Pentest Checklist

Ihr Leitfaden zur erfolgreichen Sicherheitsanalyse

Ein Service Ihrer Cybersecurity-Partner – SilentSec

Einleitung

Cybersecurity ist keine einmalige Maßnahme, sondern ein kontinuierlicher Prozess.

Penetrationstests simulieren reale Angriffe, um Schwachstellen aufzudecken, bevor sie ausgenutzt werden.

Diese Checkliste unterstützt Sie strukturiert bei Vorbereitung und Beauftragung eines Pentests.

Kapitel 1: Scope Definition – Was soll getestet werden?

- ☐ Öffentliche Webanwendungen
- ☐ Interne Webanwendungen
- ☐ API-Schnittstellen
- ☐ Mobile Apps inkl. Backend
- ☐ Netzwerk-Infrastruktur
- ☐ Interne Netzwerke
- ☐ Cloud-Umgebungen
- ☐ IoT / OT Komponenten
- ☐ Physische Sicherheit / Social Engineering

Weitere Details zum Scope:

Testtiefe & Methodik

- ☐ **Black-Box Test**
- ☐ **Grey-Box Test**
- ☐ **White-Box Test**

Primäres Ziel des Pentests:

Budgetrahmen:

Testzeitraum:

Kapitel 2: Vertragliche & organisatorische Vorbereitung

- ☐ **Management-Freigabe vorhanden**
- ☐ **Primärer Ansprechpartner benannt**
- ☐ **Systemeigner informiert**
- ☐ **IT / SOC informiert**

Primärer Ansprechpartner (Name / Kontakt):

Kapitel 3: Technische Vorbereitung

- ☐ **Test-Accounts / API-Keys bereitgestellt**
- ☐ **Staging-/Testumgebung verfügbar**
- ☐ **Backups & Rollback geprüft**
- ☐ **Architektur-/API-Dokumentation vorhanden**
- ☐ **Pentest-IP freigeschaltet**

Besondere technische Hinweise:

Kapitel 4: Nachbereitung & Reporting

- ☐ **Executive Summary**
- ☐ **Methodikbeschreibung**
- ☐ **Detaillierte Findings**
- ☐ **Handlungsempfehlungen**
- ☐ **Technischer Anhang**

Fragen für das Review-Meeting:

Ihr nächster Schritt

Diese Checkliste dient der Vorbereitung und stellt keine Beauftragung dar.

Name / Funktion: _____

Datum: _____