Abstract
Case Study of one large state agency testing all vendor supplied applications to ensure that state data is protected. This study covers the early obstacles that come with testing Commercial off the Shelf (COTS) applications, the successes of comprehensive security testing, value provided to a customer that improved application security for multiple state agencies.
CASE STUDY: COTS APPLICATION PENETRATION TEST

CLIENT PROFILE

- State Government Agency providing services for state residents.
- Over 50 servers, 1 data center, heavy reliance on Infrastructure as a Service (IaaS), over 200 client endpoints, 10 mission critical enterprise applications.
- Heavy reliance on Vendors providing and supporting Commercial off the Shelf (COTS) applications in order to deliver on Agency strategy.

KEY CHALLENGES

The primary driver for the project was to provide agency leadership with a list of security risks that pose a threat to the agency and recommendations to remediate security risk. Agency leadership was also looking for assurances that their technology vendors and partners were securely developing and supporting agency applications as required by their contracts.

The key business challenges:

- Application development, maintenance, patching performed in black-box methodology.
- Vendors had submitted their applications for technical security testing in previous years through work with other state agencies and security firms.
- One of the largest application development partners providing a major application to this agency and multiple other state governments was apathetic to the idea of technical security penetration testing citing previous lack of value in the effort.
- State agency leadership has limited engagement from this application development partner because the partner feels their practices are adequate and maintains a list of high profile state clients whom have not expressed security concerns.
- The application provider offers to provide any one of the nine previous penetration tests provided by other security firms to justify not doing another penetration test.

Since this application contained sensitive information the immediate goal from Agency Leadership was to obtain assurance that state information was being protected and application security controls are sufficient.
SOLUTION

The state agency required a security testing solution that was efficient, minimized disruption to the business of the agency, comprehensive in its coverage, and extended the capabilities of internal IT teams to discuss technical security controls with mission critical application providers.

NuHarbor Security and Core Security were brought onboard to leverage their extensive experience in working with large Fortune 500 companies and Federal entities performing technical security penetration testing and translating results into meaningful operational outcomes that improve the posture of the enterprise security program.

In order to minimize disruption of the mission critical application NuHarbor Security established a security testing process and cadence of communication with agency leadership 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 all technical penetration testing services. Core Security leveraged their extensive tool set which included Core Impact, open source tools, and technologies developed in Core Security Labs in order to perform all penetration testing. The team from Core Security found numerous vulnerabilities in the application and was able to prove to agency leadership and the application vendor that the vulnerabilities were not false-positives by demonstrating active exploits, and providing instructions and screen shots on how to perform the exploit.

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 exploit, and the complexities involved in each exploit.

NuHarbor Security worked with agency leadership and the application vendor to provide 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.

OUTCOME

- The vendor became very responsive when they realized they had an elevated risk profile and were very cooperative with agency leadership.
- The vendor performed many application architecture enhancements to improve security of the application.
- The application was patched and configuration changes were made to mitigate the risk for this State Agency as well as all other State Agencies where the application was installed.
- The application vendor had a more favorable view toward security in the application once they learned and understood the breadth or security risk that existed in the application.