SOLUTION BRIEF

SECURING DEMOCRACY: INTEGRATED AND EFFECTIVE ELECTION SECURITY WITH THE FORTINET SECURITY FABRIC

EXECUTIVE SUMMARY

Election security is a top-of-mind concern for state and local governments, given the ongoing efforts by foreign players to impact U.S. elections. Election systems in many jurisdictions face a significant risk of compromise because of inadequate funding for cybersecurity. Federal funding of $380 billion from the Help America Vote Act (HAVA) fills a portion of that gap, and state and local governments need to be strategic in how they invest those dollars. The most effective solution is to move toward an integrated network security approach like the Fortinet Security Fabric. Such a strategy integrates a next-generation firewall with identity and access control, plus advanced threat protection—including the use of artificial intelligence (AI) and machine learning (ML). Finally, cybersecurity training for the diverse team that administers elections is critical.

Election security has been in the news in the United States since the aftermath of the 2016 presidential election, when Russian meddling in particular filled the headlines and fueled controversy. Foreign efforts to breach election systems have reportedly continued in the lead-up to the 2018 midterm elections, and diverse voices are sounding an alarm.

Since U.S. elections are decentralized by design, the responsibility for securing them falls on a patchwork of state and local governments. Most elections officials understand the challenge and are doing everything in their power to secure their systems, but insufficient funding has hampered the progress they would like to make.

LEVERAGING HAVA FOR (AT LEAST SOME) SECURITY FUNDING

Fortunately, while gridlock in the U.S. Congress has prevented new legislation from being passed, $380 million in federal funding from the 2002 Help America Vote Act (HAVA) has been made available to jurisdictions to help bolster cybersecurity ahead of the November 2018 midterm elections. The Election Assistance Commission (EAC) has already distributed most of this appropriation across states, territories, and the District of Columbia.

Though the HAVA funds are welcomed by cash-strapped elections administrators, no one is claiming that they are sufficient to fully solve the problem. Jurisdictions need to ensure that they are making informed and strategic decisions for how to allocate these funds, in order to derive the maximum benefit from each dollar spent. Of course, a one-size-fits-all approach is not possible given the diversity of elections systems and current levels of readiness. Recognizing this, the EAC has attached minimal strings to the funding, and how the grants are used will largely be determined locally.

A FEW EXAMPLES OF STATE-LEVEL ELECTION SECURITY INITIATIVES

- **Arizona**: Created a comprehensive, focused cybersecurity team
- **Colorado**: First state in the nation to launch comprehensive post-election audits
- **Minnesota**: Upgrading cybersecurity hardware, training, and procedures
- **New York**: Creating Election Support Center; conducting vulnerability assessments
- **Rhode Island**: Conducting comprehensive security risk assessment
- **Washington**: Assessing vulnerabilities via multi-state information sharing
INTEGRATING AND AUTOMATING FOR CENTRALIZED VISIBILITY AND CONTROL

As a general rule, HAVA grants are best used to unify and integrate an organization’s security architecture—rather than add more silos. Integration brings centralized visibility and controls, and enables true automation of security processes across all parts of the network.

The Fortinet Security Fabric provides a comprehensive, integrated solution that eliminates silos and provides transparent visibility on a single pane of glass—across all on-premises, virtual, and cloud-based services. It offers broad visibility and protection, integrated detection and response to advanced threats, and automated operations and analytics via a single console.

UNDERSTANDING RISKS AND PRIORITIZING INVESTMENT

Given the need for strategic use of scarce resources, state and local governments would do well to conduct an outside, formal assessment of the current state of security for the entire elections process—including registration, voting, tabulation, auditing, and records management.

The Fortinet Cyber Threat Assessment provides a thorough picture of what gaps currently exist and which infrastructure elements should be prioritized for remediation—especially in the short window of time before the midterms. Since elections systems absorb a lot of use during a compressed timeframe, the assessment’s analysis of network utilization and performance is also valuable in allocating resources.

SAFEGUARDING AGAINST ADVANCED THREATS

Regardless of the locality, the traditional perimeter-based approach to network security is no longer adequate given today’s distributed network architectures and the quickly evolving nature of the threat landscape. Even local governments now use cloud-based and virtual services applications in addition to traditional, on-premises applications—which expands the attack surface and increases risk.

The Fortinet Security Fabric is built on the foundation of FortiGate Next Generation Firewalls, which provide security beyond the perimeter, incorporating web application firewalls and internal segmentation firewalls to drive security deep into the network. This ensures that applications are protected and sensitive voter information is isolated as it moves across the network.

When the inevitable breach does occur, the FortiSIEM security information and event management solution provides the real-time visibility and analysis that is critical for fast remediation. This visibility makes it easier for security teams to detect anomalous behavior that might indicate an attack or breach.
KEEPING UP WITH CYBER CRIMINALS AT MACHINE SPEED

When it comes to threat detection, artificial intelligence (AI) and machine learning (ML) are no longer optional elements. Today’s threat landscape involves more zero-day attacks than ever before—nearly one-third of the total according to one analysis. Cyber criminals are using automation and ML tactics to make attacks faster and more targeted, which means that response must be at machine speed.

FortiGuard AI is now a part of every solution in the Fortinet Security Fabric. It autonomously collects, analyzes, and classifies threats at machine speed and with an extremely high degree of accuracy. Fortinet’s artificial neural networks (ANNs) consist of more than 3 million security sensors around the globe, each of which collects samples that are then processed by more than 5 million nodes to identify unique malicious or clean features. Using ML to train the model, threat detection is continuously updated as threats evolve, and overall accuracy is improved.

ENSURING STRONG IDENTITY AND ACCESS MANAGEMENT

One of the most critical components to election security is ensuring that only those verified as authorized users can view sensitive data. Strong access management, combined with secure network segmentation to isolate voting devices and data, will ensure that even privileged users in other areas of government—or cyber criminals who have intruded via less secure entry points—cannot view or alter votes or registration information.

FortiAuthenticator verifies the identity of those seeking access using two-factor identification, token management, single sign-on, and even biometrics. It can also provide separate access channels to secure and isolate guests and BYOD devices accessing network resources through those same access points.

BOLSTERING AWARENESS THROUGH STAFF TRAINING

Elections are administered by a very diverse group—often including full-time and temporary elections staff, other state and local government employees, and citizen volunteers who staff local precincts and vote-counting operations. Given the diversity of skills and experience represented, cybersecurity training is especially crucial.

Such training should explain cybersecurity best practices, how to identify voting machine tampering, and how to maintain proper cyber hygiene. Security awareness among the diverse team that administers elections is critical for detecting malicious activity. And since most of the staff will be working in a concentrated period of time, training can be timed so that it is top of mind when Election Day rolls around.

CONCLUSION

Election security is crucial to a functional democracy, and local elections administrators have a difficult and important job in ensuring that elections operate smoothly and their results are reliable. As with all other organizations, state and local governments do best to build an integrated security architecture and strategy that incorporates technology, awareness, and processes to protect, defend, and remediate their election environments against potential malicious intrusions and breaches.

The Fortinet Security Fabric provides a comprehensive approach to network security that covers a jurisdiction’s entire infrastructure—from the data center to multiple clouds, from voting machines to voter registration databases. With transparent visibility and centralized control, administrators can avoid manual security processes and stop advanced threats before they cause a threat to democracy.
