albiTC GmbH
BusinessIT + Components
Lilienthalstr. 3
82178 Puchheim

Fon 089 - 360 55 272
Fax 089 - 360 55 278

Mail info@albitc.de
Web www.albitc.de

Cyber Security Services

Basic Penetration Test (BPT)

Bei einem Basic Penetration Test (BPT) wird der aktuelle Sicherheitsstatus eines Systems oder Netzwerks bewertet, um Schwachstellen zu finden, die ein Angreifer ausnutzen könnte, um sich unbefugt Zugang zu Informationen und Systemen zu verschaffen. Dieser Prozess beinhaltet die Identifizierung von Sicherheitsschwachstellen, die zu einer mangelhaften Sicherheitskonfiguration von Systemen oder Anwendungen führen könnten, sowie bekannten oder unbekannten Schwachstellen in Hardware- oder Softwaresystemen.

Das Basic Penetration Testing deckt die IT-Systeme wie Firewalls, Router, VPN, IDS/IPS, Webserver, Anwendungsserver, Datenbankserver etc. des Unternehmens ab. Der Test liefert Erkenntnisse über den aktuellen Sicherheitsstatus, entdeckt mögliche Eindringwege und prüft die Wirksamkeit der Gegenmaßnahmen eines Unternehmens.

Unser Ansatz listet nicht nur die einzelnen Schwachstellen in jeder IT-Komponente auf, sondern ermittelt die systematischen Unzulänglichkeiten im Unternehmen, die zu diesen Problemen geführt haben. Wir wenden oftmals ein Probenahmeverfahren an, um uns auf die Grundursachen zu konzentrieren und die wichtigsten Korrekturmaßnahmen zu priorisieren.

Unsere Prüfungen im Rahmen des Basic Penetration Testing Services sind relativ zu den Sicherheitsprüfungen, die dazu dienen, negative Auswirkungen auf die Produktionsumgebung des Unternehmens zu begrenzen.

Unser PenTest-Partner-Team nutzt für seinen Basic Penetration Testing Service eine Kombination aus automatischen und manuellen Scanverfahren sowie handelsübliche und öffentliche Tools und eigens entwickelte benutzerdefinierte Skripte und Anwendungen.

Der Penetrationstestprozess umfasst die folgenden Schritte:

- Erkundung: Erfassung vorläufiger Daten oder Informationen über das Zielunternehmen. Die Daten werden gesammelt, um den Angriff besser planen zu können. Die in diesem Schritt erfassten Informationen umfassen IP-Adressenbereiche, öffentliche E-Mail-Adressen, Webseiten etc.

- Scan und Aufzählung: Sammlung weiterer Informationen über die verbundenen Systeme, laufenden Anwendungen und Dienste im Netzwerk des Unternehmens. Darüber hinaus werden Informationen wie Version und Typ des Betriebssystems, Benutzerkonten, E-Mail-Adressen, Dienstversionen und Versionsnummern gesammelt.

- Identifizieren der Schwachstellen: Basierend auf den in den vorherigen beiden Phasen gesammelten Informationen werden wir schwache Dienste in Ihrem Netzwerk oder Anwendungen mit bekannten Schwachstellen identifizieren.

- Ausnutzung: Wir nutzen bereits verfügbaren Code oder erstellen einen benutzerdefinierten Code, um die identifizierten Schwachstellen zu nutzen und Zugang zu dem angestrebten anfälligen System zu erhalten.

- Eskalation der Zugangsrechte: In einigen Fällen bietet die bestehende Schwachstelle nur Zugang auf einer einfachen Ebene wie etwa der normale Benutzerzugang mit begrenzten Zugangsrechten. In diesem Schritt werden wir versuchen, einen Zugang mit vollständigen Administratorrechten zu diesem Computer zu erhalten.

Nach Abschluss des Basic Penetration Testings erhält der Kunde einen ausführlichen Bericht, der Folgendes enthält:

- Zusammenfassung: Eine Zusammenfassung des Zwecks dieser Analyse sowie eine kurze Erläuterung der geschäftlichen Bedrohungen, denen das Unternehmen ausgesetzt ist.
- Erkenntnisse: Eine ausführliche technische Erläuterung der Erkenntnisse der Analyse zusammen mit Schritten und Nachweisen der Erkenntnisse.
- Schlussfolgerung und Empfehlungen: Dieser Abschnitt enthält abschließende Empfehlungen und eine Zusammenfassung der während der Sicherheitsbewertung festgestellten Probleme.

Möchten Sie mehr über unsere Cyber Security Assessment Services erfahren?

Dann wenden Sie sich bitte an uns.