Penetration Testing

Vertrauen ist gut – Kontrolle ist besser. Unser Penetration Testing prüft angemessen Applikationen und Systeme und liefert nachvollziehbare Berichte über den Stand der Sicherheit.

DIE HERAUSFORDERUNG

Man kann vieles tun, um Software und Systeme sicherer zu machen. Das Penetration Testing zum Schluss zeigt, wie erfolgreich man war.

„Penetration Testing bedeutet, die Brille des Angreifers aufzusetzen, mit dessen Tools und Wissen ein technisches System auf Verwundbarkeit zu prüfen – bevor es ein wirklicher Angreifer tut.“

Testarten und typischer Ablauf

Es gibt verschiedene Arten des Penetration Testing: Bei einem Black-Box-Test hat der Tester keinerlei Informationen über sein Zielsystem. Im Gegensatz hierzu bildet ein White-Box-Test den Fall eines voll informierten Innentäters ab. Eine häufig genutzte Variante ist der sogenannte Grey-Box-Test, der mit einem realistischen Maß an gegebenen Informationen einen guten Kosten-Nutzen-Faktor erreicht.

Die eigentlichen Tests laufen nach folgendem Muster ab:

1. Informationsbeschaffung aus Sicht des Angreifers
2. Scannen der Zielsysteme
3. System- und Anwendungserkennung
4. Recherche nach Schwachstellen
5. Ausnutzen der Schwachstellen

Nach Beendigung der Tests wird eine umfangreiche Dokumentation erstellt, die die durchgeführten Tests, die gefundenen Schwachstellen und insbesondere Verbesserungsvorschläge zum Schließen der Schwachstellen enthält. Die Inhalte der Dokumentation können auch durch eine Präsentation, einen Praxisworkshop oder ein Live-Hacking anschaulich vermittelt werden. Da ein Penetration Testing immer nur eine Momentaufnahme darstellen kann, folgt später ein Nachtest, der im besten Fall die gefundenen Schwachstellen als abgestellt klassifiziert.

LEISTUNGSSPEKTRUM

Governance, Risk & Compliance

- Sicherheits- und Notfallmanagement
- Best Practices nach ISO 27001, ISO 22301, IT-Grundschutz und A-960/1
- Vulnerability und Risk Assessments
- Risikomanagementstrategien
- Aufbau von Sicherheitsprozessen
- Datenschutz und Datensicherheit
- EU-Datenschutzgrundverordnung
- Awareness Training

Secure Systems Engineering

- Sichere Netzarchitekturen
- Identity- und Accessmanagement
- Sichere Softwareentwicklung
- Security Testing

Managed Security Services

- Penetration Testing
- Monitoring und Alerting
- SOC/SIEM-as-a-Service
- Forensics und Malware Analysis
- Advanced Threat Intelligence

CGI ist Partner der Allianz für Cyber-Sicherheit des BSI und BITKOM.

Allianz für Cyber-Sicherheit

de.cgi.com/cybersecurity

UNSERE ANTWORT

Nachvollziehbare Testframeworks

Penetration Testing nach anerkannten Frameworks wie OWASP, OSSTMM, SANS CWE Top 25, WebAppSec und PCI DSS garantieren eine nachvollziehbare und überzeugende Arbeit.

Für jede Aufgabe das richtige Werkzeug

Unsere Experten besitzen ein reich gefülltes Toolset für jeden Test. So können wir jeden Angriffsvektor optimal analysieren.

- Netzwerk-Sniffer
- ARP Spoofing Tools & IP Packet Generatoren
- Port & Vulnerability Scanner
- Man-in-the-Middle-Tools
- Web-Attack-Proxys
- Fuzzing Tools
- WLAN Decryption Tools

Aggressivität nach Bedarf

Penetration Tests können in verschiedenen Aggressivitätsstufen durchgeführt werden. So können Live-Systeme ohne Ausfallgefahr getestet werden, während es für nicht produktive Systeme möglich ist, bis zum Ausfall zu testen.

Verdeckt oder öffentlich – RedTeaming oder PenTest

Verdeckte Penetration Tests stellen Alarmsysteme und Eskalationsprozeduren auf die Probe. Bei öffentlichen Tests hingegen werden die Systemverantwortlichen direkt eingebunden. Dies ist besonders bei hochkritischen Live-Systemen zu empfehlen, um bei unvorhergesehenen Problemen zeitnah reagieren zu können.

Zusätzlich besteht die Möglichkeit, den Penetration Test zu erweitern. Beim sog. RedTeaming testen unsere Experten nicht nur die eigentliche Applikation bzw. das System, sondern verfolgen einen ganzheitlichen Testansatz, angefangen bei der Informationsbeschaffung mittels Social Engineering über den physikalischen Zugangsschutz zu Netzwerk und Systemen bis hin zum eigentlichen Penetration Testing – das ist Informationssicherheit auf einem ganz neuen Level.

IHR GEWINN

Profitieren Sie von den Erfahrungen unserer zertifizierten Experten im Penetration Testing, Threat Hunting, Forensics und Malware Analysis.

Flexible Leistungserbringung

Unsere Services schneidern wir nach Maß auf Ihre individuellen Bedürfnisse zu. Penetration Testing wird als alleinige Leistung ebenso wie zur Verstärkung von Sicherheits- und Risikoanalysen angeboten. Den Schwerpunkt bestimmen dabei immer Sie!

ÜBER CGI

CGI ist ein globaler Dienstleister für IT und Geschäftsprozesse. Wir wurden 1976 gegründet und verfügen heute an 400 Standorten in 40 Ländern über insgesamt 77.500 Mitarbeiter.

Für unsere Kunden sind wir weltweit vor Ort – mit strategischer IT und Business-Beratung, Systemintegration, Managed IT, Business Process Services und Intellectual Property auf Top-Niveau.

Wir unterstützen unsere Kunden dabei, laufende Investitionen besser zu nutzen und gleichzeitig neue digitale Technologien und Business-Strategien einzusetzen, durch die sich optimale Lösungen entlang der gesamten Wertschöpfungskette realisieren lassen.

Im Hinblick auf Zeit- und Budgettreue bekommen wir auf Grund unserer strikten Lieferdisziplin regelmäßig Bestnoten. Dazu konnten wir in den Kundenzufriedenheitsanalysen der vergangenen zehn Jahre kontinuierlich mehr als neun von zehn möglichen Punkten erzielen.

Für weitere Informationen kontaktieren Sie uns unter info.de@cgi.com oder besuchen Sie uns auf: de.cgi.com/cybersecurity

de.cgi.com/cybersecurity