Visibility

The integrity of voting machines has become a growing concern, particularly during election years, as cybersecurity threats continue to evolve. According to a report by the Brennan Center for Justice, nearly 16 million Americans voted on machines without a voter-verified paper trail during the last major election, leaving those votes more vulnerable to breaches. Additionally, a study from the U.S. Cybersecurity and Infrastructure Security Agency (CISA) revealed that over 60% of election jurisdictions were operating systems more than 10 years old, which are increasingly susceptible to hacking attempts. These alarming statistics highlight the urgent need to modernize voting infrastructure and strengthen election security to protect democratic processes.

To defend against voting machine breaches during an election, elections agencies need to consider visibility gaps. Due to the explosion of unmanaged assets in recent years, many agencies are experiencing a visibility gap where IT and security leaders can't see all of the vulnerable assets within their environment. Expect state and local entities to prioritize visibility into all vulnerable assets, especially voting machines. Entities cannot secure what they can't see or track, so visibility will be the foundation of improving their security posture ahead of an election.

Agentless Monitoring for Election Systems Protection

Comprehensive network asset monitoring is pivotal, but software agents can be impractical for election systems. Voting machine manufacturers typically design devices to reject monitoring agent installations. This is where agentless monitoring, as Armis exemplifies, proves invaluable because it identifies device details and behavior without requiring software agents. During the 2020 U.S. election cycle, a significant breach occurred that took four hours to trace, even with access to top cyber defense experts. If Armis Centrix™ had been in use, its agentless monitoring approach could have likely identified the issue in minutes instead of hours. Armis Centrix™ continuously monitors all network assets, detects anomalies, and leverages a global database along with AI/ML algorithms to analyze real-time network behavior and identify deviations.

Enhance Use of AI

Integrating AI into Whole-of-state cybersecurity strategies

Whole-of-state is a cybersecurity strategy that aims to improve defenses at every level of state and local government by breaking down governmental silos and encouraging entities to share cybersecurity resources and information to enhance their collective cybersecurity posture. We'll see further emphasis on this framework in the year ahead, driving the adoption of security strategies across the entire ecosystem with state and local government, educational institutions, and other public and private organizations.

Ways state and local entities can go beyond traditional vulnerability scanning to address the full cyber risk management lifecycle by using intelligence engines to gain deep situational awareness along every asset while also enriching context based on what was seen before Collective AI-powered Asset Intelligence Engines can monitor billions of assets worldwide to identify cyber risk patterns and behaviors. In a universe of government assets, unique, actionable cyber intelligence to detect and address real-time threats across the entire attack surface will be a winning ticket to cut costs with secure innovation.

State and local entities will also utilize AI to preempt cyber attack threats:

- Traditionally, whole-of-state cybersecurity strategies are reactive; a "fix what is broken" tactic. In the age of generative AI, it's possible to leverage the dark web, dynamic honeypots, and HUMINT to stop attacks before they impact your government or agency. Look for governments to stop playing catch up and identify and prioritize vulnerabilities and patch them before they become breaches.
- Federal policies will incentivize organizations to integrate AI into their cybersecurity strategies, acknowledging its transformative potential in threat detection and mitigation. In the coming year, policymakers are anticipated to delineate guidelines for leveraging AI as a proactive tool in cybersecurity, fostering innovation while ensuring security and ethical standards are upheld.

Initiate FedRAMP Policies

The Federal Risk and Authorization Management Program (FedRAMP®) provides a standardized approach to security authorizations for Cloud Service Offerings. It is a prerequisite for selling security products and services to federal agencies and ensures that any technology implemented at a state or local level is "certified."

With security top-of-mind across state and local governments, more states this year will start to adopt StateRamp or similar programs modeled on what we're seeing on the federal level. As is already the trend, states will likely grandfather in organizations authorized with FedRAMP into the localized programs to expedite the deployment of trusted solutions.

Fund Critical infrastructure

During elections, bad actors could seek to cause chaos or disturbances to the electoral process and increase doubt regarding election security. Attacks against infrastructure can cause huge amounts of damage, human suffering, and financial loss. This in addition to causing distrust in government and potentially disrupting important governmental processes- everything from election administration to the regular functioning of public schools.

Organizations should take steps to protect their infrastructures, however, traditional security tools can be ineffective, including industrial control systems (ICS) and operational technology (OT) since ICS/OT assets are unable to accommodate security agents. Organizations must implement good cyber hygiene practices with a zero-trust approach, and invest in security specifically designed to see, protect, manage, and optimize all OT, IoT, and ICS assets, systems, and processes in your environment.

As elections ramp up, the need for increased cybersecurity in the U.S. state and local entities will continue to increase, necessitating proactive measures to mitigate evolving threats. By prioritizing asset intelligence, embracing AI-driven technologies, fostering public-private partnerships, and funding critical infrastructure, public sector organizations can fortify their defenses. As we navigate the uncertainties of the digital age, collaboration, innovation, and preemptive planning will be indispensable in securing the future of the U.S. state and local entities against cyber threats.

Armis, the cyber exposure management & security company, protects the entire attack surface and manages an organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world, Armis ensures that organizations continuously see, protect and manage all critical assets - from the ground to the cloud. Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society stay safe and secure 24/7.

Armis is a privately held company headquartered in California.

1.888.452.4011

Website

Platform
Industries
Solutions
Resources
Blog

Try Armis

Demo
Free Trial