Penetration Testing

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

DIE HERAUSFORDERUNG

Man kann vieles tun, um eine Software fehlerarm zu machen und Systeme sicher zu implementieren. Am Ende steht ein Test, ob es erfolgreich war.

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

Die Testarten

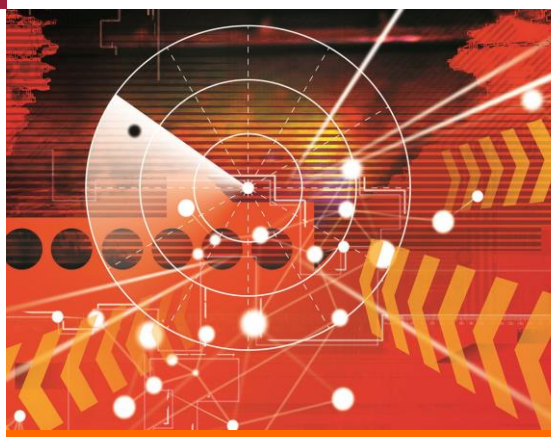
Penetration Tests sind unter verschiedenen Voraussetzungen möglich. Bei einem Black-Box Test hat der Tester keinerlei Informationen über sein Zielsystem und nimmt so die Rolle eines Außenstehenden ein. Im Gegensatz hierzu bildet ein White-Box Test den Fall eines voll informierten Innentäters ab. Eine häufig genutzte Testvariante ist der sogenannte Grey-Box Test, der mit einem realistischen Maß an gegebenen Informationen einen guten Kosten-Nutzen-Faktor erreicht.

Der Ablauf

Zu Beginn steht immer ein Kick-Off Meeting, bei dem die Randbedingungen des Tests besprochen und festgehalten werden. Anschließend folgt der eigentliche Testblock nach folgendem generischem Muster:

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

Nach Beendigung des Testblocks wird eine umfangreiche Dokumentation erstellt, die die durchgeführten Tests, die gefunden Schwachstellen sowie Verbesserungsvorschläge zum Abstellen der Schwachstellen enthält. Diese Inhalte der Dokumentation können auch durch eine Präsentation, einen Praxisworkshop oder ein Live Hacking anschaulich vermittelt werden. Da ein Penetration Test immer nur eine Momentaufnahme darstellen kann, folgt später ein Nachtest, der im besten Fall die gefundenen Schwachstellen als abgestellt klassifiziert.



PENETRATION TESTING
gehört zum Lösungsportfolio der
CGI CYBERSECURITY SERVICES

Strategy, Compliance & Transformation

- Informationssicherheits- und Notfallmanagement
- Best Practices nach ISO 27001, ISO 25999, IT-Grundschutz und A-960/1
- Vulnerability Assessments und Penetration Testing
- Risikomanagementstrategien
- Aufbau von Sicherheitsprozessen
- Datenschutz und Datensicherheit
- Awareness Training

Secure Systems Engineering

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

Managed Security Services

- Managed Services
- Monitoring & Alerting
- SIEM design & operations
- Forensics & Malware Analysis
- Advanced Threat Intelligence

de.cgi.com/cybersecurity

UNSERE ANTWORT

Nachvollziehbare Testframeworks

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

Für jede Aufgabe das richtige Werkzeug

Eine Vielzahl von Tools unterstützen den Penetration Tester bei seiner Arbeit. Jede Facette des Tests kann so optimal abgearbeitet werden.

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

Aggressivität nach Bedarf

Penetration Tests können in verschiedenen Aggressivitätsstufen durchgeführt werden. So können Livesysteme ohne Ausfallgefahr getestet werden, während es für nicht produktive Systeme möglich ist bis zum Ausfall zu testen. Folgende Stufen werden unterschieden:

- Passiv scannend
- Vorsichtig
- Abwägend
- Aggressiv

Verdeckt oder Öffentlich

Verdeckte Penetration Tests ermöglichen das Testen von Alarmsystemen und Eskalationsprozeduren. Dies ist genauso möglich wie offensichtliche Tests, bei denen die Systemverantwortlichen direkt eingebunden werden. Dies ist besonders bei hochkritischen Systemen aufgrund der schnellen Reaktionsmöglichkeiten bei unvorhergesehenen Problemen zu empfehlen.

IHR GEWINN

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

Flexible Leistungserbringung

Unsere Services schneiden wir nach Maß auf Ihre Bedürfnisse zu. Penetration Testing wird als alleinige Leistung ebenso wie zur Verstärkung von Sicherheits- und Risikoanalysen angeboten.

Schwerpunkte können z.B. die Netzwerk-Infrastruktur, Betriebssysteme, Datenbanken oder auch mobile oder Web-Applikationen sein.

Über CGI

Mit 70.000 Mitarbeitern an 400 Standorten in 40 Ländern übernimmt CGI vor Ort Verantwortung für den Erfolg seiner Kunden und bietet ihnen gleichzeitig globale Lieferfähigkeit. Seit unserer Gründung im Jahr 1976 pflegen wir eine strikte Lieferdisziplin, dank der unsere Projekte in Bezug auf Zeit- und Budgettreue in der Branche führend sind. Mit Business und IT Consulting, Systemintegration sowie Outsourcing Services auf höchstem Niveau unterstützt CGI seine Kunden dabei, laufende Investitionen besser zu nutzen und gleichzeitig neue Technologie- und Business-Strategien einzusetzen, mit denen sich optimale Lösungen für die gesamte Wertschöpfungskette erreichen lassen.

Das Resultat unseres Commitments zeigt sich im gemessenen Kundenzufriedenheitswert, der in den vergangenen zehn Jahren durchgängig mehr als 9 von 10 möglichen Punkten betrug.

IHR ANSPRECHPARTNER

CGI Deutschland Ltd. & Co. KG

Practice Cybersecurity

(Practice Head: **Frank Reiländer**)

Ettore-Bugatti-Straße 6-14
51149 Köln
T: +49 2203 6993 1050
Für weitere Informationen kontaktieren Sie uns unter csi@cgi.com
oder besuchen Sie uns auf de.cgi.com/cybersecurity.