

Informationen zu Penetrationstests

Penetrationstests auf Basis der Studie des Bundesamts für Sicherheit in der Informationstechnik (BSI)

Penetrationstests sind die erste Wahl, wenn es darum geht, das ordnungsgemäße Funktionieren der IT-Sicherheit zu überprüfen. Diese Art der Schwachstellenanalyse geht dabei vom Blickwinkel des Angreifers aus und bietet somit einen realitätsnahen Sicherheitscheck der IT-Infrastruktur.

Je nach Umfeld und Bedarf des Kunden können Penetrationstests völlig unterschiedlich aufgebaut sein, eine Standardisierung ist daher nur begrenzt möglich. Das Bundesamt für Sicherheit in der Informationstechnik hat dieses Thema in seiner "Studie zur Durchführung von Penetrationstests" aufgegriffen und eine grundlegende Methodik entwickelt. Diese beinhaltet neben einer Unterteilung des Vorgehens in mehrere Phasen die Klassifizierung des Penetrationstests anhand vordefinierter Kriterien.

Die fünf Phasen eines Penetrationstests

1. Vorbereitung
2. Informationsbeschaffung
3. Bewertung
4. Eindringversuche
5. Abschlußanalyse

Durchführung des Penetrationstests

Bei der Vorbereitung eines Penetrationstests werden zunächst Ziele, Umfang, Vorgehen und weitere Eckdaten, wie Notfallmaßnahmen besprochen und festgelegt. Die gründliche Betrachtung von organisatorischen und rechtlichen Aspekten dient dabei der beiderseitigen Absicherung, da die Durchführung eines Penetrationstests ohne vollständige Berücksichtigung der relevanten gesetzlichen Bestimmungen möglicherweise strafrechtliche oder zivilrechtliche Konsequenzen nach sich ziehen kann. Nachdem diese Eckdaten in einem Vertrag schriftlich definiert wurden, kann mit dem ersten Schritt, der Informationsbeschaffung, begonnen werden. Hier werden zunächst passiv Informationen über das Unternehmen, Netze, Systeme sowie mögliche Angriffspunkte gesammelt. Je nach Umfang kann der Zeitbedarf hierfür mehrere Tage bis Wochen betragen. Die gesammelten Informationen werden nun analysiert und bewertet und bilden die Grundlage für die folgenden Eindringversuche. Hier werden die zuvor definierten Ziele aktiv angegriffen, um Schwachstellen zu identifizieren. In dieser Phase sind insbesondere Kreativität und Fachwissen des Penetrationstesters gefordert, da neben fundierten Kenntnissen der grundlegenden Netzwerk- und Systemkomponenten auch langjährige Erfahrung auf den Gebieten Administration und Programmierung notwendig sind. Die Abschlussanalyse beinhaltet neben der vollständigen Dokumentation der einzelnen Prüfungsschritte eine Bewertung der gefundenen Schwachstellen, sowie konkrete Empfehlungen zur Kompensation der daraus resultierenden Risiken.

Klassifizierung von Penetrationstests

Informationsbasis

Blackbox, Whitebox

Aggressivität

Passiv, Vorsichtig, Abwägend, Aggressiv

Umfang

Vollständig, Begrenzt, Fokussiert

Vorgehensweise

Verdeckt, Offensichtlich

Technik

Zugangsart, Social Engineering, Sonstiges

Ausgangspunkt

Von außen, Von innen

Nach Übergabe der Dokumentation an den Kunden wird diese abschließend in einem ausführlichen Gespräch erörtert. Anhand der Ergebnisse und deren Priorisierung kann nun ein Aktionsplan für die Behebung der Schwachstellen erstellt werden.



Secutrends GmbH

Secutrends GmbH
Im Westpark 8
D-35435 Wettenberg

Kontakt

Fon: +49 641 250390 0

Fax: +49 641 250390 100

E-Mail: sales@secutrends.com

Web: www.secutrends.com