PENETRATION TEST

By COMBACK

In einer sich ständig verändernden IT-Landschaft mit immer besser organisierten Angreifern und immer
neuen Bedrohungen ist Sicherheit ein zentrales Thema. Cybersicherheit ist inzwischen eine der wichtigsten Herausforderungen für Unternehmen und Organisationen geworden!

Die Lösung:

Penetration Tests

Penetration Tests sind simulierte Angriffe aus externen oder internen Quellen. Es handelt sich um umfassende Sicherheitstests einzelner oder mehrerer Rechner oder Netzwerke jeglicher Größe. Durch diese Angriffe werden die Sicherheitslücken von Anwendungen, Netzwerken und Infrastrukturen ermittelt. Durch methodische und manuelle Validierung der Wirksamkeit von Sicherheitsmechanismen werden mögliche Schwachstellen in den Systemen erkannt und können so behoben werden.

Gemeinsam finden wir den Schlüssel für die Sicherheit Ihrer IT!

Um die Penetration Tests optimal auf Ihr Unternehmen und Ihre Anforderungen abzustimmen, sind diese modular aufgebaut. Wir unterstützen Sie im Vorfeld bei der Auswahl der jeweiligen Module. Nach einer Vorbesprechung und Informationsbeschaffung werden die entsprechenden Tests und Analysen durch unsere Experten durchgeführt. Als Ergebnis erhalten Sie von uns einen ausführlichen Bericht mit entsprechenden Handlungsempfehlungen.
Im Rahmen der Beauftragung erhalten wir von Ihnen die Erlaubnis Ihre Umgebung im Rahmen eines Penetration Tests „angreifen“ zu dürfen. Danach läuft der Penetration Test nach folgenden Schritten ab.

Der Ablauf

1. Vorgespräch und Erfassung des Bedarfs – Im Rahmen der Vorbesprechung stellen wir den Status quo fest. Hierbei wird auch die aktuelle Gefährdungslage ermittelt.
2. Informationsbeschaffung – Erhebung der für den Angriff relevanten Informationen. Die Betrachtung des Unternehmens aus Sicht eines Angreifers.
3. Durchführung des Tests auf Basis der einzelnen Module.
    - Identifikation vorhandener Schwachstellen – Gezielte automatische und manuelle Tests zur Erkennung der Schwachstellen. Hierbei kommen auch aktuelle Methoden von kriminellen Hackern zum Einsatz.
    - Ausnutzung von Schwachstellen – Unsere Experten nutzten Sicherheitslücken bewusst aus. Es wird versucht auf geschützte Daten zuzugreifen.
4. Dokumentation, Berichterstellung und Präsentation – Wir fassen in unserem Abschlussbericht die Ergebnisse der Tests und Analysen zusammen. Die Schwachstellen werden aufgeführt und entsprechende Handlungsempfehlungen werden gegeben. Im Rahmen der Berichterstattung präsentieren wir die Ergebnisse und den Abschlussbericht in einem von Ihnen gewünschten Umfeld.

Die Module

1. Vorbesprechung und Informationsbeschaffung

2. Modul Infrastruktur
    - System, Diensteerkennung
    - Schwachstellenscan
    - Scan einzelner Dienste
    - Manuelle Dienstanalyse
    - Unautorisierte Zugriffe
    - Tests auf veraltete Dienste
    - Firewall Regeln
    - Netzsegmentierung
3. Modul Webanwendung
    - Basis Open Web Applikation
    - Security – OWAS
    - SSL Sicherheitsprüfung
    - Web Schwachstellenscan
    - Eingabevalidierung
    - Fehlermanagement
    - Manuelle Prüfung
4. Modul System – Reverse Proxy
    - System, Diensteerkennung
    - Schwachstellenscan
    - Scan einzelner Dienste
    - Manuelle Überprüfungen
5. Modul Dokumentation
6. Modul Präsentation
7. Modul Berichtsübergabe
8. Modul Umsetzungsreview
9. Modul Nachbesprechung