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. Any kind of breach would be damaging to the college’s reputation, as well as the trust between the students and their school. Because some parts of the network were running outdated operating systems and web applications, Bucks County Community College knew there could be vulnerabilities. A financial auditor recommended the college complete a yearly external penetration test to find possible issues. By examining its most critical assets, such as the departments that handle financial aid and class registration, the school could find and remediate security weaknesses.

Taking the advice of their financial auditor, Bucks County Community College made plans to complete a penetration test to continue to maintain a secure environment. For this task they needed the help of a trusted partner. Because yearly testing is so vital to the school’s security, it needed a group of consultants with extensive field experience and knowledge of best practices.

After creating a request for proposal, Bucks County Community College found that Accuvant, above all other competitors, provided the best value and a team of consultants who were both easy to get along with and knowledgeable.

Accuvant’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. To start the project, Accuvant’s consultants worked with the Bucks County Community College IT team to understand the engagement goals and objectives. These goals included performing asset testing against a single network using software-based and manual testing techniques, as well as providing documentation with findings, analysis and recommendations for remediation of identified issues. The engagement included a kick-off call and a remote testing phase, as well as various deliverables along the way such as status reports, a technical findings document and a vulnerability tracking spreadsheet.

During the kick-off call, Accuvant’s consultants introduced themselves and learned more about the Bucks County Community College security team. Accuvant also used this time to gather more detailed information about the client’s environment, as well as confirm the scope of work to identify possible obstacles for completing the engagement.

Next, Accuvant began the remote network testing phase. Starting with the external network, Accuvant consultants conducted discovery and vulnerability testing of the agreed upon externally visible devices and tested them for network and service-level vulnerabilities. After completing testing on the external network, the consultants moved on to look for security issues within the internal network. This included testing server-based, workstation and network devices for weaknesses using vulnerability scanners. The consultants also tested Bucks County Community College’s web applications for flaws in the coding. Then, acting as an outside hacker, they attempted to exploit the underlying infrastructure. Throughout the project, Accuvant consultants delivered regular status reports so the Bucks County Community College team was always aware of activities and progress.
BUSINESS IMPACT

After all testing was complete, Accuvant’s team met with Bucks County Community College to discuss the findings. Through the testing, Accuvant assigned a technical severity score to the environment and detailed the criticality of issues that they identified. Accuvant provided Bucks County Community College with an executive summary that detailed this severity score, along with each deficiency in the environment, analysis and examples of negative impacts that could occur if the issues are not remediated. The executive summary also delivered recommendations for short- and long-term goals and strategies to achieve those objectives.

Accuvant’s work gave Bucks County Community College valuable information relating to previously unknown security issues. The college remediated the identified vulnerabilities and created a more secure environment for its users’ sensitive information. In addition, Bucks County Community College was also able to meet internal requirements, allowing for peace of mind in knowing its environment is properly protected and up to date.

“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. Accuvant 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 Accuvant for our next yearly pen test.”

- Doug Burak, IT security officer, Bucks County Community

SOLUTION OVERVIEW

Organization Size: Serves more than 9,000 students

Organization Industry: Education

Organization Profile: A public two-year college offering nearly 80 educational programs for associates degrees and certificates.

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

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