Managing Threats and Remediating Risk for State of Vermont Applications

BACKGROUND
State of Vermont encompasses multiple state agencies providing various services to state residents such as administration, human services, agriculture, natural resources, and transportation. They have a complex infrastructure with over 100 servers, one data center, heavy reliance on Infrastructure as a Service (IaaS), over 50 client endpoints, and 10 mission critical enterprise applications. With a heavy reliance on vendors providing and supporting Commercial off the Shelf (COTS) applications, State of Vermont needed to establish rigid penetration testing processes and controls.

CHALLENGE
The primary driver for this project was to provide agency leadership with a concise view of security risks that pose a threat to the agency, along with recommendations for remediation. Leadership at the State of Vermont also required assurances that their technology vendors and partners were securely developing and supporting agency applications as required by their contracts.

One of the largest application development partners for the State of Vermont and multiple other state governments were reluctant to penetration test their application, citing previous lack of value in the effort. As an alternative option, this application partner offered to provide penetration test results from previous years to ease concerns about the level of security within their application. The State of Vermont instead chose to conduct a new independent penetration test given the shifting security landscape and elevated risk posed to the State and its applications that contain sensitive information. This independent testing gave the State of Vermont assurances that state information was being protected and application security controls are sufficient.

APPROACH
The State of Vermont required a security testing solution that was efficient, minimized disruption to the business, comprehensive across vectors, and extended the capabilities of internal IT teams to evaluate technical security controls with application providers.

NuHarbor Security and Core Security were leveraged for their extensive experience with performing technical security penetration testing for large Fortune 500 companies and Federal entities.
In order to minimize business disruption, NuHarbor Security established a security testing process and cadence of communication with the State of Vermont and the application vendor to ensure full transparency of all penetration testing performed. The security testing process ensured that there were no disruptions to active application development, application availability, or to IT support staff.

Core Security provided end-to-end penetration testing services, leveraging an extensive tool set which included Core Impact Pro, open source tools, and technologies developed in CoreLabs. Numerous vulnerabilities were discovered in the application. Core Security was able to demonstrate active exploits and provided instructions and screen shots on how to perform the exploit.

BENEFITS

The results were shared with the application vendor who noted the penetration test performed by Core Security was by far the most comprehensive and valuable test performed in the history of the application because of the fact Core Security took the time to explain how the exploits worked, provided instructions to the vendor on how to perform the exploit, and the complexities involved in each exploit.

NuHarbor Security worked with agency leadership and the application vendor to provide a security architecture advisory and incorporate risk mitigation techniques into the agency security program to prevent these types of security risks from recurring in the future.

“"We know we can trust Core Security to give us visibility into our true security risk. Core has been very successful in helping us reduce our third-party risk by ensuring our technology partners are developing and delivering highly secure solutions.”

Steve Mattera
Vermont Secretary of State, IT Manager