NASCIO 2019 Recognition Awards Nomination

iVOTE.DE.gov

State of Delaware

Department of Elections

Department of Technology and Information

iVote Security Remediation

Category: Cybersecurity

Project Initiated: Summer, 2017

Project Completed: (implementation-ongoing) - August, 2018

Contact:
James Collins, State CIO
james.collins@delaware.gov
302-739-9500

Executive Summary

Over the past several years, there has been an increasing number of reports regarding cyber-attack breaches of election systems nationwide. Due to the heightened awareness regarding these attacks, leadership from the Department of Elections (Elections) and the Department of Technology and Information (DTI) proactively formed a team to exclusively work on assessing Delaware's election system in order to identify and correct any vulnerable areas to prohibit malicious users from gaining access to secure information. The team assessed the election system in July and November 2017, providing DTI and Elections leadership with a list of the security vulnerabilities that were discovered. These vulnerabilities were within a major component of the Election's system also knows as iVote, which is the primary website for voter and absentee services. If the vulnerabilities were exploited, it could have resulted in citizens being unable to vote, a loss of voter data and a lack of voter confidence in the democratic process.

In May 2018, the team began to fix the security vulnerabilities and faced a tight timeline of only three months to deliver a more secure voting system and processes. Due to the September primary election, the major iVote system risks had to be mitigated by August 1, 2018. The team successfully addressed the vulnerabilities in time for the primary election. The team also developed an auditing process to capture cyber activity from all system components which significantly enhanced the security monitoring. The auditing process alerts IT personnel in real time if and/or when a malicious attack is attempted, allowing staff to take action to negate the threat immediately.

All of the security measures implemented resulted in a successful primary election. This project ensured the protection and integrity of Delaware's electoral process and voter data, prevented system hacks from cyber criminals and increased voter confidence.

Exemplar

One of DTI's strategic goals is delivering Reliable, Secure, and Resilient Services. DTI oversees Executive Order 55, Establishment of the Delaware Cyber Security Council, which focuses on developing best practices to mitigate cyber security risks and improve the overall security posture of the State. The iVote project directly relates to Executive Order 55 objectives centered on cyber security protections. Due to heightened awareness regarding the increasing prevalence of election systems cybersecurity attacks and data breaches, leadership from the Department of Elections (Elections) and the Department of Technology and Information (DTI) proactively formed a team to exclusively work on assessing Delaware's election system. The goal was to identify and correct any vulnerable areas to prohibit malicious users from gaining access to secure Delaware voter information. The benefits of this project were to secure Delaware's election system and processes, thus providing integrity in the process and the confidence of our citizens. Election systems were also designated critical infrastructure by the federal government.

Concept

DTI's Application Delivery team was the project sponsor/champion. DTI and Elections leadership and management were engaged during the assessment with the anticipation that some remediation work would need to be completed. Support was obtained by outlining the vulnerabilities, risks, and impacts. DTI leadership provided feedback to the project team on a monthly basis and when requested. DTI leadership also provided direction when technical team members could not reach consensus on the best course of action for various cyber security issues and proposed fixes. The Chief Information Officer acted as a liaison with the Elections Commissioner.

The iVote Security Remediation team was created to ensure the security of voter data and the integrity of Delaware's electoral processes. IT processes that are necessary for a fully functioning election system includes results transmission, storage of election data collected from the voting locations, and logging of all transactions and activities throughout the election system. Team members were temporarily re-assigned from their normal job duties to work exclusively on mitigating the cyber security vulnerabilities and tasked with the security remediation. This project was labor-intensive and fast paced. Many hours were invested after normal work hours on the development and delivery of solutions. The team was extremely dedicated and aware that the work they were doing was not only important to DTI, Elections and the General Assembly, but also to Delaware citizens. Each team member took personal ownership in delivering a solution that addressed critical security threats in the Elections systems.

In order to properly convey the impact and risk of cyber security vulnerabilities, the team had to translate information from technical to non-technical terms for the senior leadership of DTI and Elections. The team proactively evaluated major components of Delaware's election system using a combination of security scanning tools and manual reviews of software, networks, and processes to determine areas of vulnerability. Prioritization of these vulnerabilities was made jointly by Elections and DTI as to the areas where significant enhancements could be made within the allotted timeframe. In order to provide Delaware's citizens with a secure system and confidence regarding the safeguarding of their information, this project was made a top-priority for both agencies

DTI's Application Delivery team was the project sponsor/champion. They began the election system assessment in July 2017. DTI and Elections leadership and management were engaged during the assessment with the anticipation that some remediation work would need to be completed. Support was obtained by outlining the vulnerabilities, risks, and impacts. The team communicated continuously with each other on a daily basis through formal meetings and informal emails and discussions. The members had touch points with the customer on a bi-weekly basis. The team communicated with leadership through weekly written status updates and scheduled monthly meetings. Detailed descriptions of challenges and technical fixes to those challenges helped frame the reason why changes were needed. Demonstrations to the Elections personnel after each sprint kept all stakeholders updated. System testing scripts, utilizing a template for consistency, assisted testers in understanding the desired functions or output of a software component. Department of Elections handled communication with any other interested parties, that were not project stakeholders. DTI leadership provided feedback to the project team on a monthly basis and when requested. DTI leadership also provided direction when technical team members could not reach consensus on the best course of action for various cyber security issues and proposed fixes. The Chief Information Officer acted as a liaison with the Elections Commissioner.

The team provided a list of security vulnerabilities to DTI and Elections leadership in November 2017. The list categorized the security vulnerabilities by risk (critical, high, medium and low), specific election processes (election results tabulation, voter registration, counting of absentee ballots, and acceptance of provisional votes), supporting technical discipline (network layer, application layer) and estimated remediation time for each identified vulnerability category. The vulnerabilities were prioritized jointly by Elections and DTI. The team officially began system remediation efforts in May 2018.

The team used an Agile methodology to manage the project. This approach allows teams to work together on a small set of requirements within short timeframes. A few members of the team had formal training and received Agile certification prior to participating on the project and led the team through the Agile process. Agile tools used were bi-weekly feedback on updates to the systems and debriefs to review and implement lessons learned for the next sprint. Strategies for remediation focused on the most critical issues. The team tracked technical fixes, implemented an abbreviated change/release process, and validated updates using a scanning toolset. Many of the team members had training in these tools and onsite training was provided to team members who had not been trained.

They performed the process of grouping needs or issues that are alike, worked on them collectively, tested the system updates, and reviewed the results with Department of Elections, the agency partner. The team continued this cycle until all the enhancements were addressed. This approach was very helpful on the iVote project due to the limited time to implement the security enhancements. It allowed the team to apply small sets of fixes quickly and regularly based upon the current need. The Agile approach allowed for continual enhancement testing with the Department of Elections, which was crucial to ensure that the business functionality of the system was not impacted.

The implementation phase of remediating the security vulnerabilities began in July 2018 with two releases of the iVote application, which is the system used by the voters. Each release contained a prioritized set of security enhancements. Additionally, supporting Election system components, which include the transmission of voting results, building of a new server to house election results with up to date security protocols, and deployment of stricter security controls for system access, was designed by the team. Leadership approval of these additional security controls allowed the team to meet their intended goals for securing the Elections iVote system by August 2018 in time for the September 2018 state primary and the subsequent 2018 general election.

The iVote project was successfully concluded in August 2018. Elections systems continue to be in use and monitored by DTI security systems and personnel in real time to determine if and/or when a malicious attack is attempted. The Elections systems are used not only for federal elections but also for state, local, and school board elections throughout the year.

Significance

New cyber security threats are detected daily; addressing vulnerability to these threats is an ongoing task for all IT professionals. During the Elections evaluation, security vulnerabilities of various levels were discovered and documented. Elections and DTI leadership recognized the importance of implementing new and improved security controls to enhance services delivered to our citizens. By evaluating, purchasing, and implementing security scanning toolsets for applications, the expediency and quality of the evaluation vastly improved.

The primary stakeholders affected by this project were Elections and DTI and, more importantly, every Delaware citizen registered to vote. The benefits include increased security of citizen voter information, successful transmission of election results, modernized and secure software, and enhanced auditing practices. Each of these system improvements leads to less entry points for cyber criminals, better methods to discover attempted attacks, and higher integrity of Delaware's election results.

Impact

The stakeholders measured the enhanced election system against the priority list of enhancements. To date no unauthorized elections system access reports have been registered. Enhanced auditing monitors the system in real time to ensure integrity. The enhanced system is in place for local and school elections until Elections migrates to a new voting system slated for the 2020 elections. While the benefits are ongoing, new cyber vulnerabilities are introduced regularly. As such, Elections' dedicated a security resource and DTI maintain support of the system. This ensures continued monitoring of the system and security patches/updates as required.

Secondary benefits are being realized through the continued use of the Agile methodology on other projects. Additionally, the robust auditing process can be applied to other technology systems. Application level cyber security processes and toolsets were refined for use with other systems and best practices from the project were shared with software developers in other state agencies.

Cyber Security best practices and standards need to be considered by all IT professionals. DTI publishes security standards and provides toolsets that can be used by other organizations to identify risks and remediation. Additionally, a DTI team that performs application security work as one of their functions has developed training which was provided to other State of Delaware developers to realize the benefits of securing code and to sustain cyber security protections through coding best practices and participation in DTI cyber security workshops. The system continues to be monitored through scanning and dedicated technical resource assignment. Measurable quality improvement occurs through updated scans and implementation of change/release processes.

Toolset training was provided to agencies in the State to scan other types of critical code. DTI has identified application security champions in State agencies to train their own staff in Application

Security best practices and to sustain an increased application security posture within the State. Application Code Scanning Toolsets are regularly updated as new cyber vulnerabilities are discovered throughout the world and incorporated into scanning and outreach capabilities within the state. This ensures that Application Security champions within State Agencies stay up to date on vulnerabilities and protect against them as they become known. Delaware Cyber and Application Security Standards are the minimum that should be applied to application coding practices in State agencies; however, agency leadership can change their approach to be more stringent depending on the criticality of their applications and other federal regulatory requirements. The scanning toolsets follow the same principle, where minimum scanning algorithms are applied to application code, but custom algorithms can be added to the minimum algorithm to address unique cyber protections within each agency based on their technology assets, federal requirements and services provided to the public.