



Topics: Application Security, Software QA

Case Study: Software Security Fortification Services Provided to Leading Retail Organization

Overview

SiegeWorks is a leading global enterprise security services, consulting and integration firm, serving as clients' critical first line of defense. A comprehensive portfolio of Digital Defense Services (SiegeWorks DDS™) and technology solutions is available, from digital risk assessment and management, to business continuity assurance services. SiegeWorks solutions enable proactive business and revenue protection and unconstrained information exchange.

The Issues

Today's IT security landscape is treacherous. Staying one step ahead of computer hackers, crackers, viruses, worms, Trojans and spyware that threaten the security of software applications is a daunting task. This is especially true given the growing number of attacks on well-known software program vulnerabilities. To make matters worse, using offshore software developers is a rising trend, and this practice makes it extremely difficult to detect hidden malware and "back door" programs, in addition to software defects that expose applications to a wide range of exploits. Companies must protect themselves against the many lurking threats. As leading firms make headlines for failing to ensure the security of their software, application fortification issues have come to the forefront.

The Situation

A West Coast retail company needed to roll out a new ERP package that would incorporate strong security measures, preventing internal and external security breaches. They needed to protect critical business transactions and processes, confidential data stores, inventory tracking and fulfillment and other backend systems. They also wanted to assure that the supply chain management application could not be compromised and their suppliers would not be able access one another's information.

The Challenge

This ERP initiative was one of the largest, most complex and costly projects that the company had ever undertaken; it would affect every area of the business. Due to the scope of such a project, team members from all key business groups were assigned roles and responsibilities with the intent of ensuring the best possible functionality; some had data entry work, others were in charge of integrating processes, and so forth. The IT security groups were also involved, addressing issues that would affect the organization's firewall, intrusion detection and other systems. What they needed, however, was a partner that would take overall security responsibility; one that had visibility into the complete systems architecture, and expertise in strategically fortifying the areas crucial to core business processes. They also needed a partner that could ensure compliance with corporate policy and privacy laws. They selected SiegeWorks.

The Solution

Drawing upon proprietary methodologies and best practices, SiegeWorks first conducted an in-depth audit and security assessment of the new ERP and existing software. They identified vulnerabilities that were determined to make the business susceptible to threats. They exploited those holes using penetration tests and techniques in order to demonstrate to the client's management team the critical nature of the issues. They issued reports detailing these findings as well, while a separate report was provided to the IT staff, detailing the vulnerabilities found and outlining strategic remediation recommendations. Intensive training and a Secure Coding session provided the staff with the ability to harden their new ERP implementation and mitigate risk to their business, ensuring proactive protection of critical processes, compliance with laws and adherence with corporate policies.

Credentials

SiegeWorks consultants have deep domain expertise in some of the least understood and most complex areas of security—large enterprise applications and databases, and business process security. The firm has demonstrated leadership as a valued and trusted strategic security resource and services implementation provider. Drawing upon experience in thousands of real-world scenarios spanning multiple industries, SiegeWorks has the professionalism and proven track record to provide unrivaled secure software fortification services.

Sidebar:

Working with OEMs

SiegeWorks also works with many of the leading OEMs to build security directly into enterprise applications.

Security is a vital strategic component of building business-critical software and upgrades, and applications today need to be able to meet the barrage of challenges that exist in the "real world" or production environment.

Yet, experts agree that the previous industry approach, called Software QA (SQA), which adds security to applications almost as an afterthought, is not good enough. Adequate security measures need to be implemented in the earliest phases of the production lifecycle: design, review, documentation and development. QA is too late.

Working with both OEM's and directly with clients, SiegeWorks brings greater expertise and a 360-degree view into issue resolution, benefiting all involved.

Contact SiegeWorks today for software security fortification solutions, training and certification programs to meet your company's needs.