IT Security Management

Penetrationstests für Webapplikationen

Die Untersuchung webbasierter Anwendungen ist eine Sonderform des Penetrationstests: Während der Schwerpunkt bei allgemeinen Penetrationstests auf den IT-Systemen liegt und Webapplikationen, wenn vorhanden, meist ohne Zugangsdaten und daher nur eingeschränkt untersucht werden können, liegt der Fokus beim Web Application Testing auf einer tiefgehenden und umfassenden Prüfung der Anwendung. Dies spiegelt sich auch in unserem bewährten Testkonzept wider: Es basiert auf der Vorgehensweise allgemeiner Penetrationstests, trägt jedoch auch dem besonderen Schwerpunkt Rechnung.

Arbeitspaket 100: Kick-off

Vor Beginn des eigentlichen Penetrationstests klären wir mit Ihnen folgende Eckpunkte:

- Ziele des Penetrationstests
- Vorgehensweise und Techniken
- Aggressivität der Tests, Aufklärung über gefährliche Tests und mögliche Ausfälle
- Ansprechpartner für den Test
- Weiterer Projektablauf

Dieses Arbeitspaket ist ein essenzieller Schritt, da eine gründliche Vorbereitung, wie z. B. die genaue Abstimmung der Testziele, für uns eine wesentliche Voraussetzung dafür ist, Ihre Erwartungen zu erfüllen.

Arbeitspaket 200: Informationssammlung

Diese sogenannte „passive Phase“ dient dazu, die Anwendungslogik zu analysieren und Informationen zu folgenden Themen zu sammeln:

- Infrastruktur
- Webumgebung
- Interaktive Webapplikationen
- Generierung von dynamischem Content

Diese Analyse wird sowohl mit automatisierten Tools als auch manuell durchgeführt.

Arbeitspaket 300: Penetrationstest von außen

In dieser sogenannten „aktiven Phase“ werden die Webanwendungen mithilfe der Informationen aus Arbeitspaket 200 auf Schwachstellen untersucht. Dabei führen wir folgende Tests durch:

- Login-Vorgang
- Input-Validierung
- Manipulation der Session-Daten
- Manipulation der Autorisierungsparameter
- Bekannte Angriffe auf Webserver und Application-Server

Diese Tests bestehen aus den beiden folgenden Modulen:

- Automatischer Test mithilfe eines Sicherheitsscanners
- Manuelle Tests mit Software und Techniken aus eigener Entwicklung

Angriffe auf Webapplikationen sind anspruchsvoll und fordern Erfahrung und Phantasie. Aus diesem Grund sind automatische Scanner nur bedingt geeignet. Den Schwerpunkt dieses Arbeitspakets bilden daher manuelle Tests. Pro Applikation kalkulieren wir in etwa 2–3 Tage, da bei jeder Applikation jede einzelne Seite und jedes Eingabefeld überprüft werden.

Beistellleistungen des Kunden

- Bereitstellung zweier normaler Benutzerzugänge

Arbeitspaket 400: Erstellung eines Berichts

Die Ergebnisse der Arbeitspakete 200 und 300 fassen wir zu einem ausführlichen Bericht zusammen, in dem auch das Risiko der Schwachstellen bewertet wird. Zudem gibt der Bericht Auskunft darüber, welche Sofortmaßnahmen eingeleitet werden sollten und welche mittelfristigen Änderungen ggf. nötig sind.

plan42

plan42 ist ein Beratungsunternehmen, das sich auf die Bereiche IT Service Management, IT Security Management & Business Solutions spezialisiert hat. Von der Prozessanalyse über die Beratung und Konzeption bis hin zur Realisierung – plan42 verbindet technische Expertise mit praxisbewährten Konzepten aus den Bereichen IT Service & Security Management.