



PDF-Druck der Internetseite

Titel der Seite:Datensicherheit

Stand:06.09.2010 08:14

[Home](#)>>[Service](#)>[Datensicherheit](#)

Penetrations-Tests: Sind Sie sicher?

Sind Sie sicher? Penetration-Tests sind eine Möglichkeit, ein Unternehmensnetzwerk auf Schwachstellen und Sicherheitslücken zu testen. Diese Tests werden im Wesentlichen nach den Richtlinien des "Open Source Security Testing Methodology Manual" durchgeführt. Das ermöglicht unseren Kunden eine unabhängige Bewertbarkeit des Testergebnisses. Dabei werden wir versuchen, mit den Methoden eines potenziellen Angreifers in Ihr Netzwerk bzw. Ihre EDV einzudringen.

Sämtliche Testergebnisse werden dabei penibel registriert und anschließend mit Ihnen ausgewertet. Wir besprechen und planen die Vorgehensweise zuvor mit Ihnen ausführlich. Die zuständige EDV-Abteilung bzw. die Verantwortlichen für die Sicherheit im Unternehmen müssen dabei nicht informiert werden, um das entsprechende Risikomanagement unter realistischen Bedingungen zu testen.

Möglichkeiten des Tests sind:

- Externe Tests (von außen nach innen)
- Interne Tests (Interne Schutzmechanismen testen)
- Mit oder ohne Kenntnis der Infrastruktur

Die Grenzen der Tests werden vor Testbeginn deutlich gemacht, um eventuelle Beeinträchtigungen weitgehend auszuschließen.

Einige Testmethoden im Überblick:

- Überprüfung offener Ports
- Überprüfung erreichbarer Dienste
- Überprüfung WLAN-Netze
- Informationssammlung zu Systemcharakteristiken
- Automatische Überprüfung auf Schwachstellen
- Tests auf bekannte Schwachstellen und Sicherheitslücken
- Test der Firewalls
- Überprüfung der Zugriffsberechtigungen
- Passworttests (Schwache Kennwörter, Einsatz von Entschlüsselungsprogrammen)
- Denial of Service - Attacken und Tests
- Manuelle Überprüfungen
- Social Engineering