Webserver /Webseiten Überprüfung

Webseiten sind natürlich frei aus dem Internet erreichbar. Damit sind sie aber auch einem erhöhten Risiko ausgesetzt. Webseiten können so für politische Statements missbraucht werden (Webseiten-Verunstaltung) oder mit Trojanern verseucht werden. Ausserdem dienen die Informationen auf der Webseite für gezielte Angriffe mittels Social Engineering.

Fingerprinting

Im ersten Schritt geht es um generelle Informationen zur Webseite wie Geolocation, Webhoster und dergleichen. Das Aufspüren aller Subdomains und die Zuordnung der IP Adresse sind die Grundlage der weiteren Untersuchungen.

- Domain Identifikation und Informationen dazu (WHOIS, Geolocation)
- DNS Brute Forcing (Identifikation Subdomains)
- NS Lookup (Identifikation IP Adressen)

Google Hacking

Google Suchoperatoren wie site, filetype, inurl, intitle sowie intext.
Bezogen auf die Webseite können damit versteckte Login-Bereiche, Internal Server Errors, DSA private Keys und anderes aufgedeckt werden.

Port und Vulnerability Scanning

Mittels professioneller Software wird der Webserver geprüft:

- Scannen der offenen Ports.
- Schwachstellenanalyse mittels professionellen Vulnerability Scanner.
- Analyse Webserver OS, PHP Version, SQL-Version, Content Management System auf Schwachstellen.
- Anfälligkeit auf SQL Injection und Cross Site Scripting.

Social Engineering

Inhalt der Webseite auf ihr Social Engineering Potential untersuchen. Dabei geht es um die Informationen, die auf der Webseite zu finden sind. Nicht zu verwechseln mit dem Modul Footprinting, dass weitaus aufwendiger ist, da es auch Soziale Netzwerke und ähnliches einbezieht.

Organisation

Nebst einer Präsentation der Resultate wird ein detailliertes Protokoll erstellt und Lösungen zur Beseitigung der Sicherheitsmängel vorgeschlagen.

Preis

CHF 950.00 exkl. MwSt.

Aeussere Bahnhofstr. 30c • CH-8854 Siebnen • T +41 55 440 74 18 • M +41 78 600 68 99
info@hegner-engineering.ch • www.hegner-engineering.ch