CONTROL AND MEASURE THE RISK OF WEB BASED BUSINESS APPLICATIONS

CAN WEB APPLICATION SECURITY TESTING HELP PREVENT DISASTERS?

Recent successful attacks on big corporations like HBGary, Sony and Gawker media have shown that web applications are gradually becoming the preferred entry-point for attackers. Even security minded corporations such as Comodo and Baraccuda Networks proved to be vulnerable to these types of attacks. So what more could you do to protect your assets?

Dave van Stein, test consultant, ps-testware

Nowadays security is more than just protecting your web applications against attacks from malicious outsiders. Contemporary threats with privacy issues and stricter legal requirements demand a higher level of security in terms of integrity, confidentiality and availability in all your applications.

The consequences of a possible exposure can be severe: confidential data loss or theft resulting in confidence issues, companies are unable to communicate online and are suspended as legal requirements are not met or corporate reputations are severely damaged after extensive media coverage of a security breach. In a nutshell, Web Application Security is a business critical issue.

Web Application Security Testing provides the means to identify and remediate vulnerabilities that could expose your business.

MISCONCEPTIONS

Unfortunately though, there are many misconceptions about web application security: Traditional countermeasures like firewalls, server hardening and data encryption are simply not enough to protect your data – and your reputation – against attacks on the application layer. And unfortunately, limiting yourself to intranet applications or commercial applications also only provides a false sense of security.

At the same time, the development of secure web applications is influenced by a number of evolutions: there is a growing pressure to make existing applications available for the internet, even if they were never designed for that purpose. Fast evolving, feature rich technologies also make it harder for developers to

RESEARCH SHOWS

> Half of all breaches are caused by erroneous or malicious user input

> One third of all breaches result in a violation of policies

> One third of all breaches remain unnoticed due to flawed logging management

(Data compiled from various resources including epic.org, perkinscoie.com, cenzic.com, and webappsec.org)

Contemporary threats with privacy issues and stricter legal requirements demand a higher level of security.

gain the necessary experience, resulting in a tradeoff between security and functionality. And finally, the changing compliancy regulations and privacy laws also add to the already demanding task of Security and IT Officers.

BETTER BE SAFE THAN SORRY

This situation leads to the reality that web application security is, often unknowingly, simply not in scope of either operational security or development departments. This realization makes the solution simple enough: Web application security is a development issue and should therefore be part of the design from the start, making Web Application Security Testing an integrated part of the software development lifecycle.

Web Application Security Testing makes it possible to control and measure the risk of web based business applications and provides the means to identify and remediate vulnerabilities that could expose your business.

This approach will help the software development manager with the important challenge of building software that ensures a high availability with complete data integrity and confidentiality. It ensures the early detection of changes in functionality that may provoke vulnerabilities or vice versa.

Web Application Security Testing provides you with full control over the test process, resulting in higher cost efficiency with clear, verifiable and traceable results. After all, when it comes to security, it is better to be safe than sorry.