Community College Seeks Out Vulnerabilities through Penetration Testing

Managing and protecting the personal information of more than 9,000 students is no small task – Bucks County Community College knew they faced cyber security chall enges, but where do you start?

Bucks County Community College, a public two-year education institution in Pennsylvania, must maintain a secure environment for sensitive information. With more than 9,000 students attending classes at Bucks County Community College, it's not an option to allow anyone's personal and financial information to be vulnerable to an attack. Because some parts of the network were running outdated operating systems and web applications, Bucks County Community College knew there could be vulnerabilities.

Using recommendations from a financial auditor, Bucks County Community College set out to find a partner that could use best practices and experience to seek out security weaknesses.

What was the best way to approach this challenge?

- Conduct external penetration test to identify vulnerabilities.
- Provide findings and recommendations for remediation.
- Perform knowledge transfer with client security team.

PROJECT OVERVIEW

Organization Size:
Serves more than 9,000 students

Organization Industry:
Education; a public two-year college

Challenge:
Complete a penetration test to find vulnerabilities within the internal, external and web application environments.

IMPACT

- Identified possible vulnerabilities
- Remediated issues
- Achieved knowledge transfer between consultants and client team

"As an educational institution, we face certain unique challenges that are different from other organizations. We have thousands of students and hundreds of teachers who all need the ability to access online materials and web applications that could unfortunately open the college up to vulnerabilities such as phishing attacks or malware.

Optiv understood these challenges and worked with us to meet our needs and address our concerns. We had such a successful engagement, we plan to use Optiv for our next yearly pen test."

– Doug Burak, IT security officer, Bucks County Community College Community College.

PENETRATION TESTING:

A View into Information Security Posture

Optiv's external penetration testing services provide clients with a thorough view in to their current information security posture, including the level of protection around its most important assets.

Goals

To start the project, Optiv's consultants worked with the client to understand the engagement goals and objectives. These goals included:

- Perform asset testing using various techniques.
- Provide findings, analysis and recommendations for remediating identified issues.

Kickoff

During the kick-off call, Optiv gathered more information about the environment and identified possible obstacles.

Remote Testing

Starting with the external network, Optiv consultants conducted discovery and vulnerability testing and tested the externally visible devices for vulnerabilities.

Seeking Vulnerabilities

Next, the consultants looked for security issues within the internal network, including testing server-based, workstation and network devices for weaknesses.

Penetration Testing

Finally, acting as an outside hacker, Optiv attempted to exploit the underlying infrastructure to find vulnerabilities.

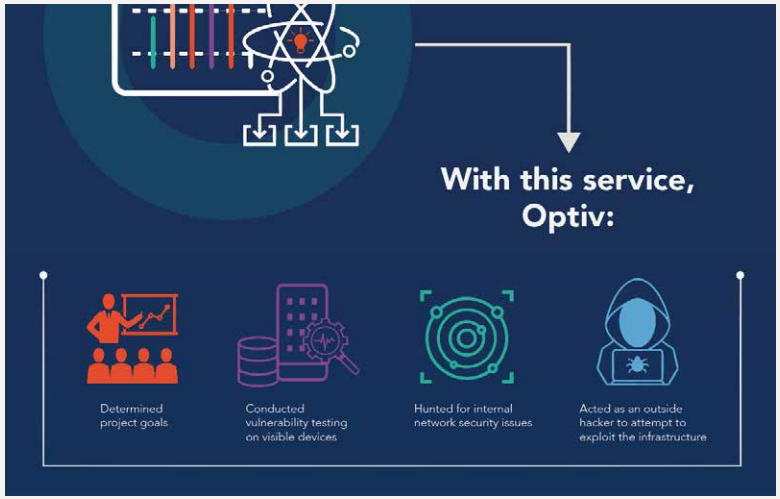
A Secure Environment and a Strategy for the Future

Through the various testing, Optiv assigned a technical severity score to the environment and detailed the criticality of identified issues.

- Optiv delived an executive summary, which included:
  - › The new severity score.
  - › Information on each deficiency in the environment.
  - › Analysis and examples of negative impacts that could occur if the issues are not remediated.
  - › Recommendations for short- and long-term goals and strategies to achieve those objectives.

IMPACT:

- Optiv's work provided valuable information about previously unknown security issues.
- The college remediated vulnerabilities and created a more secure environment for sensitive information.
- Client met internal requirements with a properly protected and up to date environment.



View the Client Spotlight Infographic at www.optiv.com/resources/library

OPTIV

Optiv is the largest holistic pure-play cyber security solutions provider in North America. The company's diverse and talented employees are committed to helping businesses, governments and educational institutions plan, build and run successful security programs through the right combination of products, services and solutions related to security program strategy, enterprise risk and consulting, threat and vulnerability management, enterprise incident management, security architecture and implementation, training, identity and access management, and managed security. Created in 2015 as a result of the Accuvant and FishNet Security merger, Optiv is a Blackstone (NYSE: BX) portfolio company that has served more than 12,000 clients of various sizes across multiple industries, offers an extensive geographic footprint, and has premium partnerships with more than 300 of the leading security product manufacturers. For more information, please visit www.optiv.com.

1125 17th Street, Suite 1700 | Denver, CO 80202 | 800.574.0896 | www.optiv.com

2.16 F1