Penetrationstest

Sicherheit testen und Schwachstellen erkennen

Um möglichen Gefährdungen entgegenzuwirken und vorzubeugen, sind Maßnahmen zur kontinuierlichen Verbesserung der IT-Sicherheit zu ergreifen. Sicherheit definiert sich durch Sicherheitsorganisation und Eskalationsvorschriften, technische und oranisatorische Maßnahmen, wie Zugriffsschutzmechanismen, Mitarbeitersensibilisierung, Verschlüsselung und Firewallsysteme. Hierbei soll ein bestimmtes Sicherheitsniveau erreicht werden. Diese und weitere Aspekte sollten in einer unternehmensweiten IT-Security Policy bzw. IT-Sicherheitshandbuch zusammengeführt werden.

Haben Sie sich schon-mal gefragt?

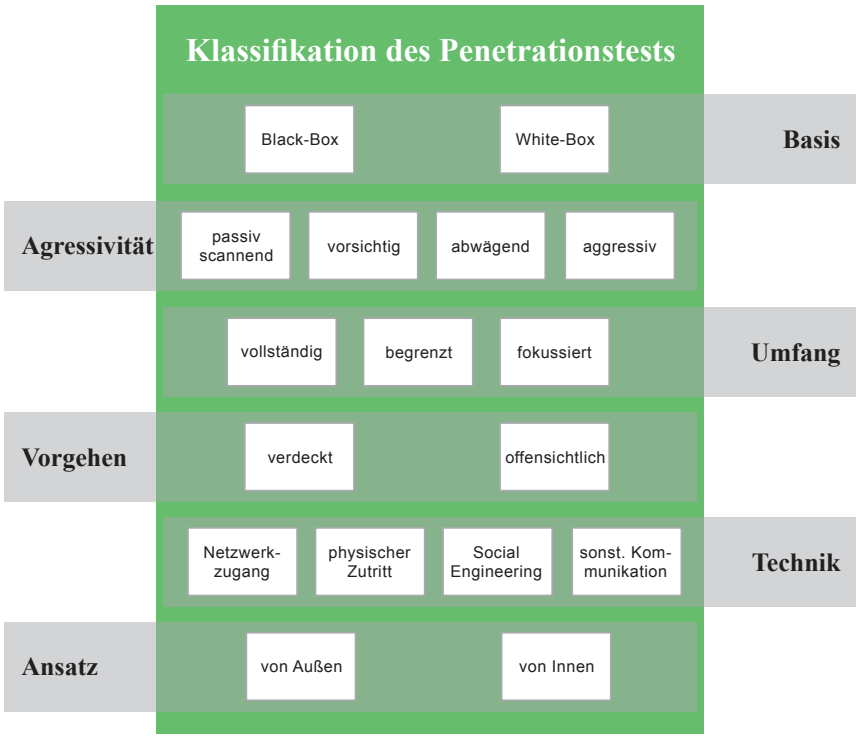
- Wie gut ist unser IT-Sicherheits-konzept tatsächlich?
- Sind unsere IT-Sicherheitsmaß-nahmen auch „State of the Art“?
- Wird unsere IT-Sicherheitspolitik wirklich gelebt?
- Können Externe an unsere Daten kommen? Können diese sogar ge-stohlen oder manipuliert werden?

Ziele eines Penetra-tionstests

- Identifikation von **Schwach-stellen**
- Aufdecken **potenzieller Feh-ler**, die sich aus der (fehler-haften) Bedienung ergeben können
- **Erhöhung der Sicherheit** auf technischer und organisatori-scher Ebene
- **Bestätigung** der IT-Sicherheit durch einen externen Dritten

Können Sie die Fragen positiv beantworten?

Durch die ständige Änderung der Bedrohungsbilder und sicherheitsrelevanten Faktoren in der Informationstechnik ist ein Penetrationstest allerdings eher als Momentaufnahme zu begreifen. Im Extremfall kann ein System unmittelbar nach dem Beheben der durch den Test aufgedeckten Schwachstellen durch eine neue Sicherheitslücke wieder verwundbar sein.



UIMC Dr. Vossbein GmbH & Co KG
Nützenberger Straße 119
42115 Wuppertal
Tel.: (0202) 265 74 - 0
Fax: (0202) 265 74 - 19
E-Mail: consultants@uimc.de
Internet: www.UIMC.de

Penetrationstest

Sicherheit testen und Schwachstellen erkennen

Vorgehensweise und Instrumente

Je nach vertraglicher Vereinbarung bietet die UIMC eine Vielzahl hochkomplexer Prüfungsmethoden:

- Verdeckte und offensichtliche Verifikation von Schwachstellen
- Verifikation tatsächlicher Schwachstellen
- Verdeckter und offensichtlicher Test der Router
- Test von Vertrauensbeziehungen zwischen Systemen
- Verdeckter und offensichtlicher Test der Firewall von außen
- Test des IDS-Systems
- Brute-Force-Attacken
- Abhören und Test von Passwörtern
- Test von „Denial-of-Service“ Anfälligkeit
- Direktes und indirektes Social Engineering mit physischem Zutritt
- Überprüfung der drahtlosen Kommunikation
- Test der administrativen Zugänge zur Telefonanalage, des Voicemailsystems oder der administrativen Zugänge zum Faxsystem
- Aktiver Test der Zutrittskontrollen
- Überprüfung von Eskalationsprozeduren
- Test der vorhandenen VPN-Schnittstellen

Darüber hinaus werden auf Wunsch aggressive Scans durchgeführt; sowohl solche, bei denen es ein Absturzrisiko gibt als auch solche, deren Ziel der Absturz des jeweiligen Systems ist. **In gegenseitiger Absprache** kann in Abhängigkeit der Penetrationstestergebnisse eine **tiefergehende Analyse** durchgeführt werden.

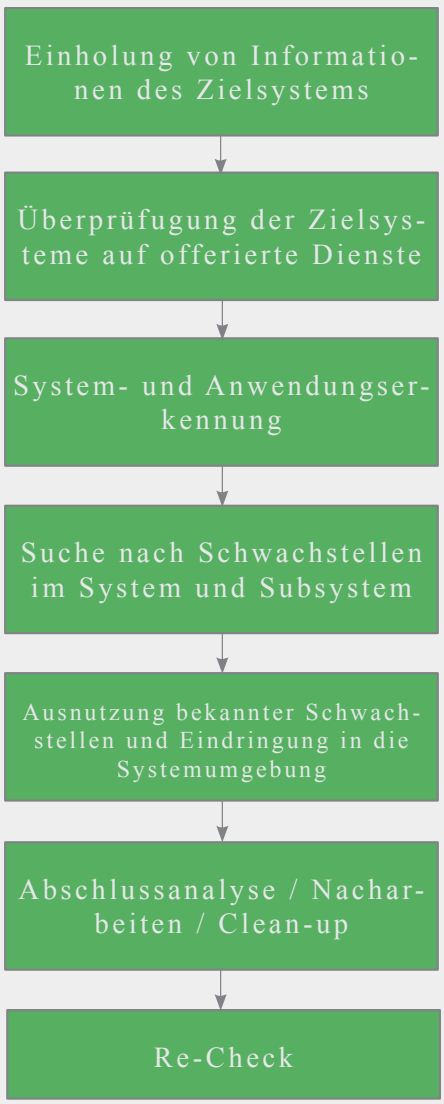
Das Angebot der UIMC

- Systemexperten mit Kenntnissen in den Bereichen Systemadministration, Datenbanken, Netzwerktechniken, Programmiersprachen und IT-Sicherheitsprodukten
- Black-Box- und/oder White-Box-Test
- umfangreiche, eigenentwickelte Testmethoden
- umfassende Dokumentation von Penetrationstest und Ergebnissen
- Einbringung von Know-How aus themenverwandten Projekten, z.B. Aspekte des Datenschutzes, Notfall- und Risikomanagement oder Business-Continuity-Management
- Erstellung eines Maßnahmenkatalogs sowie ein auf auf das Unternehmen angepasstes IT-Sicherheits- und Datenschutzkonzept

Voraussetzungen

Falls kein Sicherheitskonzept bzw. keine Sicherheitsleitlinien erstellt wurden, ist es insbesondere bei komplexen IT-Landschaften fragwürdig, ob ein Penetrationstest sinnvoll ist. Vermutlich wäre es für eine Steigerung der IT-Sicherheit viel effizienter, zunächst ein geeignetes Sicherheitskonzept bzw. IT-Sicherheitshandbuch zu erarbeiten und umzusetzen.

Unsere Vorgehensweise



Weitere Informationen?

Informieren Sie sich über unsere weiteren Kerngebiete

- Datenschutz,
- Informationssicherheit oder
- Notfallmanagement.

Wir haben auch Lösungen, die speziell auf KMU-Bedürfnisse zugeschnitten sind.

www.UIMC.de/Leistungen