Penetration Testing

Für Energieunternehmen ist ein hohes Maß an Sicherheit unverzichtbar. Im Rahmen unseres Penetration Testing prüfen wir Ihre Applika-tionen und Systeme und liefern Ihnen zuverlässige Berichte.

Die Herangehensweisen beim Penetration Testing

Wer ein Penetration Testing durchführt, versetzt sich in die Rolle eines Angreifers und prüft mit dessen Tools und Wissen ein technisches System auf seine Verwundbarkeit hin – bevor ein tatsächlicher Angriff stattfindet.

Dabei gibt es verschiedene Herangehensweisen: Bei einem Black-Box-Test haben die Testerinnen und Tester keinerlei Informationen über das Zielsystem und nehmen so die Rolle von Außenstehenden ein. Im Gegensatz hierzu bildet ein White-Box-Test den Fall einer voll informierten internen Täterin bzw. eines internen Täters ab. Eine häufig genutzte Testvariante ist auch der sogenannte Grey-Box-Test, der mit einem realistischen Maß an gegebenen Informationen einen guten Kosten-Nutzen-Faktor erreicht.

Der Ablauf unseres Penetration Testing

Unser Penetration Testing startet mit einem Kick-off-Meeting, in dem die Rahmenbedingungen des Tests besprochen und festgehalten werden. Anschließend folgt der eigentliche Testblock nach diesem Muster:

1. Informationsbeschaffung aus Sicht des Angreifers
2. Scannen der Zielsysteme
3. System- und Anwendungserkennung
4. Recherche nach Schwachstellen
5. Ausnutzen der Schwachstellen
6. Aufrechterhaltung des Zugriffs
7. Verdecken der Spuren

Unsere ganzheitliche Sicherheitsstrategie

Unser Penetration Testing prüft Ihre technischen Systeme auf Verwundbarkeit, deckt Sicherheitslücken auf und definiert notwendige Sicherheitsmaßnahmen.

Es ist ein wesentliches Element unserer ganzheitlichen Sicherheitsstrategie.

Unser Penetration Testing bieten wir sowohl als alleinige Leistung an, als auch zur Verstärkung von Sicherheits- und Risikoanalysen. Besondere Schwerpunkte können dabei in der Netzwerkinfrastruktur, den Betriebssystemen, den Datenbanken oder auch mobilen bzw. Online-Apps liegen.

Nach Beendigung des Testblocks wird eine umfangreiche Dokumentation erstellt, die alle durchgeführten Tests, identifizierten Schwachstellen und Verbesserungsvorschläge enthält. Die Inhalte dieser Dokumentation können 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 zeigt, dass alle Schwachstellen beseitigt werden konnten.

Unsere Testframeworks und Tools

Unser Penetration Testing wird auf der Basis anerkannter Frameworks wie OWASP, OSSTM, SANS CWE Top 25, WebAppSec und PCI DSS durchgeführt. Dies garantiert Ihnen die Nachvollziehbarkeit und Zuverlässigkeit unserer Arbeit.

Eine Vielzahl von Tools unterstützt unsere Penetration Testerinnen und Tester bei ihrer Arbeit:

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

So kann jede Facette des Tests optimal abgearbeitet werden.

Anforderungsgerechte Aggressivität

Unsere Penetration Tests werden in verschiedenen Aggressivitätsstufen (passiv, vorsichtig, abwägend oder aggressiv) durchgeführt. Auf diesem Weg können Livesysteme ohne Ausfallgefahr getestet werden, während es bei nichtproduktiven Systemen möglich ist, bis zum Ausfall zu testen.

Verdeckte oder offensichtliche Tests

Verdeckte Penetration Tests ermöglichen das Testen von Alarmsystemen und Eskalationsprozeduren. Bei offensichtlichen Tests werden dagegen die Systemverantwortlichen direkt miteingebunden. Bei hochkritischen Systemen ist dieses Verfahren aufgrund der schnellen Reaktionsmöglichkeiten bei unvorhergesehenen Problemen besonders empfehlenswert.

Individuell angepasst und anforderungsgerecht

Profitieren Sie von den Erfahrungen unserer zertifizierten Expertinnen und Experten in den Bereichen Penetration Testing, Threat Hunting, Forensics & Malware Analysis. Unsere Services schneiden wir jeweils auf Ihre Bedürfnisse zu.

Die Sicherheit Ihrer Systeme lässt sich durch viele Maßnahmen verbessern. Am Ende beweist der Test, ob diese erfolgreich waren.

Über CGI

Wir sind ein globales Dienstleistungsunternehmen für IT- und Geschäftsprozesse und wurden 1976 gegründet. Heute sind wir mit 88.500 Mitarbeitenden an 400 Standorten in 40 Ländern vertreten. Unsere flexiblen End-to-End-Services umfassen strategische IT- und Business-Beratung, Systemintegration, Managed IT und Intellectual Property auf Top-Niveau. Wir unterstützen unsere Kunden bei der Transformation ihres Unternehmens zu einer agilen Organisation und setzen unsere IP-Lösungen dafür ein, Innovation zu beschleunigen. Durch intelligente Systemintegration treiben wir die IT-Modernisierung unserer Kunden voran; mit unseren Managed IT Services und Geschäftsprozess-Dienstleistungen helfen wir ihnen, den Kostendruck zu mindern und ihre Technologie-Lieferketten optimal einzusetzen.

Unser Ansprechpartner für Informationssicherheit:

Ludwig Ederle
ludwig.ederle@cgi.com
+49 172 4498230

Für weitere Informationen:
www.cgi.com/de
info.de@cgi.com