

CYQUEO

Cyber-Security Solutions

Pentest & Schwachstellenanalyse

Ihr Schutz vor
unerkannten Sicherheitslücken



Unser Ansatz

In einer zunehmend digitalisierten Welt sind Sicherheit und Vertrauen entscheidende Faktoren für den nachhaltigen Erfolg eines Unternehmens. Bei CYQUEO verstehen wir die Bedeutung einer proaktiven Sicherheitsstrategie und die Notwendigkeit, Schwachstellen frühzeitig zu erkennen und zu beseitigen.

Unser Team verfügt über langjährige Erfahrung im Bereich IT-Sicherheit und kombiniert technisches Know-how mit praxisorientiertem Denken. Dadurch sind wir in der Lage, Systeme aus unterschiedlichen Perspektiven zu analysieren und selbst versteckte Schwachstellen zuverlässig aufzudecken.

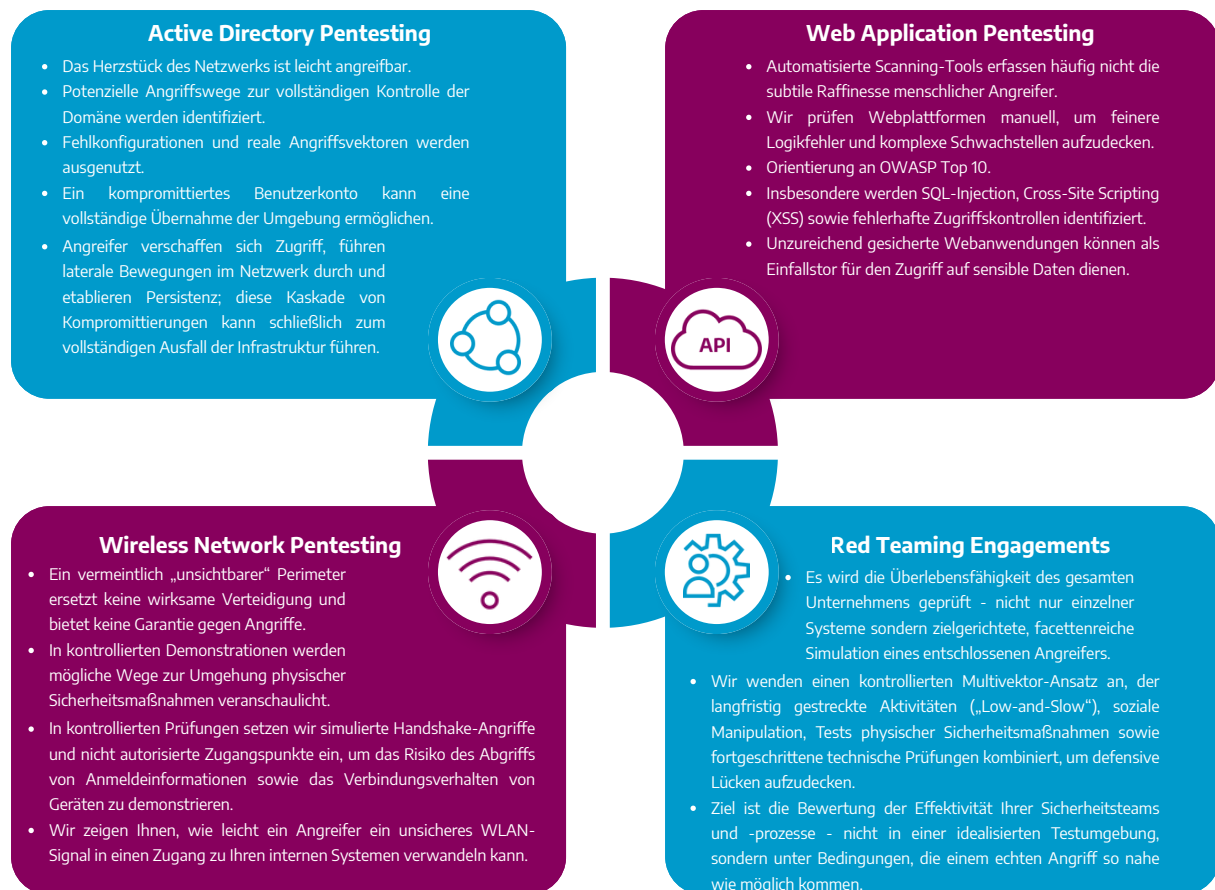
Unsere Pentest und Schwachstellenanalysen sind individuell auf die spezifischen Anforderungen jeder Organisation zugeschnitten. Wir kombinieren modernste Techniken, praxisnahe Angriffsszenarien (u.a. MITRE Angriffsszenarien) und tiefgehendes technisches Fachwissen, um ein realistisches Bild Ihrer Sicherheitslage zu liefern.

Für jeden Pentest stellen wir ein dediziertes Expertenteam ab, das den Testprozess begleitet und regelmäßig transparentes Feedback zum aktuellen Stand und zu ersten Erkenntnissen liefert.

Vertrauen Sie auf uns, um Ihre Informationssysteme zu schützen, regulatorische Anforderungen zu erfüllen und die Sicherheit Ihrer geschäftskritischen Assets nachhaltig zu gewährleisten.

Testszenarien

Unser Pentest simuliert reale Angriffe und deckt potenzielle Schwachstellen in Ihrer IT Infrastruktur auf. So können Sie proaktiv handeln, Sicherheitslücken schließen und Ihre Daten sowie Netzwerke vor Cyberbedrohungen schützen. Vertrauen Sie auf unsere Expertise, um Ihre IT Sicherheit auf das nächste Level zu heben und langfristige Risiken zu minimieren.



✓ **Active Directory Pentesting**

Wir führen autorisiertes Active Directory Pentesting durch, um Fehlkonfigurationen und Angriffsvektoren in der Identitäts- und Zugriffsinfrastruktur aufzudecken (z. B. laterale Bewegungen, Persistenz, Domänenübernahme). Ziel: Risiken priorisieren und konkrete Gegenmaßnahmen empfehlen (Rechte, Härtung, Authentifizierung, Monitoring, Incident-Response).¹

✓ **Web Application Pentesting**

Wir führen autorisiertes Web-Application-Pentesting durch: automatisierte Scanner ersetzen keine menschliche Raffinesse - wir prüfen manuell auf Logikfehler und nach OWASP Top-10. Wir identifizieren und bewerten Risiken (z. B. Injections, XSS, Broken Access Control) Ziel: priorisierte Befunde und praxisnahe Gegenmaßnahmen (Input-Validierung, Zugriffskontrollen, Secure-Coding, Monitoring).¹

✓ **Red Teaming Engagements**

Wir führen autorisierte Red-Team-Engagements durch: zielgerichtete, facettenreiche Simulationen (u.a. Low-and-Slow, Social-Engineering, physische Zugriffstests und fortgeschrittene technische Methoden) zur Bewertung der Überlebensfähigkeit sowie der Effektivität von Sicherheits-teams und -prozessen. Ergebnis: priorisierte Erkenntnisse und umsetzbare Empfehlungen; Umfang und Regeln werden schriftlich vereinbart.¹

✓ **Wireless Network Penetration Testing**

Wir führen autorisiertes Wireless-Network-Pentesting durch: kontrollierte Simulationen zeigen, wie ein unsicherer Perimeter und schwache WLAN-Konfigurationen Zugang zu internen Systemen, Datenverlust und Gerätekompromittierung ermöglichen. Ergebnis: priorisierte Befunde und konkrete Gegenmaßnahmen (Verschlüsselung, Segmentierung, 802.1X, Monitoring).¹

¹Alle Tests nur mit schriftlicher Genehmigung und im Rahmen der Projektvereinbarung.

Pentest Verfahren

Wir wissen, dass jede Organisation einzigartige Anforderungen hat, wenn es um Pentests geht. Deshalb bieten wir eine Reihe von Pentest-Ansätzen an, die auf die spezifischen Anforderungen zugeschnitten sind.

White-Box Pentest

Ideal für Unternehmen, die Systeme oder Anwendungen umfassend prüfen wollen. Mit vollem Zugriff auf Quellcode, Dokumentation und Infrastruktur identifizieren unsere Experten Schwachstellen, verbessern die Codequalität und liefern priorisierte, umsetzbare Maßnahmen. Voraussetzung: Vollständige Netzwerkinfrastruktur.



Grey-Box Pentest

Effizient, praxisnah, aussagekräftig.

Unser Grey-Box-Ansatz kombiniert gezielte Vorinformationen mit realistischen Angriffsszenarien. So identifizieren unsere Experten Schwachstellen schnell und effektiv, ohne auf vertrauliche Daten zugreifen zu müssen. Ideal für Unternehmen, die ihre Systeme und Anwendungen zügig und realitätsnah prüfen wollen.



Black-Box Pentest

Unser Black-Box-Ansatz testet die Fähigkeit Ihres Unternehmens, Angriffe zu erkennen und darauf zu reagieren. Ohne Vorwissen über Systeme oder Anwendungen simulieren unsere Experten reale Angriffe, führen eigenständige Aufklärung durch und decken verborgene Schwachstellen auf. So verbessern Sie gezielt Ihre Sicherheitslage und schützen kritische Ressourcen.



White-Box Pentest

Tiefgehende Sicherheitsanalyse Ihrer Systeme -

Beim White-Box Pentest erhalten unsere Experten vollen Zugang zu Dokumenten und Quellcode, arbeiten eng mit Entwicklern zusammen und verbessern so Sicherheit und Codequalität. Eine vollständige Netzwerkinfrastrukturübersicht ist Voraussetzung. Die Dauer hängt von der Projektkomplexität ab. Ideal für Unternehmen, die interne Sicherheitslücken erkennen und gezielt Sicherheitsverbesserungen umsetzen wollen.

Active Directory Security

Vollzugriff auf AD-Server, GPOs, Konten und Einstellungen zur Aufdeckung von Fehlkonfigurationen und Privilegieneskalationen.



Web Application Security

Überprüfen Sie den Quellcode, die Konfigurationsdateien und die Authentifizierungsmechanismen, um Sicherheitslücken (angelehnt an OWASP Top 10 Security Risks) zu identifizieren.



Wi-Fi Network Security

Testen Sie das interne WLAN-Netzwerk auf Verschlüsselung, Fehlkonfigurationen und schwache Sicherheit durch modernste Angriffsvektoren.



Grey-Box Pentest

Kombinierte Analyse für tiefere Einblicke -

Der Grey-Box Pentest bietet eine ausgewogene Lösung zwischen externen und internen Angriffen. Tester erhalten vorab gezielte Informationen wie Benutzeranmeldedaten oder Netzwerkinfrastruktur, um Schwachstellen schneller zu identifizieren, ohne auf vertrauliche Daten zugreifen zu müssen.

Dieser Test ist zeitlich effizienter als ein White-Box Pentest und eignet sich für eine schnelle, gründliche Analyse von Anwendungen und IT Infrastrukturen. Er bietet Unternehmen eine realistische und effektive Sicherheitsprüfung, um Risiken zu erkennen und zügig zu beheben.

Active Directory Security

Testen Sie mit begrenzten Kenntnissen und identifizieren Sie Misconfiguration für die Ausweitung von Berechtigungen.



Web Application Security

Suchen Sie nach bekannten Schwachstellen mit Zugriff auf Teilinformationen (z. B. exponierte Dienste, veraltete Komponenten).



Wi-Fi Network Security

Testen Sie segmentierte oder Gastnetzwerke auf Verschlüsselungsschwächen oder Fehlkonfigurationen.



Black-Box Pentest

Realistischer Schutz vor externen Bedrohungen -

Beim Black-Box-Test simulieren wir externe Angreifer ohne Vorwissen (nur Domain/IP). Tester führen eigenständige Aufklärung (mehrere Arbeitstage) durch und identifizieren verborgene Schwachstellen.

Active Directory Security

Externe Penetrationstests zum Scannen nach exponierten AD-Diensten, schwachen Anmeldedaten und falsch konfigurierten Zugangspunkten.



Web Application Security

Penetrationstests zur externen Suche nach offenen Ports, Schwachstellen wie SQLi oder XSS und Fehlkonfigurationen im Web.



Wi-Fi Network Security

Externe WLAN-Tests zur Überprüfung auf schwache Verschlüsselung, SSID-Sichtbarkeit und Netzwerksicherheit.



Unser Pentest Prozess

Wir von CYQUEO glauben an einen systematischen und umfassenden Ansatz für Pentests.

Daher unser vollständiger Pentest-Prozess:

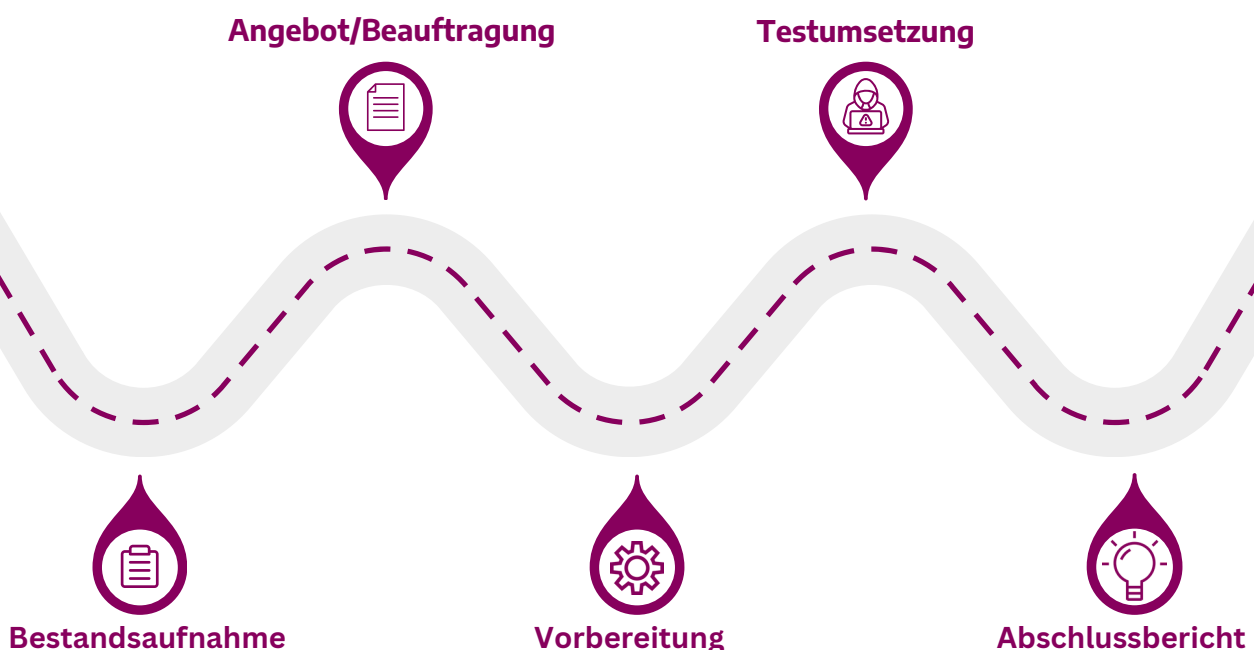
1. Bestandsaufnahme: Wir beginnen mit einem Erstgespräch, um die individuellen Bedürfnisse und spezifischen Anforderungen Ihrer Organisation für das Pentesting-Projekt zu verstehen.

2. Angebot & Beauftragung: Unser Vertrieb erstellt Ihnen ein individuelles Angebot in denen der Umfang, der Zeitplan und die erwarteten Ergebnisse des Projekts dargelegt sind.

3. Vorbereitung: Unsere Techniker erstellen einen detaillierten Pentesting-Plan, der potenzielle Schwachstellen, Testmethoden und einen Zeitplan identifiziert, um eine möglichst effiziente Nutzung der Ressourcen zu gewährleisten.

4. Testumsetzung: Unser erfahrenes Team aus Hackern führt Tests mit den neuesten Tools und Techniken durch, um potenzielle Sicherheitslücken zu identifizieren. Wir geben regelmäßiges Feedback während des gesamten Tests.

5. Abschlussbericht: Wir erstellen einen umfassenden und detaillierten Bericht über die Ergebnisse des Penetrationstests, einschließlich einer Analyse der identifizierten Schwachstellen und empfohlenen Abhilfemaßnahmen.



Abschlussbericht

Unser Abschlussbericht fasst alle relevanten Aspekte des Pentest kompakt zusammen – von den angewandten Testmethoden und dem definierten Scope bis zu den eingesetzten Tools.

Alle identifizierten Schwachstellen werden technisch präzise beschrieben und mit klaren, praxisnahen Handlungsempfehlungen ergänzt. Die Risikobewertung erfolgt nach anerkannten Standards wie der OWASP-Methode und berücksichtigt Eintrittswahrscheinlichkeit sowie Auswirkung.

Das Ergebnis: ein klar strukturierter Bericht, der Risiken transparent darstellt und gezielte Maßnahmen zur Stärkung Ihrer IT-Sicherheit aufzeigt.

Risikobewertung				
Auswirkung	HOCH	Mittel	Hoch	Kritisch
	MITTEL	Gering	Mittel	Hoch
	GERING	Informativ	Gering	Mittel
			Wahrscheinlichkeit	

**Starten Sie jetzt in eine sicherere Zukunft und
sichern Sie Ihre Organisation proaktiv ab!**

Kontaktieren Sie uns unter:
info@cyqueo.com oder direkt unter +49 89 45 220 94 0

