WBS IT-Service

Kompetent.
Zuverlässig.
Individuell.

Lassen Sie sich von uns hacken – nicht von Angreifern

Mit Penetrationstests Sicherheitslücken erkennen

Schwachstellen in IT-Systemen bergen erhebliche Gefahren. Gelingt es Angreifern in Ihre Systeme einzudringen, kann es zu Betriebsstörungen sowie zu unbefugtem Datenzugriff, Datenschutzverletzungen oder Datenverlust kommen. Die Folgen sind weitreichend: Finanzielle Schäden, Vertrauensverlust und rechtliche Konsequenzen drohen. Bei KRITIS-Unternehmen ist sogar die Versorgung der Bevölkerung in Gefahr.

Die rechtzeitige Identifizierung und Behebung von Schwachstellen sind daher von entscheidender Bedeutung für die Sicherheit und Betriebsfähigkeit Ihres Unternehmens. Unsere erfahrenen IT-Sicherheits-Experten decken mit Penetrationstests genau diese Schwachstellen in IT-Systemen und Netzwerken auf. Gemeinsam stärken wir Ihre Sicherheitsarchitektur, minimieren Risiken und schützen Ihre IT und Ihre wertvollen Daten vor Angriffen.

Kurz erklärt: Was sind Penetrationstests?

Penetrationstests (kurz *Pentests*) sind manuell und gezielt durchgeführte Sicherheitsprüfungen von IT-Umgebungen und IT-Systemen.
Sie zeigen, inwiefern Ihre bestehenden IT-Sicherheitsmaßnahmen wirksam sind, und liefern ein aktuelles Bild von der Sicherheitslage Ihrer IT-Systeme und Netzwerke.

Die einzelnen Schritte eines Pentests

1 | Vorbereitung

- Planung des Angriffs entsprechend der abgestimmten Testziele
- Optional: Sammlung von Informationen über Zielunternehmen (z. B. IP-Adressen, Domains und Mitarbeiterinformationen)

2 | Scannen

- Detaillierte Analyse zur Identifikation von Sicherheitslücken und möglichen Angriffsvektoren
- Nutzung verschiedener Tools, um potenzielle Angriffsziele wie offene Ports im Netzwerk zu ermitteln

3 | Ausnutzung

- Ausnutzung identifizierter Sicherheitslücken in Form konkreter Angriffe
- Maximaler Zugriff auf Daten und/oder Dienste durch Erlangen von Privilegien und Netzwerkinformationen
- Ermittlung der potenziellen Auswirkungen der Sicherheitsverletzungen

4 | Analyse & Reporting

- Detaillierte Dokumentation des Testablaufs
- Auswertung der Angriffe inkl. eingesetzter Tools
- Risikobewertung der identifizierten Schwachstellen
- Empfehlungen zur Optimierung Ihrer Schutzmaßnahmen

Unsere Penetrationstests bieten Ihnen zielgenaue Sicherheit!

WBS IT-Service GmbH • Friedrich-Ebert Str. 61 • 04109 Leipzig
+49 341 98271 0
security.solutions@wbs-it.de
www.wbs-it.de

Von Einzelprüfungen zum Rundumcheck – Sie bestimmen den Testumfang

Mit unserem Penetrationstest bieten wir Ihnen eine gezielte Überprüfung von IT-Umgebungen oder einzelner Komponenten unter der Berücksichtigung individueller Bedrohungsszenarien. Um bestmöglich auf Ihren Bedarf einzugehen, bieten wir Ihnen den **Pentest in Form verschiedener Module**. Die Durchführung kann als Black-Box- oder White-Box-Test erfolgen. Sie bestimmen mit der Auswahl der einzelnen Elemente den Umfang und die Tiefe des Pentests.

Vom Ersteindruck ...

MODULE

1. Test einzelner Clients, Server, Apps oder anderer Netzwerkkomponenten
2. Test des Perimeters: Angriffssimulation auf das Netzwerk von außen
3. Interner Test: Angriffssimulation innerhalb des Netzwerks
4. WLAN-Test: Prüfung der WLAN-Sicherheit
5. Physische Sicherheitstests: Zutrittsprüfung für Gebäude und Anlagen
6. Red Team Assessment: eine vollumfängliche Angriffssimulation

... zum Klarblick

Ihr Weg zur maximalen Stärkung der Cyberabwehr

Penetrationstests sind eine Momentaufnahme des aktuellen Zustands Ihrer IT-Sicherheit und somit ein idealer Ausgangspunkt für die Optimierung Ihrer Security-Maßnahmen. Zuerst sollten die im Test identifizierten Sicherheitslücken geschlossen werden. Außerdem empfehlen wir die jährliche Wiederholung des Pentests, um die neu implementierten Sicherheitsmaßnahmen auf ihre Wirksamkeit hin zu prüfen.
Im Sinne unseres 360°-Security-Ansatzes unterstützen wir Sie auch gern mit Security-Services, die den Pentest sinnvoll ergänzen, zum Beispiel mit einem kontinuierlichen Schwachstellenmanagement oder Security Operation Center (SOC). So sind Sie bestmöglich vor Cyberangriffen gewappnet.

Ihre Vorteile unserer WBS-Pentests im Überblick:

Individualität statt Standard:
Passgenaue Bedarfsanalyse als Teil der Dienstleistung

IT-Sicherheit erhöhen:
Schwachstellen vor den Angreifern erkennen, um sie rechtzeitig schließen zu können

IT-Compliance umsetzen:
Regelmäßige Pentests als wirksames Werkzeug zur Einhaltung von IT-Security-Vorgaben (zum Beispiel für KRITIS-Betreiber)

Vertrauen schaffen:
Pentests als Beleg für hohe interne IT-Sicherheitsstandards und starker Wettbewerbsvorteil

Penetrationstests sollten in keiner nachhaltigen IT-Sicherheitsstrategie fehlen:

- Sie tragen dazu bei, die Gesamtsicherheit Ihres Unternehmens zu stärken.
- Sie minimieren das Risiko von Sicherheitsvorfällen.
- Sie senken das Risiko von Ausfallzeiten, Reputationsschäden und finanziellen Verlusten deutlich.

1.0 | 012024 | ö

+49 341 98271 0 security.solutions@wbs-it.de www.wbs-it.de