SIZ

Finanzgruppe

Penetrationstest

Test Ihrer IT-Infrastruktur gegen Angriffe und unbefugtes Eindringen

Wirksamkeit der vorhandenen Absicherung praxisnah überprüfen

Penetrationstest – ein unverzichtbarer Bestandteil von Sicherheitsüberprüfungen

Wir bieten die Durchführung von Penetrationstests als Bestandteil einer ganzheitlichen Vorgehensweise zur Durchführung von Sicherheits-Audits an. Hierbei wird die Sicherheit Ihrer Systeme aus Sicht eines Angreifers (Hacker, Cracker) getestet. Die Bandbreite der getesteten Systeme erstreckt sich von einfachen Internet-Anwendungen bis hin zu komplexen Unternehmensnetzwerken. Der Ergebnisbericht enthält die identifizierten Schwachstellen und auch Empfehlungen für technische und organisatorische Maßnahmen zur Behebung derselben.

Arten von Penetrationstests

Die SIZ GmbH unterstützt Sie mit verschiedenen Arten von Penetrationstests, wie:

- **Off-Site-Tests:** Überprüfung der aus dem Internet erreichbaren Anwendungen des Unternehmens.
- **On-Site-Tests:** Angriffsversuche auf Anwendungen und Systeme aus dem internen Netzwerk des Unternehmens sowie das Abhören von vertraulichen Informationen (z. B. Passwörter).

Sie legen den Rahmen fest

Abhängig von Ihren Wünschen können wir die Penetrationstests auf unterschiedlicher Informationsbasis durchführen. Unterschieden wird hierbei zwischen **Black-Box-Tests** (ohne Kenntnis der zu prüfenden Systeme), **White-Box-Tests** (mit Kenntnis der zu prüfenden Systeme) und **Mischformen** dieser beiden Grundprinzipien.

Gemeinsam wird das Niveau der **Aggressivität**, mit der die Penetrationstests durchgeführt werden bestimmt. Hierbei wird das Vorgehen grob unterschieden zwischen **„passiv“** (Zielobjekte werden nur passiv untersucht, z. B. durch Port- oder Vulnerability-Scans), **„vorsichtig“** (Identifizierte Schwachstellen werden nur ausgenutzt, wenn eine Beeinträchtigung eines Systems hinreichend ausgeschlossen werden kann) und **„aggressiv“** (ausnutzen aller Schwachstellen auch wenn es zu Beeinträchtigung, z. B. der Verfügbarkeit kommen kann).

Erprobte Vorgehensweise

Die Durchführung von Penetrationstests erfolgt mit einer erprobten Vorgehensweise.

SIZ Vorgehensweise: Definierte Schritte

Hierdurch sind hohe Qualität der Ergebnisse und Sicherheit bei der Test-Durchführung gewährleistet.

Wir sind kompetent, verfügen über langjährige Erfahrung und das entsprechende Know-how
Bei der konkreten Durchführung von Penetrationstests kommen unterschiedliche Techniken zum Einsatz.

Oft werden zunächst automatisierte Schwachstellen-Scans durchgeführt. Die daraus erhaltenen Ergebnisse lassen alleine noch keine qualifizierten Aussagen zu – nach unserem Verständnis ist ein Penetrationstest deshalb mehr: Die von den Scannern identifizierten potenziellen Schwachstellen werden von uns sowohl technisch als auch logisch verifiziert und bewertet.

Für die erfolgreiche Umsetzung vieler Angriffstechniken ist entsprechende Kreativität und Erfahrung notwendig, die in zahlreichen Penetrationstests bewiesen wurde. Darüber hinaus stehen wir auf dem Standpunkt, dass echte Penetrationstester Erfahrung im Design und der Implementierung von Sicherheitskonzepten haben müssen.

Diese Erfahrung haben wir!

Unsere Dienstleistung
Vor der Durchführung des Penetrationstests beraten wir Sie über die Vor- und Nachteile einzelner Arten von Penetrationstests und erarbeiten gemeinsam mit Ihnen einen Lösungsweg.

Als effektives Vorgehen hat sich die Kombination von Penetrationstest und System-/Anwendungsaudit erwiesen. Hierzu kann auf unser Portfolio von Audit-Modulen aus dem Produkt „Sichere IT-Plattform“ zurückgegriffen werden.

Sie erhalten ein auf Ihre konkreten Anforderungen zugeschnittenes Ergebnis unter Berücksichtigung eines optimalen Kosten-Nutzen-Verhältnisses.

Die SIZ GmbH

Wir setzen Maßstäbe für zukunftsfähige IT- und Sicherheitsstandards sowie für das Beauftragtenwesen in der Finanzwirtschaft und darüber hinaus.

Unsere Schwerpunkte
- Informationssicherheit
- S-CERT
- IT-Steuerung
- Revision
- Payments
- Beauftragtenwesen
  - Datenschutz
  - Informationssicherheitsbeauftragter
  - Geldwäsche- und Betrugsprävention
  - Wertpapier- und MaRisk-Compliance

Unser Angebot
- Individuelle Beratung und Unterstützung
- Übernahme von Beauftragtenfunktionen
- Softwareprodukte
- Standards im Zahlungsverkehr

Unsere Kunden
- Privat- und Geschäftsbanken, genossenschaftliche Banken, Sparkassen, Landesbanken sowie deren Verbände und Verbundpartner
- Kartengesellschaften, Zahlungsverkehrs-Dienstleister
- Versicherungsunternehmen
- Unternehmen aus Industrie und Handel
- IT-Dienstleister und IT-Anbieter

Fokus: Informationssicherheit, S-CERT, IT Steuerung
- Informationssicherheits-Managementsysteme (ISMS)(Aufbau, Beratung und Auditierung)
- Sicherer IT-Betrieb: ISO 27001-konforme Produkte für das ISMS
- Zertifizierung von ISMS
- Beratung und Unterstützung für das ISMS/den ISB
- Beratung und Audits zur Geschäftsfortführung (BCM) und Durchführung von Notfallübungen
- Konzeption von IT-Sicherheitslösungen
- Durchführung von Sicherheitsaudits (inkl. Pentests)
- CERT-Dienstleistungen
- Beratung und Lösungen für das Management von IDV und zum Programmeinsatzverfahren

Sie können sich darauf verlassen!

Wir finden die optimale Lösung für Ihre individuellen Anforderungen.

Haben Sie Fragen, Wünsche oder möchten Sie einen konkreten Gesprächstermin vereinbaren?

Ihr Ansprechpartner

Stephan Rostmann
Managementberater
Services RiMaGo
und Informationssicherheit
Telefon: +49 (0)228 4495-7306
E-Mail: stephan.rostmann@siz.de