Carlson Wagonlit Travel

Carlson Wagonlit Travel Implements Comprehensive Vulnerability Management

NetSPI Helps Bridge the Gap Between Internet Security and Application Development Operations and Provides an Ongoing Process for Hardening Online Applications

As a global provider of business travel and travel management services with a presence in over 150 countries and territories, Carlson Wagonlit Travel (CWT) depends on a strong Internet presence. The company recognizes the challenges inherent in doing business on the Internet and the importance of maintaining the security of applications it develops to support online operations.

Confronting Online Threats

"We had detailed security requirements in place," says Interim Chief Information Security Officer Dané Smiley of Carlson Wagonlit Travel, "but, over time, we realized that they were largely 'visionary.' Our defined requirements were detailed—sometimes too detailed—and not really specific enough to be useful to our developers. We needed a solution that would allow us to keep moving forward with development while reconsidering our goals and redesigning our development process to reduce vulnerability to online threats. We turned to NetSPI. We've worked with them in the past and knew we could count on them for a speedy, thorough solution."

CASE STUDY AT A GLANCE

Client

Carlson Wagonlit Travel is a global leader in business travel management services to one-third of the Fortune Global 100 as well as government and non-governmental organizations. The company helps optimize travel programs, provides a range of services to travelers, and delivers meeting and event management services.

Challenge

The company needed to implement a system for testing existing applications, defining security needs for in-house application developers, and communicating those needs in clear, specific, actionable form.

Solution

NetSPI worked with security staff and developers to identify gaps, implement testing tools and processes, and institutionalize procedures for ongoing communication between security and development groups.

Results

CWT started seeing change within days. General statements of goals were converted to specific requirements, enabling developers to code more effectively. CWT has been able to clearly identify areas of vulnerability, prioritize remediation steps, implement fixes, and track the progress of the entire process.

VMPD Defined

"Vulnerability management program development (VMPD) is a process for building or enhancing a comprehensive threat response methodology," says NetSPI Security Team Lead Ryan Wakeham. "Partial or piecemeal solutions don't provide the kind of protection you need. Real security doesn't leave gaps that can be exploited. And it has to be an ongoing process because threats keep evolving and threat avoidance has to evolve as well. VMPD is really a cycle that begins with planning—defining what your policies and standards will be—followed by assessment, which includes selection of tools and actual testing. You can then analyze, prioritize and report your findings and remediate the vulnerabilities you've identified to complete the cycle. Of course each organization has its own needs, and our goal is to work with clients to identify those aspects of program development we can support and help them develop a customized program they can use on an ongoing basis."

"We wanted a process we could use to test applications in-house," says Dané Smiley. "The developers working on our applications weren't always able to find the actionable information they needed in our existing security documentation, and once the applications were written we had no broad-based, fundamental program for vulnerability testing. Of course we value the security of all our operations, but our immediate concern was Internet-facing applications. We wanted to make our development process more efficient, to beef up perimeter security, and to make sure that secure elements are embedded in our code.

"We didn't have a team dedicated to testing, and when we did identify problems, we had no established process for validating findings and definitively fixing problems to prevent future occurrences. Some of our applications were better than others, but we are committed to having a strong Internet presence, so we knew we needed a thorough, consistent approach that we could apply across the board."

> ***"Partial or piecemeal solutions don't provide the kind of protection you need. Real security doesn't leave gaps that can be exploited. And it has to be an ongoing process because threats keep evolving and threat avoidance has to evolve as well."***
>
> Ryan Wakeham
> Security Team Lead, NetSPI

Implementation

"Working with NetSPI CTO Seth Peter and NetSPI Security Consultant Anna McDonough, we began by identifying gaps in our process. The NetSPI folks were incredibly creative; any skepticism we might have had evaporated when we saw how quickly deliverables started appearing. They understood our developers' concerns and started working on revisions of our security requirements, translating general statements into actionable specifics. As we began actual testing and identifying potential security problems we got lots of useful feedback we could use in reworking the applications, and the process was incorporated into documentation we could use on our own and procedures like the ones Anna wrote for our WebInspect software testing tool. We started seeing change and value literally within days.

"At the same time, Anna was training our people and helping us internalize the whole process. NetSPI's work product helped bridge the gap between Internet security and application development groups. They provided pointers on communication and helped us internalize the whole process so we could keep it up on our own. And after the process was handed over to us they stayed available to provide support when we needed it."

The Bottom Line

"While there's still a lot to be done we've seen big changes already," says Smiley. "As a direct result of our work with NetSPI we are able to identify the level of vulnerability of our applications. We can score and prioritize our remediation plan. We have month-by-month reports on our progress, and we are able to prove out the states of our various applications. We know the number vulnerabilities found and can state with some certainty when they'll be fixed. We're very pleased with the progress we've made, and we've loved working with NetSPI."

> ***"NetSPI's work product helped bridge the gap between Internet security and application development groups. They provided pointers on communication and helped us internalize the whole process so we could keep it up on our own. And after the process was handed over to us they stayed available to provide support when we needed it."***
>
> DANÉ SMILEY
> INTERIM CHIEF INFORMATION
> SECURITY OFFICER

A Better Approach to Risk, Compliance, and Security Consulting

NetSPI provides a range of assessment and advisory services designed to analyze and mitigate risks and ensure compliance with relevant regulations and industry standards. By using its consulting team's deep security knowledge and its CorrelatedVM vulnerability management and reporting solution, the company has become a trusted advisor to large enterprises. Clients include large financial services firms, retailers, healthcare organizations and technology companies.

netSPI
RISK COMPLIANCE SECURITY