NØN GRATA
Security Consulting

PENETRATION TESTING - IHRE SICHERHEIT AUF DEM PRÜFSTAND

Was ist ein Penetration Test?

Penetration Testing (auch „Pen Test“ genannt) bezeichnet einen kontrollierten, gezielten Sicherheitsangriff auf IT-Systeme, Netzwerke, Anwendungen oder physische Einrichtungen.
Ziel des Tests ist es, Sicherheitslücken zu identifizieren, bevor Angreifer dies tun – und das unter realistischen Bedingungen.

Cyberangriffe und Sicherheitsvorfälle sind heutzutage keine Seltenheit mehr. Sie kosten Unternehmen jährlich Milliarden.
Ein professioneller Penetration Test gibt Ihnen die Möglichkeit, Ihre Mitarbeiter zu sensibilisieren und Schwachstellen frühzeitig zu erkennen, bevor diese Schaden anrichten.

Physisches Penetration Testing: Schutzschild gegen Spionage und Infiltration

In einer Zeit geopolitischer Spannungen und zunehmender Bedrohungen durch fremde Nachrichtendienste ist die Sicherung sensibler Infrastruktur von zentraler Bedeutung.
Während Cybersecurity in aller Munde ist, bleibt ein ebenso kritischer Bereich oft unbeachtet: der Zutritt zu Gebäuden, Anlagen und Sicherheitsbereichen.
Saboteure setzen gezielt auf Infiltration durch physisches Eindringen.
Sei es durch manipuliertes Personal, gefälschte Identitäten oder das Ausnutzen baulicher und organisatorischer Schwächen.
Im Fokus sind nicht nur militärische Einrichtungen, sondern auch Unternehmen, kritische Infrastruktur, Forschungseinrichtungen und Behörden.

Ein physischer Pen Test (auch „Red Teaming“ genannt) ist der kontrollierte Versuch, im Auftrag eines Unternehmens oder einer Behörde, deren physische Sicherheitsbarrieren zu überwinden.
Dabei wird simuliert, wie reale Angreifer vorgehen würden, um unbefugt Zugang zu Gebäuden, Serverräumen, Archiven oder Produktionsbereichen zu erlangen.

Typische Testmethoden

Überwindung von Zugangskontrollen (Schließsysteme, Kartenleser, Scanner)

Social Engineering (Manipulation von Personal - „Schwachstelle Mensch“)

Nutzung baulicher Schwächen (Notausgänge, Fenster, Wartungsschächte)

Analyse von Wachroutinen und Alarmierungsprozessen

Unser Vorgehen

Auftrag & Zieldefinition
Abstimmung der Testziele mit dem Auftraggeber,
Umfang und rechtlicher Rahmen (z. B. NDA)

Informationsgewinnung (Reconnaissance)
Sammlung von Daten über Systeme, Infrastruktur oder Räumlichkeiten

Durchführung der Tests
Simulierte Angriffe durch unser Team

Analyse & Reporting
Ausführlicher Bericht mit gefundenen Schwachstellen, Risikobewertung und konkreten Handlungsempfehlungen

Abschlussbesprechung
Klärung offener Fragen, gemeinsame Planung möglicher Gegenmaßnahmen

Unser Team bedient sich einer breiten Palette an Erfahrungen, Fähigkeiten und Kreativität. Dadurch sind wir in der Lage, unterschiedlichste Szenarien auf verschiedenen Ebenen für Ihr Unternehmen abzubilden.

Senden Sie uns eine kurze Kontaktanfrage an info@nongrata-consulting.com
Wir setzen uns zeitnah mit Ihnen in Verbindung.