Secure your Systems

Security Scan Webseiten / Internetserver

incl. Erstellung automatisierter Securityberichte

Das Angebot umfasst einen zu überprüfenden (Web-)Server welcher aus dem öffentlichen Netz erreichbar ist.

Schritt 1 - Webseitensicherheit (nur Webserver):

Die erste Analyse erfolgt mit dem **Acunetix Security-Analyser** mit folgendem Umfang:

- Javascript Analyser (Ajax und Web 2.0 Anwendungen)
- SQL-Injection zum Test unerlaubter Zugriffe auf Datenbanken
- Cross Site Scripting (XSS) zur Überprüfung interaktiver Applikationen einer Web-Seite
- Port Scanning
- Analyse von Flash-Anwendungen
- Test von Formularen
- Test von Passwort-geschützten Seiten
- Remote File Inclusion (Ausführung externer Scripts bzw. Programme)
- Directory Traversal (unerlaubter Zugriff auf Verzeichnisse und Dateien des Servers)
- Überprüfung von HTTP, HTTPS, FTP, IMAP, SQL-Servern, POP3, SSH, TELNET und anderen DNS Services
- Automatische Erkennung und Versionskontrolle verbreiteter Internet-Anwendungen (incl. einzelner Module und Erweiterungen)
- etc.

Schritt 2 - Schwachstellenanalyse:

Eine weitere Sicherheitsüberprüfung Ihres Serversystems erfolgt mit dem **Nexpose** Schwachstellenscanner mit folgendem Umfang:

- Port-Scanning
- Banner Grabbing
- identifizieren von Sicherheitsbedrohungen wie Schwachstellen, Fehlkonfigurationen und Exploit- und Malware-Exposition
- vollständige Bewertung der gesamten physischen und virtuellen IT-Infrastruktur durch u. a. Netzwerke, Betriebssysteme, Web-Anwendungen und Datenbanken

Der Security-Scanner **Nexpose** untersucht das Zielsystem auf konkrete Angriffsmöglichkeiten. **Nexpose** hat dazu in seiner Datenbank alle bekannten Sicherheitslücken verzeichnet, die das ganze Spektrum von CGI-Lücken bis hin zu spezifischen Windows-Schwachstellen abdecken.

Aufpreispflichtige Option:

Ergänzend kann nach der Durchführung der Security Scans mit einem **Penetrationstest via Metasploit** überprüft werden, ob die gefundenen Schwachstellen für weitere Angriffe nutzbar sind:

- Validierung von identifizierten Bedrohungen, die eine echte Gefahr in Ihrer Umgebung darstellen (via **Metasploit**)

Der ausführende Prüfer (Thomas Floß) hat in Bezug auf die Aufgabenstellung folgende Zertifizierungen/Ausbildungen:

- zertifizierter Datenschutzbeauftragter nach dem Ulmer Modell (udis)
- TÜV geprüfter Datenschutzbeauftragter
- Teletrust Information Security Professional (T.I.S.P)
- geprüfter EDV-Sachverständiger für Systeme und Anwendungen
- Certified Ethical Hacker (CEH)
- TÜV geprüfter Compliance Officer
- IT-Forensiker
- Certified Information Systems Auditor (CISA)