Penetrationstests für mobile IoT-Geräte.

Schützen Sie Ihr Produkt und Ihre Reputation.

www.tuv.com/pentest

TÜVRheinland®
Genau. Richtig.

UNSER LEISTUNGSUMFANG

- Mithilfe eines strukturierten Testansatzes überprüfen wir Ihr mobiles IoT-Gerät auf Sicherheitslücken, die von Hackern ausgenutzt werden könnten.
- Wir bieten einen Überblick über die Schwachstellen, die die Sicherheit Ihres IoT-Geräts gefährden können.
- Wir geben Ihnen Empfehlungen zur Verbesserung der Sicherheit Ihres IoT-Geräts.
- Zusätzlich zu den Standard-Kommunikationskanälen umfasst unser Test auch die Interaktion mit 2G/3G/4G- und bald auch 5G-Netzwerkumgebungen.

IHRE VORTEILE

- Mit Zuhilfenahme automatisierter und manueller Tests geben wir Ihnen Aufschluss über bekannte und unbekannte Schwachstellen in Ihrem Produkt.
- Sie lernen die Angriffsflächen und Schwachstellen Ihres Produkts kennen und können dessen Sicherheit und Zuverlässigkeit auf dieser Grundlage verbessern.
- Sie erkennen die Sicherheitslücken in Ihrem Produkt, bevor sie von einem Hacker ausgenutzt werden können. Damit haben Sie die Möglichkeit, Schwachstellen zu beseitigen und die Reputation Ihrer Marke zu schützen.
- Unser Bericht enthält eine Zusammenfassung für Entscheider und detaillierte Informationen für Systemingenieure.
- Wir unterstützen Sie umfassend bei der Entwicklung und dem Betrieb eines sichereren Mobilgeräts und helfen Ihnen, Ihre Daten und Ihre Integrität zu schützen.

UNSERE KOMPETENZ

- Über 20 Jahre Erfahrung mit Penetrationstests
- Wir führen jedes Jahr weltweit mehr als 1.000 Penetrationstests durch.
- Sie erhalten einen objektiven Überblick über Ihre Sicherheitsdefizite und wir stehen Ihnen auch im Anschluss mit den passenden Empfehlungen zur Behebung zur Seite.
- Unsere Sicherheitsprüfer sind auf Penetrationstests spezialisiert. Darüber hinaus besitzen sie anerkannte Branchen-Zertifizierungen, wie z. B. OSCP, OSCE. Dies garantiert eine hohe Qualität der Testergebnisse.
- Entwicklungslabor für Konformitätsprüfungen und interne Testsysteme für lange Reichweiten (2G bis 5G) sowie für kurze Reichweiten (Wi-Fi, BT, BT-SIG, LoRa usw.).

UNSERE METHODIK

1. KICK-OFF UND ANALYSEAUFBAU

Wir beginnen unser Projekt mit einem Kick-off, in dessen Rahmen wir den genauen Umfang des Projekts definieren, die Voraussetzungen für die Analyse festlegen, um nützliche Ergebnisse zu erhalten, sowie den ordnungsgemäßen Aufbau der Analyse besprechen.

2. EINRICHTUNG DES GERÄTS UND GRUNDLEGENDE PRÜFUNG AUF FUNKTIONSFÄHIGKEIT

Wir richten das IoT-Gerät in unserem Labor ein und führen vor Beginn der Analyse einige grundlegende Funktionstests durch, um zu prüfen, ob das Gerät erwartungsgemäß funktioniert.

3. INFORMATIONEN SAMMELN

Wir beginnen die Analyse Ihres Geräts mit dem Einholen von Informationen. In dieser Phase sammeln wir verschiedene Informationen über das System und seine typische Betriebsumgebung. Dies hilft uns, das Produkt und seine Angriffsflächen zu erfassen.

4. ERMITTLUNG VON SCHWACHSTELLEN

In dieser Phase beginnen wir mit der Suche nach potenziellen Schwachstellen und Sicherheitslücken. Dies umfasst bekannte Schwachstellen, die wir durch automatisierte Scans erfassen und unbekannte Schwachstellen, die wir mit manuellen Tests ermitteln.

5. AUSNUTZUNG VON SCHWACHSTELLEN

Sobald wir potenzielle Schwachstellen identifiziert haben, beginnen wir, sie auszunutzen. Dabei ist das Ziel, falsch-positive Schwachstellen auszuschließen und die mit einer Schwachstelle verbundenen Risiken zu verstehen. Dieser Prozess liefert außerdem weitere Informationen über das Produkt.

6. BERICHT

Im nächsten Schritt dokumentieren wir unsere Ergebnisse in einem offiziellen TÜV Rheinland-Bericht. Der Bericht enthält eine Kurzfassung sowie detaillierte Informationen zu den gefundenen Schwachstellen. Darüber hinaus enthält er Empfehlungen zu Strategien, mit denen Sicherheitslücken beseitigt werden können.

TÜV Rheinland i-sec GmbH
Am Grauen Stein
51105 Köln
pen_cellular_testing@tuv.com
www.tuv.com/pentest

TÜVRheinland®
Genau. Richtig.