VITA Web Application Vulnerability Scanning Program

Cybersecurity

Initiation date: July 2016

Completion date: December 2016

Nomination submitted by:
Nelson P. Moe
Chief Information Officer
Commonwealth of Virginia
Virginia Information Technologies Agency

2017 Commonwealth of Virginia NASCIO Award Submission

Project: Web Application Vulnerability Scanning Services, Virginia Information Technologies Agency (VITA)

Category: Cybersecurity

Executive Summary

Public-facing websites and systems are one of the primary conduits for cyberattacks. What's a state to do when technology such as public-facing websites and systems are an integral part of business across the executive, judicial and legislative branches of government and state institutions of higher education?

Effective July 1, 2016, the Virginia Information Technologies Agency's (VITA) revised its security standard to require scanning of public-facing websites and systems every 90 days. VITA also worked with elected officials to implement legislation mandating and funding scanning as required in VITA's security standard. As a result, the Code of Virginia now requires VITA to perform vulnerability scans on all of the commonwealth's public-facing websites and systems to pinpoint weaknesses that could be exploited by malicious outsiders.

More than 1,400 scans were conducted in the second half of 2016 by VITA's commonwealth security and risk management (CSRM) staff. The results were eye-opening and provided the commonwealth with valuable information. The scans identified and exposed weaknesses in site design, implementation, operation and internal controls. Vulnerabilities were categorized as low-, medium- or high-risk to the commonwealth. Results of the scans showed 33 percent as a medium risk and nearly 10 percent as high risk. The scans resulted in state agencies taking down inactive websites. Pages that had to remain active were quickly remedied, eliminating vulnerabilities and potential openings for attackers. Both actions immediately decreased the commonwealth's threat surface. Results of follow-up scans have been equally impressive.

The web application vulnerability scan service provided by VITA has resulted in a safer web environment in the commonwealth by exposing weaknesses and risks allowing state agencies and institutions of higher education to eliminate potential access to attackers.

Description of Business Problem

In 2016 the Verizon Data Breach Investigation Report (DBIR) determined that more than 40 percent of data breaches it measured were due to compromised web applications. In Virginia, there is a proliferation of websites and systems used to effectively serve citizens, businesses, visitors and others for anytime, anywhere access. The nature of these systems combined with threats such as those identified in the DBIR results in constant exposure to attack attempts and compromises from an unknown number of malicious third parties.

In 2013, VITA began offering web vulnerability testing by its CSRM staff when requested by agencies and institutions. The use of the VITA service for scanning was optional and VITA billed for each website test to recoup costs. While some agencies were able to use the service, a number of them did not have adequate funding to cover all, or often any, of the websites at the agency. Some agencies performed their own scanning, but often those scans were performed by those without the needed expertise or with tools not effective in picking up vulnerabilities. The lack of capabilities was leaving Virginia sites exposed.

Throughout 2016 Virginia received nearly 71 million attack attempts (four per second), blocked more than 679 million spam messages, blocked 61,000 pieces of malware and received almost 200 attack attempts that became cybersecurity incidents. Based on the analysis of all the malicious activity within the commonwealth, VITA came to the same conclusion as Verizon DBIR – Virginia web applications were being targeted for attack by malicious third parties. Leaving public websites and systems vulnerable potentially could put the entire state infrastructure at risk. Additionally, due to sheer number of websites within Virginia, it was clear that the risk to compromise within the commonwealth was significant. The resources required for each agency with web applications to perform vulnerability testing of more than 1,400 public web sites across 63 agencies would be extremely costly. The commonwealth was in a difficult situation of carrying an unacceptable amount of risk without a clear path to mitigate that risk.

Solution

VITA recognized that the ever-increasing threats to public-facing websites and systems would continue to impact the commonwealth's ability to provide services to its citizens, business, visitors and others anytime, anyplace. VITA had to establish a mechanism to address this risk in a fiscally reasonable manner.

Effective July 1, 2016, VITA revised its security standard to require scanning of public-facing websites and systems every 90 days. VITA then worked with elected officials to create legislation implementing and funding a centralized scanning program which meets the requirements in VITA's security standard. As a result, the Code of Virginia now establishes VITA as the primary body to perform vulnerability scans on all of the commonwealth's public-facing websites and systems to pinpoint weaknesses that could be exploited by malicious outsiders.

The VITA web application scanning program established three primary objectives. These objectives included:

- Identifying vulnerabilities
- Providing a risk analysis and explanation of the identified vulnerabilities regarding how they impact the business

- Offering advice regarding remediation of vulnerabilities and possible approaches for updates.

Scanning under the new standard and state code began July 1, 2016, and continued through the end of the calendar year. The initial review of the sites that needed to be scanned returned approximately 1,500 targets that needed testing. After reviewing the contents of the planned targets, CSRM identified an issue before beginning vulnerability testing. The number of testing sites that was exposed was higher than expected. Prior to starting the scan CSRM worked with agencies to identify sites that were used for testing and eliminated some sites that were no longer in use. Agencies then were asked to move public-facing test, user acceptance testing (UAT) and development sites to private networks. Stale entries were identified and agencies decommissioned outdated domain name server (DNS) entries. Just those initial steps reduced the number of websites exposed by approximately 10 percent.

Once the initial reduction was complete the first round of vulnerability testing was started. A total of 1,408 scans were conducted, resulting in 30,614 findings (see Table A below). Ten percent of the scans came back as high vulnerability. One-third of the findings were ranked as a medium vulnerability. The remaining was a combination of low and information items identified by the testing. The scans were conducted quickly and results were delivered within 10 days. Scans with high vulnerability findings that required immediate action were delivered as soon as they were detected.

Table A

First Round Results of Virginia's Web Vulnerability Scan From 1,408 Scans, Number of Findings		
	Number	**Percentage of findings**
High	2,998	9.79
Medium	10,346	33.80
Low	5,317	17.37
Informational only	11,953	39.04
Total	30,614	100

The results of the scan provided a picture of just how vulnerable the commonwealth was to one of the most used attack vectors. CSRM was also able to take information from the results and evaluate the amount of risk they brought to each agency and the enterprise. The resulting risk was documented and provided to the agencies using the commonwealth governance risk and compliance tool. The criticality of the finding gave agencies a method to prioritize their improvements and created a baseline for future scans.

The next round of scans resulted in a significant decrease in the number of findings. Results of the two sets of scans are compared in tables B and C below. The "Change" and "Improvements" columns show resulting successes in reduction of the number of vulnerabilities detected.

Table B

Second Round Scanning Results From 1,467 Scans, Number of Findings					
	Number	**Percentage of findings**	**Findings per scan**	**Number Change**	**Improvement (Reduction of vulnerabilities)**
High	2,676	10.59%	1.82	-322	10.74%
Medium	9,469	37.46%	6.45	-877	8.48%
Low	3,766	14.90%	2.57	-1,551	29.17%
Informational only	9,368	37.06%	6.39	-2,585	21.63%
Total	25,279	100%		-5,335	17.43%

Table C

	Round 1	**Round 2**	**Number Change**	**Improvement (Reduction of Vulnerabilities)**
Scans completed	1,408	1,457	+59	4.19%
High	415	318	-97	23.37%
Medium	519	612	+93	-17.92%
Low	241	200	-41	17.01%
Informational only	233	337	+104	-44.64%

The results of the scans show the effectiveness of the solutions and remediation suggestions offered by VITA CSRM. There were 5,335 fewer vulnerabilities, or a nearly 18 percent reduction after actions were taken following the first scan. Overall scan ratings also saw great improvement. The number of medium rated scans grew due to a combination of added targets and actions that reduced previously classified vulnerabilities to a less severe rating. Even with the slight increase in the medium category a net improvement and reduction of the most critical threats were realized due to the effort.

Significance of Project

The web application vulnerability scanning program protects commonwealth information technology (IT) systems, resources and information assets from compromise, damage and misuse. It provides all state entities with a funded service that otherwise was not affordable by many in the commonwealth and others may not have the IT security knowledge base to implement. It ensures all public-facing websites and services of the commonwealth are equally protected.

This project aligns with several of NASCIO's top 10 strategies, management processes and solutions, including the number one priority of security and risk management. It also supports

those related to consolidation/optimization, cloud services, fiscal management, modernization and enterprise.

Additionally, the vulnerability scanning program aligns with Gov. Terry McAuliffe's goals and key points as chairman of the National Governors Association. Gov. McAuliffe has placed a strong emphasis on cybersecurity during his tenure, and has encouraged all states – not just Virginia – to make concerted efforts to improve cybersecurity. His cybersecurity and upgraded technology goal calls for the state to "enhance current technology" while "protecting all data."

The program satisfies two agency cybersecurity objectives of the CIO: increase the results of the commonwealth IT risk management program and the IT security audit program by the end of FY 2018 and strengthen the cybersecurity framework. It also meets his FY 2017/18 strategy to expand agencies' ability to assess the risk to their IT environments.

Benefits of Project

The two primary benefits of Virginia's web vulnerability scanning program are the efficient use of state resources and the improvement to the cybersecurity posture within the state. This program ensures websites of state entities use the scan results to remediate the identified vulnerabilities. The results of the remediation close off one of the primary methods for data breaches significantly enhancing the security of commonwealth data. Citizens can be assured the commonwealth has taken steps to protect information entrusted to the state when they are interacting online. The program allowed the commonwealth to be efficient with remediation by providing valuable recommendations on how to proactively make changes and updates to heighten cybersecurity and prevent possible attacks.

The project is fiscally sound since the scanning is centrally funded and permits state agencies and institutions to leverage shared resources. Using the 2015 vulnerability scanning service pricing as a basis for how much each agency would need to invest if the agency performed scans themselves (the cost should be approximately equivalent), scans cost $1,850 per URL annually for four quarters worth of scans. If each agency were to scan their websites using their own tools and expertise the 1,408 scans would have cost $2.6 million. The scans instead cost closer to $350,000.

In addition to the financial and cyber security benefits, the web vulnerability scanning program supports strategic initiatives and goals of national CIOs, Virginia's governor, state IT and agencies.

Overall, the web application vulnerability scan service provided by VITA has resulted in a safer web environment in the commonwealth by exposing weaknesses and risks allowing state agencies and institutions of higher education to eliminate potential access to attackers.