JUL 23 2020

SECURITY

Microsoft Makes Azure Compatible with Election Security Sensors

Election cybersecurity efforts are ramping up with only a few months left before the general election.

by Phil Goldstein

Phil Goldstein is the web editor for *FedTech* and *StateTech*. Besides keeping up with the latest in technology trends, he is also an avid lover of the New York Yankees, poetry, photography, traveling and escaping humidity.

LISTEN 05:03

With a little more than 100 days before the general election on Nov. 3, state governments, nonprofits and technology companies are increasing their efforts to enhance election cybersecurity.

Latest Articles

4 State And Local Government Tech Trends To Watch In 2022

2022 Tech Trends: States Eye ID And Access Management To Serve Citizens Online

2022 Tech Trends: Cloud Migration For State And Local Agencies Will Be Measured

2022 Tech Trends: States Are Poised To Start Moving To Zero Trust

In late June, Microsoft announced a partnership with the nonprofit Center for Internet Security, which runs the Elections Infrastructure Information Sharing and Analysis Center. Microsoft has made its Azure cloud platform compatible with election network security sensors from CIS. Separately, CIS launched a pilot program with several states to test and verify voter registration databases, election night reporting systems and other systems.

Taken together, they represent increased election security efforts. However, time is running out before Election Day, making it urgent for state and local governments to put new enhancements in place sooner rather than later.

Microsoft Teams with CIS on Election Security

For several years, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency and state and local governments have worked with CIS to to monitor election systems and data.

This is enabled by Albert Network Monitoring, which, as *StateTech* reports, "is designed to provide network security alerts when standard malware is detected on a network, as well as advanced persistent threats."

Albert sensors make "use of open-source software in combination with the expertise of CIS's 24/7 Security Operations Center, providing enhanced monitoring and rapid notifications for much of the malicious traffic that election agencies may encounter," StateTech reports. Such monitoring helps protect voter registration systems, voter information portals and back-office networks.

Albert sensors sit on the network and collect data, which is then encrypted and transmitted to the CIS center for analysis. When an alert is verified as actionable, CIS sends an event notification to the state or local agency.

As *StateTech* reports, "this notification includes the affected IP addresses, identified issues, mitigation recommendations and a

MANAGEMENT

4 State and Local Government Tech Trends to Watch in 2022

PUBLIC SAFETY

First Responder Agencies Can Partner with the Private Sector to Be Prepared for Crises

copy of the subset of traffic associated with the event. This gives affected agencies the information that they need to begin taking countermeasures."

Up until now, cloud providers, such as Azure, have not been compatible with Albert sensors. Election officials were forced to choose between cloud services for election security or hosting the Albert sensor data on local servers if they wanted to take advantage of using the sensors, Ethan Chumley, senior security strategist for Microsoft Defending Democracy Program, argues in a company blog post.

"We're starting this journey through a pilot, which will begin this week, with 14 county Supervisors of Elections in Florida," he writes. "Moving forward, Microsoft and CIS will look to open the capability to states and jurisdictions across the United States."

MORE FROM STATETECH: Explore this infographic to discover how to protect voter information.

CIS Partners with States on New Election Security Program

CIS is working on a separate project with the U.S. Election Assistance Commission to launch a pilot technology verification program focused on nonvoting election technology, including electronic poll books, election night reporting websites and electronic ballot delivery systems.

In addition to the EAC, state election leaders from Maryland, Ohio, Wisconsin, Texas, Pennsylvania, Indiana and the Federal Voting Assistance Program (FVAP) will participate in the pilot program.

The proposed program is called Rapid Architecture-Based Election Technology Verification, or RABET-V, and it "relies on a risk-based approach that allows rapid verification of manufacturers' security claims," according to a press release.

The RABET-V pilot program "supports agile software development with a verification process that anticipates and supports rapid product changes," the release states.

The program is designed to incentivize "high-quality, modern design of IT systems updated in smaller, more manageable cycles at reduced cost of verification and re-verification with more reliable and consistent outcomes for purchasers of these systems."

"Congress created the EAC to serve as a national leader on election technology issues. This pilot program is an important part of a broader effort by the EAC to expand our technical program in a direction that will better serve election officials across the country," EAC Chairman Ben Hovland said in the release. "We are excited to play an integral role in the development of the CIS RABET-V pilot program and contribute our expertise toward its success."

QUARDIA/GETTY IMAGES

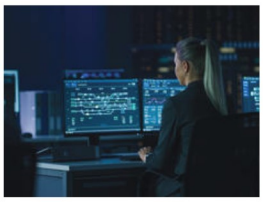
More On

NETWORK MONITORING DATA PROTECTION ENDPOINT SECURITY THREAT PREVENTION

Related Articles

Security

Security



Security