Case Study

CORE SECURITY
A HelpSystems Company

LARGE MIDWESTERN UNIVERSITY

Core Impact

Background

Based in the Midwest and spread across several other campus locations, this university is a large, geographically distributed higher-education institution with over 20,000 full-time undergraduate and graduate students, along with several thousand full-time employees, including administrators, professors, researchers and operational staffers.

Chartered in 1869, the school offers a broad range of undergraduate degrees across the fields of business, engineering, liberal arts and sciences, along with many other collegiate pursuits including government internships and competitive athletics programs.

Overview

Core Impact helped this large Midwestern University:

+ Improve security holistically
+ Find client side vulnerabilities
+ Test web applications
+ Ease PCI compliance

The IT Security Officer & Security Engineer at the institution is responsible for maintaining the University's on-site network security, along with that of its many school-owned endpoints and Web applications. In addition to working vigilantly to ensure that the University's IT assets are protected and running optimally on a daily basis, the IT Security Officer is also responsible for helping the university to prepare for its regular security audits, including those that must be performed to remain in compliance with the Payment Card Industry (PCI) Data Security Standard (DSS).

The Challenge

As with most institutions of higher education, this university is constantly faced with the challenge of attempting to secure its network and IT assets while still allowing for the most open use of those systems to foster a dynamic, unencumbered learning environment for its students and researchers. The school's security concerns are further intensified by the huge volume of mobile devices – primarily laptop computers – which it must accommodate on an ongoing basis without having direct control over the security of those individual assets.

In addition to its primary security concerns in terms of keeping its IT environment malware free and performing at acceptable speeds, the school must also work to ensure that its sizeable volumes of electronic data are protected from potential theft or exposure. The institution must also comply with requirements of PCI DSS as it processes a range of different payment card transactions.

Based on those needs, the university sought a solution that could be used in cooperation with its vulnerability scanning technologies to help validate security holes in its servers, desktops and web applications to prioritize IT risks and guide remediation efforts.

"In a diverse higher education environment with a lot of new students, faculty and staff arriving on a regular basis, ensuring that systems are secure can be challenging. PCI compliance concerns are also on the table; vulnerability assessments, while useful, don't go far enough, and are plagued with false positives," said the IT Security Officer.

The Solution

To help address its multifaceted security and compliance demands, and complement its ongoing vulnerability scanning efforts, the school decided to bring onboard Core Impact to perform ongoing and scheduled penetration tests across many of its electronic assets. By using penetration testing to validate the findings of its vulnerability scanners and help prioritize its remediation efforts, the university is now able to address its most critical risks faster.

While the University had engaged in manual penetration tests prior to licensing Core Impact, adding the product's automated assessment capabilities to its set of vulnerability management solutions has provided the school with the ability to run far more tests in a shorter timeframe.

"Core Impact's Rapid Penetration Test functionality is a huge time saver," the IT Security Officer said. "While we could test all those systems manually, Core Impact has greatly reduced the amount of time required, which allows us to assess more systems than was previously possible."

Among the many different types of penetration tests run by the university, administrators are also planning to take further advantage of the solutions' ability to run advanced client-side exploits to help identify and eliminate vulnerabilities in popular desktop client applications, and to better understand the manner in which multiple flaws may be assailed by cybercriminals. In addition, the University is using the product to actively assess the security of its many Web applications by proactively hunting for vulnerabilities that could allow for subsequent attacks including SQL injection.

> "Proving the presence of a security hole through penetration testing demonstrates the problem in the most direct way possible and Core Impact has been very useful to the university in providing us with the means to more quickly and reliably validate vulnerabilities across our systems and applications."

The Result

Improving Security Holistically

Based on the broad, open nature of its network and the need to accommodate so many mobile computing devices, the school was looking for a solution that would allow it to manage risk by directly identifying and addressing its most critical vulnerabilities, rather than putting up additional perimeter defenses which could constrict access and performance, and still fail to prevent many attacks.

Finding Client Side Vulnerablilities

With such a wide range of applications being used on its computers, coming from so many different sources, it's a significant challenge for the institution to stay on top of all the applicable vulnerabilities and security patches generated by those technologies. As a result, the university is moving to use automated penetration testing to isolate potential problems via client-side testing to identify exploitable vulnerabilities that may leave end users open to ongoing malware attacks and prioritize remediation of those most sensitive weak points first.

"When it comes to client-side penetration testing, Core Security demonstrates progressive vision by providing a huge number of exploits for common client software and a rich post-exploitation framework," said the IT Security Officer. "Anyone who pays any attention to malware attack trends knows that client-side vulnerabilities are frequently used by cyber-criminals to install malicious crime-ware such as the Zeus/Zbot, Torpig, Clampi threats and many others."