ABLAUF PENETRATION TEST

Allgemeines

Grundsätzlich folgen die Penetration Tests by COMBACK einem klar gegliederten und geregelten Ablauf

Ablauf

1. Vorgespräch mit dem Kunden
2. Erstellung eines Kundenspezifischen Angebots
3. Beauftragung durch den Kunden
4. „Permission to Attack“
5. Informationsbeschaffung
6. Umsetzung des Penetration Tests
7. Berichterstellung und Empfehlungen
8. Präsentation der Ergebnisse und des Abschlussberichts
9. Gegebenenfalls weitere Schritte

Vorgespräch

In einem Vorgespräch mit dem Kunden wird ermittelt welche Module im Rahmen des Penetrationtests benötigt werden, welchen Umfang der Penetrationtest hat und welcher Art der Penetrationtest sein soll.
Dazu sind die folgenden Informationen notwendig:

1. Art des Penetration Tests: Soll ein interner oder ein externer Penetration Test durchgeführt werden, oder beides?
2. Externe IP-Adressen: Wieviele IP-Adressen sind im Rahmen eines externen Penetration Test zu prüfen?
3. Interner IP-Range: Um welchen IP-Range handelt es sich im Rahmen eines internen Penetration Test?
4. Webanwendungen: Sind Webanwendungen vorhanden und zu prüfen?
5. Sollen Phishing-Tests durchgeführt werden?

Permission to Attack

Nach dem Vorgespräch kann ein entsprechendes, kundenspezifisches Angebot erstellt werden. Nach der Beauftragung erhält der Kunde die „Permission to Attack“ zum ausfüllen. Diese muss an uns zurückgesendet werden. Mit dem Dokument erteilt der Kunde die Erlaubis, im Rahmen des Penetrationtests seine Infrastruktur zu überprüfen. Die „Permission to Attack“ muss ausgefüllt und unterschrieben vom Kunden an die COMBACK zurückgeschickt werden. Im Rahmen der „Permission to Attack“ wird auch der geplante Zeitraum für den Penetrationtest mit dem Kunden vereinbart.

Informationsbeschaffung

Dieses Modul dient dem Kennenlernen der zu testenden Komponenten und Infrastruktur. Eventuelle Abhängigkeiten werden ermittelt, verfügbare Unterlagen identifiziert und ein Fokus der Sicherheits-analysen wird festgelegt. Aus diesem geht dann eine grobe Bedrohungsanalyse hervor.
Notwendige Voraussetzungen:

- Fachkundige Ansprechpartner auf Kundenseite, idealerweise zu den Themen IT, Security und Business Risk
- Termin mit allen beteiligten Ansprechpartnern. Dieser kann vor Ort oder remote stattfinden
- Austausch aller notwendigen Kontaktdaten beteiligter Ansprechpartner
- Ermittlung eines Notfallkontakts bei technischen Problemen
- Erstellung eines Anforderungskatalogs
- Überprüfung von Abhängigkeiten
- Vorab-Analyse von Bedrohungen

Umsetzung des Penetration Tests

Während der Umsetzung des Penetration Tests startet die Suche nach den Schwachstellen der Umgebung. Eine genaue Dokumentation des Vorgehens ist hier besonders wichtig. Die Systeme werden mit allem beschossen, so wie im Testdesign abgestimmt. Das gesetzte Ziel ist es nun, über die gefundenen Schwachstellen Zugriff auf die Infrastruktur zu erhalten.

Präsentation und Abschlussbericht

Ergebnis der Sicherheitsanalyse ist ein umfangreicher Bericht. Der Aufwand für die Erstellung der detaillierten Dokumentation stellt einen hohen Anteil am gesamten Analyseaufwand dar. Kern des Berichts ist eine Liste der Sicherheitslücken mit der Einschätzung des jeweiligen Risikopotentials. Die Präsentation des Abschlussberichts kann vor Ort oder in Form einer Websession stattfinden.
Der Bericht besteht im Wesentlichen aus den folgenden Teilen:

1. Management Teil – Der Management Teil ist zur Präsentation vor dem Management Board geeignet und beschreibt kurz zusammengefasst, in nicht technischer Sprache, das Ziel des Tests, die Ergebnisse der Analyse, Angriffsszenarien und die wichtigsten Empfehlungen.
2. Schwachstellentabelle – Die Schwachstellentabelle richtet sich an IT-Security-Verantwortliche und Projektleiter und listet identifizierte Schwachstellen, daraus abgeleitete Bedrohungen und die empfohlenen Gegenmaßnahmen auf. Die Bewertung erlaubt eine strukturierte und priorisierte Bearbeitung der Schwachstellen und legt damit das Fundament für die Verbesserung des Sicherheitsniveaus.
3. Technische Teil – Der technische Teil des Berichts beinhaltet sämtliche relevanten Details die während der Analysen erfasst und dokumentiert wurden. Er dient Administratoren, Entwicklern und technischen Projektverantwortlichen als Referenz, um die Testergebnisse nachvollziehen und empfohlene Gegenmaßnahmen ergreifen zu können.