Penetrationstests

Unverzichtbares Werkzeug für die Cybersicherheit

Herausforderung & Lösung

Penetrationstests, oft als Pentests bezeichnet, sind eine essentielle Komponente in der Cyberabwehrstrategie eines Unternehmens. Sie simulieren Cyberangriffe auf IT-Systeme, Anwendungen oder Netzwerke, um Schwachstellen und Sicherheitslücken zu identifizieren sowie zu beheben, bevor Angreifer sie ausnutzen können. Unternehmen können so ein realistisches Bild ihrer Sicherheitsanfälligkeiten erhalten und effektive Gegenmaßnahmen entwickeln.

Wichtig ist, dass Penetrationstests unter Einhaltung ethischer Richtlinien und in Übereinstimmung mit den geltenden Gesetzen durchgeführt werden, um rechtliche Probleme zu vermeiden.

Penetrationstests bieten zahlreiche Vorteile. Sie helfen nicht nur, unbekannte Schwachstellen zu entdecken, sondern auch, die Wirksamkeit bestehender Sicherheitsmaßnahmen zu bewerten und das Bewusstsein für Cybersicherheit im Unternehmen zu schärfen. Darüber hinaus stärken die Test das Vertrauen von Kunden und Partnern in die Sicherheitspraktiken von Unternehmen.

Durch die regelmäßige Durchführung können Sie Ihre Cyber-Sicherheitsstrategien kontinuierlich verbessern und sich an die sich ständig ändernde Landschaft von Cyberbedrohungen anpassen.

Penetrationstests sind ein unverzichtbares Werkzeug, das dazu beiträgt, die digitale Umgebung sicherer zu machen und das Vertrauen in die Technologie zu stärken, die unser Leben und unsere Wirtschaft antreibt.

Unser Angebot

Bei GISA wurden die Penetrationstests durch **intelligente Automatisierung** und den **Einsatz von künstlicher Intelligenz** so weiterentwickelt, dass auch komplexe Sicherheitslücken effizienter identifiziert und behoben werden können. Unsere Kombination aus manuellen Techniken und automatisierten Tools erhöht die Effektivität von Pentests und hilft Unternehmen dabei, ihre Cyberabwehrstrategien besser zu stärken.

Der Prozess eines Penetrationstests umfasst die Planung und Vorbereitung, die Durchführung der Tests, die Analyse der Ergebnisse und die Erstellung eines Berichts, der die gefundenen Schwachstellen und Empfehlungen zur Behebung aufzeigt.

Es gibt verschiedene Arten von Penetrationstests, darunter **Black Box, White Box** und **Grey Box Tests**, die jeweils unterschiedliche Ansätze und Kenntnisse über das Zielobjekt bieten. Die Wahl des geeigneten Test-Szenarios hängt von den spezifischen Anforderungen und Zielen Ihres Unternehmens ab. Jedes Szenario bietet seine eigenen Vor- und Nachteile und wird entsprechend Ihrer individuellen Bedürfnisse angepasst.

Der Aufwand bewegt sich je nach Umfang und Komplexität der Anwendungen bzw. der Art des Test-Szenarios zwischen 10.000 EUR und 45.000 EUR. Die Aufwandschätzungen erfolgen auf Stundenbasis.

Wir beraten Sie gern!

Die Penetrationstest-Szenarien

Blackbox-Test

Beim Blackbox-Test haben unsere Penetrationstester keinerlei Kenntnisse über Ihre interne Infrastruktur oder den Quellcode der Anwendung. Dies simuliert einen Angriff von außen und ermöglicht es, die Sicherheit einer Webanwendung aus Sicht eines externen Angreifers zu bewerten. Der Tester führt verschiedene Angriffstechniken durch, um Schwachstellen zu identifizieren und auszunutzen.

Aufwand: 10.000 EUR bis 25.000 EUR, abhängig von Größe und Komplexität der Anwendung/zu prüfenden Infrastruktur— Schätzung erfolgt auf Stundenbasis.

Whitebox-Test

Im Gegensatz dazu beinhaltet der Whitebox-Test eine detaillierte Kenntnis über die interne Struktur Ihres Unternehmens und den Quellcode der Anwendung. Dies ermöglicht eine gründliche Analyse der Sicherheitsmechanismen von innen heraus. Unsere Tester können potenzielle Schwachstellen identifizieren, indem sie den Quellcode überprüfen, manuelle Tests durchführen und automatisierte Tools einsetzen.

Aufwand: 25.000 EUR bis 45.000 EUR, berücksichtigt Umfang des Quellcodes & Komplexität der Anwendung — Schätzung erfolgt auf Stundenbasis.

Greybox-Test

Der Greybox-Test kombiniert Elemente von Blackbox- und Whitebox-Tests, indem unseren Testern teilweise Kenntnisse über Ihre interne Infrastruktur zur Verfügung gestellt werden. Dies kann beispielsweise Zugriff auf bestimmte Teile des Quellcodes oder begrenzte Netzwerkinformationen umfassen. Der Greybox-Test bietet eine ausgewogene Perspektive und ermöglicht es, sowohl externe als auch interne Schwachstellen zu identifizieren.

Aufwand: 20.000 EUR bis 35.000 EUR, berücksichtigt den Umfang der bereitgestellten internen Informationen und Komplexität der Anwendung— Schätzung erfolgt auf Stundenbasis.

Ihre Vorteile

Penetrationstests bieten eine umfassendere Sicherheitsbewertung im Vergleich zu Schwachstellenscans. Hier sind einige wichtige Vorteile zusammengefasst:

+ **Identifikation von Exploits:** Penetrationstests ermöglichen es, potenzielle Schwachstellen nicht nur zu identifizieren, sondern auch zu bewerten, ob diese tatsächlich ausgenutzt werden können. Während ein Schwachstellenscan nur auf bekannte Schwachstellen überprüft, können Penetrationstests auch unbekannte Schwachstellen aufdecken und deren Ausnutzbarkeit testen.
+ **Realistische Angriffsszenarien:** Penetrationstests simulieren reale Angriffe und helfen dabei, die Auswirkungen einer erfolgreichen Kompromittierung besser zu verstehen. Im Gegensatz dazu führen Schwachstellenscans lediglich automatisierte Tests durch, ohne den Kontext eines potenziellen Angriffs zu berücksichtigen.
+ **Manuelle Überprüfung:** Penetrationstests beinhalten oft manuelle Überprüfungen durch erfahrene Sicherheitsexperten, die potenzielle Schwachstellen identifizieren können, die automatisierte Tools möglicherweise übersehen. Diese menschliche Expertise ermöglicht eine gründlichere Analyse der Sicherheitslage.
+ **Compliance-Anforderungen:** Viele Branchen und Regulierungsbehörden fordern regelmäßige Penetrationstests als Teil ihrer Compliance-Anforderungen. Diese Tests gewährleisten nicht nur die Einhaltung von Vorschriften, sondern auch einen umfassenden Schutz vor potenziellen Angriffen.
+ **Ganzheitliche Sicherheitsbewertung:** Penetrationstests bieten eine ganzheitliche Sicherheitsbewertung, die nicht nur technische Schwachstellen, sondern auch organisatorische und prozessuale Schwachstellen berücksichtigt. Dadurch erhalten Unternehmen einen umfassenderen Einblick in ihre Sicherheitslage.

Vertrauen Sie dem Experten-Team von GISA! Mit der Weiterentwicklung herkömmlicher Tests durch den Einsatz von intelligenter Automatisierung, Künstlicher Intelligenz sowie die Kombination aus manuellen und automatisierten Tools bieten Pentests mit GISA eine besonders hohe Effizienz und Effektivität!

Ihr Kontakt: Wir beraten Sie gern. | Telefon +49 800 7000 585* | kontakt@gisa.de | www.gisa.de * kostenfrei im dt. Festnetz