SEC4YOU
Advanced IT-Audit Services

https://sec4you.com

Internet Security Scan / Penetration Test

SEC4YOU ermittelt die potenziellen Angriffspunkte Ihrer Internetanbindung und Webauftritte und erarbeitet konkrete Lösungsvorschläge. **Genießen Sie die Gewissheit, dass Sie für die eigene IT-Sicherheit aktiv wichtige Schritte gesetzt haben.**

Im Rahmen dieser Überprüfung werden die **Internetanbindung** des Unternehmens, sowie die **extern verfügbaren Webauftritte** automatisiert bzw. manuell auf Sicherheitsschwachstellen und potentielle Angriffspunkte untersucht. Dabei versetzt sich der Tester in die Rolle eines Hackers und verwendet dieselben Methoden und Werkzeuge.

Die Tests werden in den Varianten **Blackbox und Whitebox** angeboten. Blackbox bedeutet, dass keine über die zu prüfenden IP-Adressen bzw. Domains hinausgehenden Informationen zur Verfügung gestellt werden. Bei Whitebox werden hingegen vor Beginn der Prüfung entsprechende Informationen über die relevante Infrastruktur zur Verfügung gestellt und es findet eine laufende Abstimmung mit dem Auftraggeber statt. Hierdurch erhöht sich die Effizienz der eingesetzten Mittel und der Detaillierungsgrad der Ergebnisse.

Ein Internet Security Scan bzw. Internet Penetration Test sollte regelmäßig durchgeführt werden, um Schwachstellen und potenzielle Risiken zeitgerecht zu erkennen und beheben zu können und somit die Gefahr einer erfolgreichen Hackerattacke zu minimieren.

Private IP address leaked in HTTP headers
ICMP echo request/reply
Schwache Verschlüsselung bei Web-Server
Anonymous ftp (21/tcp) mit Schreibzugriff
Administration über Telnet (port 23/tcp)
Cross Site Scripting (XSS)
Malicious File Execution
Improper Error Handling
Broken Authentication

https://sec4you.com
office@sec4you.com
+43 1 253 17 97

Kernbestandteile & Ergebnisse

Die Prüfung wird auf Basis des Durchführungskonzeptes für Penetrationstests des Bundesamtes für Sicherheit in der Informationstechnik (BSI) durchgeführt. Dies gewährleistet eine strukturierte und methodische Vorgangsweise mit nachvollziehbaren Ergebnissen.

Phase 1: Vorbereitung
Die zu prüfenden IP-Adressbereiche bzw. Internetdomains und die organisatorischen Rahmenbedingungen, sowie die Wahl des Prüfungsansatzes (White- oder Blackbox) werden definiert.

Phase 2: Informationsbeschaffung
Alle öffentlich verfügbaren Informationen über die zu prüfende Infrastruktur werden ermittelt, wobei bei einem Whitebox-Test zusätzlich die vom Auftraggeber bereit gestellten Informationen berücksichtigt werden. Weiters erfolgen ein Internet Security Scan und ein Web Application Security Scan der autorisierten IP-Adressen und Internetdomains.

Phase 3: Bewertung der Informationen / Risikoanalyse
Hierbei werden eine Analyse und Bewertung der ermittelten Schwachstellen und Risiken durchgeführt, sowie jene Systeme und Anwendungen, bei welchen Angriffspunkte festgestellt wurden, identifiziert. Die Ergebnisse der Phase 3 werden in Form eines technischen Berichts dokumentiert und an den Auftraggeber übermittelt (nicht bei Blackbox).

Phase 4: Aktive Eindringversuche
Auf Basis des technischen Berichts der Phase 3 wird gezielt versucht, die Schwachstellen auszunützen, um unautorisierten Zugriff auf Daten bzw. Systeme zu erhalten.

Phase 5: Abschlussanalyse
Im Rahmen der Abschlussanalyse werden die Ergebnisse der Prüfung hinsichtlich möglicher Risiken (gering, mittel, hoch) bewertet und konkrete Empfehlungen ausgearbeitet, um diese Risiken zu vermindern.

Die Ergebnisse werden in Form eines Prüfberichts, der aus einem Management Summary und aus einer detaillierten technischen Beschreibung besteht, dokumentiert.