SPAN Systems OI Content

Securing Applications: It's More Than a Compliance Issue

2013 was a challenging year for major companies fighting high-profile security breaches. Apple, Twitter, Facebook, Microsoft, Tumblr, Burger King, Jeep, Evernote and The New York Times are just a few of the big-name organizations that had to combat security problems.

- Twitter's systems were compromised and 250,000 user accounts exposed.
- Apple, Facebook and Twitter were victims of a "watering hole attack" causing malware to be downloaded on to the website visitors' computers.
- After suffering a data breach, Evernote had to issue a service-wide password reset.

A security hole in the application can cause not only major financial loss but also loss of customer confidence, trust and reputation, severely impacting the business. Additionally, non-compliance with regulations such as PCI-DSS, HIPAA and Sarbanes-Oxley can lead to hefty penalties.

Here are three best practices to help secure applications and comply with regulatory requirements:

1. **Follow well-established industry guidelines and standards such as OWASP to identify application security holes and prevent breaches.**
   The Open Web Application Security Project (OWASP) is a worldwide, not-for-profit organization focused on helping individuals and organizations worldwide to make informed decisions about true software security risks.

2. **Identify the level of security required for any application with international standards such as OWASP Application Security Verification Standard (ASVS).**
   The primary aim of ASVS is to normalize the range in the coverage and level of rigor required to perform Web application security verification using a commercially workable open standard. The standard provides a basis for testing application technical security controls, as well as any technical security controls in the environment, that are relied on to protect against vulnerabilities such as Cross-Site Scripting (XSS) and SQL injection. The requirements are developed with the following objectives in mind:

   - **Use as a metric**: Provide application developers and application owners with a yardstick to assess the degree of trust that can be placed in their Web applications.
   - **Use as guidance**: Provide guidance to security control developers as to what to build into security controls to satisfy application security requirements.
   - **Use during procurement**: Provide a basis for specifying application security verification requirements in contracts.

3. **Understand that security testing, fixing and monitoring is a continuous process.** It is important and business critical to adhere to critical compliance mandates. Consider security testing that helps you meet the compliance requirements and provides strong security to build trust and confidence. Plan for security tests regularly and frequently; frequent security tests can reduce the cost of failure significantly and give more confidence about security measures of the application.

For more outsourcing best practices, trends, tools and access to free help desk services, visit www.outsourcing.com, or email the Outsourcing Institute at info@outsourcing.com.