IT Security Management

Web Application Penetration Testing

Penetration tests usually focus on the examination of IT systems. This means that web-based applications, if they are included in the scope, are usually checked without login credentials and thus only to a very limited extent. Web application penetration tests bridge this gap, as they concentrate on a deeper and more comprehensive investigation of application vulnerabilities. Our testing approach caters for this objective: while our best-practice concept follows the main steps of general penetration tests, it also takes into account application-specific testing aspects. Please refer to the following sections for a detailed description of our service packages:

Service Package 100: Kick-off

Before starting the penetration test, we discuss with you the test objectives and procedure. This meeting covers the following topics:

- Objectives of the penetration test
- Presentation of the procedure and technologies to be used for the analysis
- Test aggressiveness, information about dangerous tests and potential failures
- Designation of contact persons for the test
- Next project steps

This Service Package is an essential step, as thorough preparation, such as a detailed definition of the penetration test objectives, is vital for us to meet your expectations.

Service Package 200: Collecting Information

This “passive phase” serves to analyse the application logic and to gather information about the following topics:

- Infrastructure
- Web environment
- Interactive web applications
- Creation of dynamic content

This analysis is performed manually as well as by means of automated tools.

Service Package 300: External Penetration Test

In this “active phase” we use the information gathered in Service Package 200 to examine the web application for vulnerabilities. In the course of this phase we perform the following checks:

- Login process
- Input validation
- Manipulation of session data
- Manipulation of the authorisation parameters
- Known attacks against web servers and application servers

For the above tests we use the following methods:

- Tests by means of security scanners
- Manual tests using tools and techniques developed in-house

Web application attacks are challenging and require not only experience but also imagination. This is why automated scanners are only suitable to a limited extent. As a result, this Service Package focuses on manual tests. We calculate approximately 2–3 days per application as every page and every input field will be checked for each application.

Customer-Provided Services

- Provision of two normal user accounts

Service Package 400: Creating the Report

Upon test completion, we provide you with a final report. It includes a summary of the results from Service Package 200 and 300 as well as a rating of the identified security risks. In addition, the report describes the security controls to be implemented in the short term as well as more comprehensive actions that may be required in the medium term.

plan42

plan42 is a consulting firm specialised on IT Service Management, IT Security Management & Business Solutions. Process analysis, consulting, conception, and implementation – plan42 combines technical expertise and best-practice concepts of IT Service & Security Management.