SOLUTION SUMMARY

CUSTOMER TYPE | State government

CHALLENGE | Enable government agencies to secure information assets given limited budgets and overextended IT resources.

SOLUTION | CORE IMPACT, the first comprehensive penetration testing solution for assessing specific information security threats to an organization.

THE COMPANY

South Carolina Division of the State Chief Information Officer (CIO)
State Government

The South Carolina Division of the State Chief Information Officer (CIO) assists government agencies in using information technology to protect information about the State and its citizens. Through its "Secure South Carolina" initiative, the Division partners with the South Carolina Joint Terrorism Task Force, the Federal Bureau of Investigation (FBI) and the United States Secret Service to educate state, county and local government agencies about the critical need to secure their cyber infrastructure.

As information security (IS) manager, Walker Johnson conducts risk assessments, incident response and forensic analysis of electronic threats to government information systems. Through proactive risk assessment services, he and the security team of IS professionals engage with government agencies to help them protect against cyber terrorism and to prevent identity theft.

> "I knew that penetration testing could provide the conclusive data that the State would need to focus its IT security efforts."

THE CHALLENGE

Traditionally, the security team would conduct risk assessments based on vulnerability scans of their clients' networks. While the scans provided a general indication of an organization's security posture, they detailed all possible vulnerabilities and would yield a staggering amount of data. "When we ran a scan, we'd often receive lists of hundreds of vulnerabilities, without any idea if they were exploitable or not," said Johnson. "We quickly learned that, given budget and staffing constraints, most government agencies couldn't afford to methodically address long lists of potential vulnerabilities," he added.

Without being able to delineate which vulnerabilities posed tangible threats, the agencies often didn't know how to begin addressing their security problems. While the security team had knowledge and skills that could help, they simply didn't have the bandwidth necessary to provide widespread remediation services. Left to address nebulous lists of vulnerabilities, IT departments would often sideline security initiatives in favor of other obligations - leaving their information assets at risk.

THE SOLUTION

When the security team received grant money from the U.S. Department of Homeland Security, he immediately knew where it would best be spent. "I knew that penetration testing could provide the conclusive data that the State would need to focus its IT security efforts," Johnson said.

The security team had options when evaluating penetration testing solutions. He first considered offering manual testing services, since his team had some penetration testing experience. However, each manual testing engagement could take days and would rely on a combination of possibly suspect, publicly available exploits and custom-developed exploits. He also realized that his team would have to create and maintain their own exploit database - something that they didn't have the time or resources to do.

After conducting extensive research, CORE IMPACT was selected for its comprehensive, automated penetration testing capabilities. "We liked that IMPACT offered up-to-date, professionally developed and thoroughly tested exploits. It also appeared to eliminate a lot of manual tasks from the testing process," Johnson said.

By safely exploiting vulnerabilities in network infrastructure, CORE IMPACT allows the security team to identify real, tangible risks to the State's information assets while testing the effectiveness of its existing security investments. In addition, the product's industry-first Rapid Penetration Test (RPT) capabilities would automate the testing process, enabling them to efficiently serve the needs of government agencies throughout the State.

> "We successfully exposed machines that were thought to be protected by perimeter defenses and accessible only through the internal network."

THE RESULT

Pinpointing Real-World Threats

CORE IMPACT allows Johnson's team to efficiently locate and safely exploit real security vulnerabilities. During one his first risk assessments using IMPACT, Johnson used the product's automated testing process to access every system in a county government. "We successfully exposed machines that were thought to be protected by perimeter defenses and accessible only through the internal network," Johnson said. Using IMPACT's pivoting capability, he demonstrated how an exploit could first gain access to a computer with web access – in this case, a domain controller – and then leverage it to attack other machines on the network. County IT staff were able to address the vulnerability on the spot, without wasting time and resources.

Complementing Vulnerability Scans

When government agencies relied solely on vulnerability scans, critical issues would go unnoticed among extensive lists of "potential" vulnerabilities. Penetration testing with CORE IMPACT effectively complements scanners by identifying which vulnerabilities are real, while determining if and how they can be exploited. Johnson noted that scanners still play a role in his team's risk assessments: "We now use scanners as broad-brush tools for determining which agencies might merit a closer look. This allows us to focus our penetration testing services where and when they are needed most."

Preparing for Security Audits

Johnson also uses IMPACT to equip government agencies with the information they need to comply with security mandates from the federal government. For instance, in an initiative to prevent identity theft and other cybercrimes, the FBI regularly audits the information security of state law enforcement agencies. With CORE IMPACT, the agencies can regularly and consistently obtain information about specific security weaknesses. As a result, they are not only well prepared for audits, but also achieve the ultimate goal of staying a step ahead of attackers and other cybercriminals.

Gaining Clear Evidence of Exploitable Vulnerabilities

Johnson noted that there is no substitute for hard evidence when it comes to getting his clients to focus on security. "With CORE IMPACT, we don't have to rely on 'smoke and mirrors' to convince IT staff of the existence of security threats." IMPACT provides each agency with clear, informative reports that provide data about the targeted network and hosts, audits of all exploits performed, and details about proven vulnerabilities. "We now provide our clients with facts about exploitable vulnerabilities and their associated risks," he added.

South Carolina's government agencies can now decisively locate and remediate security weaknesses, protecting information about the government and its citizens. Summarizing his newfound ability to pinpoint and validate the existence of specific vulnerabilities, Johnson stated, "The bottom line is, there's no substitute for proof."