Security Tip (ST16-001)

Securing Voter Registration Data

Original release date: September 15, 2016

Voter Registration Databases (VRDBs) present a unique target for cyber threat actors. It is vital that security professionals take precautions to defend VRDBs against cyber intrusion.

Overview

Voter registration databases (VRDB) and election systems are rich targets and may continue to experience frequent attempted intrusions. This problem is not unique to individual states—it is shared across the nation. The keys to good cybersecurity are awareness and constant vigilance.

Voter Registration Databases (VRDBs) present a unique target for cyber threat actors. It is vital that security professionals take precautions to defend VRDBs against cyber intrusion.

What are the threats that may place voter data at risk?

Malicious actors may use a variety of methods to interfere with voter registration websites and databases. Some methods of attack are listed below.

- ***Phishing emails*** attempt to manipulate users into clicking on a malicious link or downloading a malicious file attachment. Systems infected through phishing attacks act as an entry point for threat actors to spread throughout an organization, steal voter information, or disrupt voting operations. For guidance to defend against phishing, see the United States Computer Emergency Readiness Team (US-CERT) Tip on Avoiding Social Engineering and Phishing Attacks.
- ***Structured Query Language (SQL) injection*** is an attack technique that attempts to subvert the relationship between a webpage and its supporting database, typically to obtain information in the voter registration database. See US-CERT's Publication on SQL Injection for more information.
- ***Cross-site scripting (XSS) vulnerabilities*** allow threat actors to insert and execute unauthorized code in web applications. Successful XSS attacks on voter registration websites can provide the attacker unauthorized access to voter information. For prevention and mitigation strategies against XSS, see US-CERT's Alert on Compromised Web Servers and Web Shells.
- ***Denial-of-service (DoS) attacks*** prevent legitimate users from accessing information or services. A DoS attack can make a voter registration website unavailable or deny access to voter registration data. Contact your Internet service provider (ISP) to discuss ways

they can help block DoS attacks targeting your organization. For more information on DoS, see US-CERT's Tip on Understanding Denial-of-Service Attacks.

- ***Server vulnerabilities*** may be exploited to allow unauthorized access to sensitive information. An attack against a poorly configured server running a voter registration website may allow an adversary access to critical information and to the supporting voter registration database itself. See US-CERT's Tip on Website Security for additional information.
- ***Ransomware*** is a type of malicious software that infects a computer system and restricts users' access to system resources or data until a ransom is paid to unlock it. Affected organizations are discouraged from paying the ransom, as this does not guarantee access will be restored to a compromised VRDB. For more information on ransomware, see US-CERT's Publication on Ransomware.

What prevention measures should I employ to protect against these threats?

DHS encourages election officials and network administrators to implement the recommendations below, which can prevent as many as 85 percent of targeted cyber attacks. These strategies are common sense to many, but DHS continues to see intrusions because organizations fail to use these basic measures.

- **Application whitelisting –** This is one of the best security strategies as it allows only specified programs to run while blocking all others, including malicious software.
- **Patch applications and operating systems –** Vulnerable applications and operating systems are the targets of most attacks. Ensuring these are patched with the latest updates greatly reduces the number of exploitable entry points available to an attacker.
- **Restrict administrative privileges –** Limiting user permissions to only necessary functions may prevent malicious software from running or limit its capability to spread through the network.
- **Understanding firewalls –** When anyone or anything can access your network at any time, your network is more susceptible to being attacked. Firewalls can be configured to block data from certain locations (IP whitelisting) or applications while allowing relevant and necessary data through.

A commitment to good cybersecurity and best practices is critical to protecting voter registration data. Here are some questions you may want to ask of your organization to help prevent attacks against voter registration websites and databases:

1. **Backups**: Do we backup all critical information? Are the backups stored offline? Have we tested our ability to revert to backups during an incident?
2. **Risk Analysis**: Have we conducted a cybersecurity risk analysis of the organization?
3. **Staff Training**: Have we trained staff on cybersecurity best practices?
4. **Vulnerability Patching**: Have we applied appropriate patching of known system vulnerabilities?

5. **Application Whitelisting**: Do we allow only approved programs to run on our networks?
6. **Incident Response**: Do we have an incident response plan and have we practiced it?
7. **Business Continuity**: Are we able to sustain business operations without access to certain systems? For how long? Have we tested this?
8. **Penetration Testing**: Have we attempted to hack into our own systems to test the security of our systems and our ability to defend against attacks?

How do I respond to unauthorized access to voter registration data?

Implement your security incident response and business continuity plan. It may take time for your organization's IT professionals to isolate and remove threats to your systems and restore normal operations. In the meantime, you should take steps to maintain your organization's essential functions according to your business continuity plan. Organizations should maintain and regularly test backup plans, disaster recovery plans, and business continuity procedures.

Contact law enforcement or DHS immediately. We encourage you to contact your local FBI field office, the FBI Internet Crime Complaint Center (IC3), or DHS's National Cybersecurity and Communications Integration Center (NCCIC) immediately to report an intrusion and to request incident response resources or technical assistance.

Author

US-CERT Publications