Nonprofit Organization Finds Value in Enterprise Penetration Testing Service

Staying proactive with a security plan for the future is important, but where do you start?

A nonprofit organization that has been in business for more than 20 years must protect client information and be proactive about security. To meet this need, the organization created an internal company requirement that included an annual internal audit to ensure that their systems are up to date and efficient.

During a period of rapid growth and expansion, the company revisited some of its security processes, including the internal audit. It found that the audit was not providing the value and insight needed in order to be aware of vulnerabilities and possible breaches.

What was the best way to approach this challenge?

- Provide a security assessment to examine process and identify vulnerabilities.
- Conduct vulnerability and penetration testing of the internal and external network.
- Perform targeted physical and social engineering.

PROJECT OVERVIEW

Organization Size:
Less than 2,000 employeess

Organization Industry:
A nonprofit organization

Challenge:
To improve their current internal audit processes and identify ways to advance security controls and address vulnerabilities.

IMPACT

- Increased value of future annual internal audits
- Addressed key vulnerabilities
- Received recommendations for remediating issues
- Assessment helped organization create their future security strategy

SECURITY ASSESSMENT SERVICES:

Updating Process and Protecting Assets

Planning

To start, Optiv met with the client team to discuss goals, current challenges and project timeline.

Remote Testing

Next, Optiv conducted a remote network testing phase to identify assets, listening services and applications within the perimeter network. With this information, the consultants used vulnerability scanning and testing procedures to identify flaws in defenses.

Deploying Attack Methodologies

After that, Optiv employed many different attack methodologies and exploitation attempts to try and circumvent current protections. This allowed consultants to catalogue the possible ways in which potential attackers could breach the network.

Physical and Social Engineering

Optiv worked onsite to try to get around physical controls at the facility to test its security. They also used phishing attempts to test the environment's user response to malicious emails.

Analysis

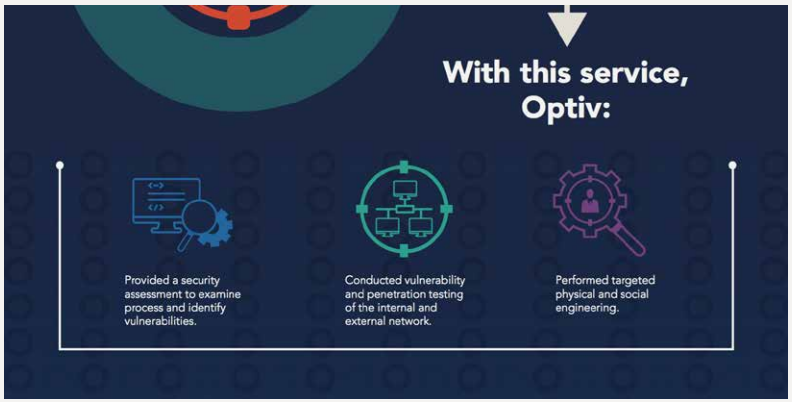
Once testing was complete, Optiv provided technical findings and an executive summary with observations and severity level ratings for each part of the assessment.

Creating a Security Strategy for the Future

Using best practices developed from years of experience in many unique environments, Optiv helped this client identify areas of weakness and make sense of the findings.

Not only did this assessment shed light on critical vulnerabilities and how to address them, but it also helped the organization create its security strategy for the next year and beyond. As a result of the project, this client:

- Received specific, actionable recommendations to address issues before they became huge problems.
- Improved its internal audit to provide more robust and actionable data in the future.
- Obtained an executive summary that listed what controls were working, and which were not.
- Gathered valuable information to share across all levels of management on the state of the security program.



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