DEFENDING THE VOTE

A Secure Data Strategy for the 2018 Elections

Solution Point Paper

Election systems are going to be a focal point for advanced cyberattacks. Protecting the data and continuously monitoring our election systems is essential to maintain the public trust and ensure any attacker is thwarted before they can be successful.

Jeff Hornberger
jhornberger@securityfirstcorp.com

Introduction

Voting is a critical aspect of American life; it's the cornerstone of our democracy. Ensuring the voting process is secure, accurate, verifiable and trustworthy are essential requirements for our election systems. It is well known that there are nations and individual bad actors that desire to penetrate the voting infrastructure to steal data, inject uncertainty into election results, and cause harm to our networks. The continuous stream of successful attacks that occupy the front pages of national and local news agencies are proof that our current defense methodology is not completely successful at protecting valuable systems in any industry or for any agency. What can we do differently to successfully thwart these attacks?

Our organizations have extremely hard working, smart folks defending the networks. But attack vectors continue to get more creative with novel approaches while using automated capabilities to find misconfigurations or exploitation of known vulnerabilities. For the most part, our layered defenses have been focused on the network functionality (firewalls, proxies, intrusion detection/prevention systems, content filters, anti-malware, etc.). We have done yeomen's work in building and maintaining these barriers and walls, but the advances in technical capabilities and persistence of the threat continues to have significant success.

One component that has historically been lacking in the overall integrated defense is data security and monitoring. Technology solutions in this area have matured and currently can provide critical capabilities beyond network defenses, such as:

- Integrated Data Encryption
- Access Control
- Continuous Data Monitoring
- Cryptographic Segmentation for Shared Infrastructure
- Separation of Duties for Administration
- Least Privilege Access Enforcement, etc.

These capabilities provide a last line of defense for the target of most of the attacks – THE DATA.

It's time to think systematically about protecting our election systems and operations – it's time to implement a data security and control strategy to augment our existing cyber defenses, to safeguard against hackers, insider threats, employee errors and unauthorized data access regardless of network breaches. This new, secure data strategy encompasses all aspects of security; network, application, identity, data, access, and analytics, to give the organization cyber resilience across the entire election system attack surface. This new strategy can be implemented today, with minimal impact to the existing election systems in use.

Election Infrastructure Challenges:

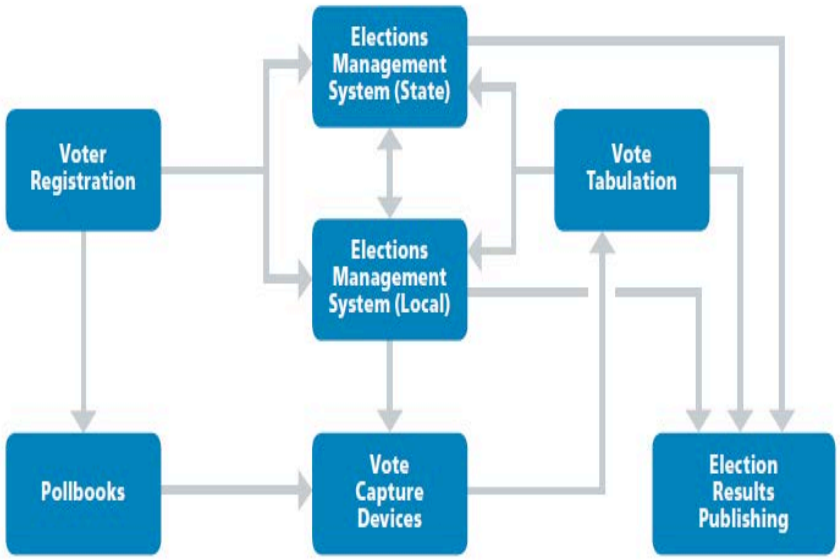

Figure 1. Standard Election Management Infrastructure

As depicted in Figure 1, the IT systems infrastructure that supports our election processes has myriad interfaces, and these vary from one location to the next, even within each state. Some of these interfaces are exclusive to the voting system and process (Vote Capture Devices, Vote Tabulation, Results Publishing); others, like the Voter registration and Pollbook system are designed to interface with other government systems (Motor Vehicles, CPS, etc.). Many of the components in our elections infrastructure are built on general purpose computing machines, such as traditional web servers and database platforms. This means they are subject to the same attacks as those in other sectors, even if they are designed for a specific purpose. Further, systems that are not always in use, that leverage shared IT resources and personnel, are subject to advanced attacks; these factors create gaps for hackers to exploit. Compound these elements with the connectivity required to external systems with multiple interfaces and different access control needs and methods; it becomes a daunting task for IT security experts to build, operate and maintain a system ready for the latest attacks.

Most IT professionals are acutely aware of and are prepared for network-based attacks. Our defenses and cyber processes are designed to stop intrusion; monitoring for unknown or unmanaged nodes, extensive use of identity management tools, etc. These defenses have been very strong, but not 100% effective. Recently there has been a significant increase in attacks that originate from within the infrastructure, where the network breach goes undetected and the hacker is able to access data and systems without being discovered for months. These hacks, termed “lateral attacks”, are effective because they occur inside the infrastructure, at the data layer, below the application where data and access are not being monitored. When

hackers successfully execute a lateral attack, they can not only get access to the most valuable asset in the system, the data, but they can operate without being discovered because there is no monitoring capability in place to determine that unauthorized access is occurring.

For election officials, these types of attacks are especially concerning. As described earlier, election systems are comprised of general computing platforms with multiple interface, access and data sharing requirements. This functionality significantly increases the attack surface available to today's sophisticated hacker, especially those that are interested in disrupting or undermining our voting process. So how can lateral attacks be mitigated or stopped?

Secure Data Strategy for 2018

Voting systems are too tempting for hackers, especially sophisticated and well supported hackers, to pass up. Success means achievement of their nefarious goal, but also frontpage news, and a psychological impact on millions of people. It doesn't matter if the effects are known immediately; as 2016 has shown finding out well after an election can be just as disconcerting and disruptive to the basic functions of government and its people. Finding out as soon as possible that a hack has been attempted is critical for stopping these ill effects; it gives you actionable information to thwart, contain, mitigate, and remediate the attack in near real time. This is achievable using continuous data monitoring and access control security defenses at the data layer.

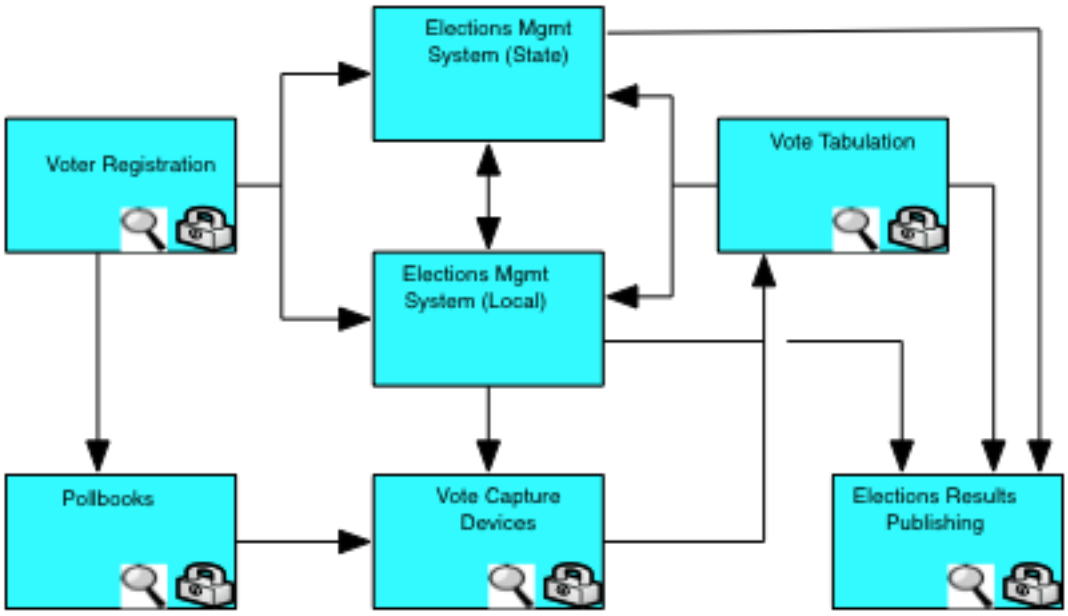

Figure 2. Election Infrastructure with Secure Data Strategy Deployed

Figure 2 is a nominal depiction of what an election system would look like deployed with a Secure Data Strategy. All existing security defenses remain in place, they are just augmented with a data security and continuous data monitoring capability.

The Secure Data Strategy must, at a minimum, provide integrated data encryption and continuous monitoring of data access at the volume, file or object level. Integrated encryption provides confidentiality and privacy of the data internal to the election system and ensures that the data remains protected if it is exfiltrated. An important distinction; not all encryption is effective for this strategy. Full disk encryption only provides data security in the event that the device is actually powered down or removed; when in use it does not restrict access to unauthorized personnel.

Continuous data monitoring provides real-time observation of data access attempts. Unauthorized access attempts are immediately identified, providing actionable information for security teams to investigate. Because this monitoring is happening below the application, any unauthorized access attempt is considered a potential threat; frequently, when unauthorized attempts are observed at this layer of the infrastructure it is due to inappropriate insider activity or hackers trying to escalate privileges. In any event, the access is denied and logged for investigation and subsequent action.

Advanced capabilities, such as automated reporting to SIEM analytics tools, cryptographic segmentation for standardized infrastructure protection, and separation of duties between application/data owners and server/storage administrators are available in some advanced data security solutions platforms offered by trusted cybersecurity experts.

Summary

Ensuring the vote is accurate, verifiable and trustworthy is essential for our election systems and processes. Our election systems face the same advanced attacks as other IT systems, but when they are affected, the consequences can be traumatic for society. Network based security is critical, but not sufficient for today's advanced hackers and attacks; a new strategy is required. The Secure Data Strategy, taking security down to the data level and delivering continuous monitoring, is essential for protecting our election systems and to defend the vote. This strategy is straightforward and available today for election officials and state directors to deploy.

About SecurityFirst

SecurityFirst™ delivers data-centric solutions that address the high-profile cyber threats facing organizations today, such as data breaches, ransomware and cloud security. We emphasize protection of the data itself and continuous data monitoring to serve as your last line of defense. Data is always protected no matter where it resides and recoverable in the event of an unexpected failure or malicious attack such as malware or ransomware. As organizations and governments mandate stricter requirements for data privacy, SecurityFirst helps protect data from compromise and exposure.