TÜVRheinland®
Genau. Richtig.

Mobile Applikationen

Es wird eine mobile Applikation (bspw. Messaging-, Spiele- oder Online-Banking-Apps) auf häufig ausgenutzte Schwachstellen untersucht. Dabei werden manuelle und automatisierte Tests durchgeführt, um Schwachstellen zu identifizieren. Gefundene Schwachstellen werden dokumentiert und Empfehlungen zur Behebung gegeben. Vor der Analyse werden der Untersuchungsbereich und die Schwerpunkte festgelegt. Die Untersuchung basiert auf dem OWASP Mobile Application Security Testing Guide und besteht aus einer passiven und einer aktiven Phase.

Bitte beachten sie, dass Mobile Applikationen, die nur auf speziellen Managed-Devices laufen, hiervon ausgenommen sind. Bitte kontaktieren Sie uns über das Kontaktformular, wenn Sie die Analyse einer solchen Applikation benötigen.

Leistungsbeschreibung und Prüfumfang

In dieser Position sollen die im Geltungsbereich angegebenen mobilen Applikationen auf Schwachstellen untersucht werden, die von Angreifern häufig für Angriffe ausgenutzt werden oder deren Angriffe erleichtern können. Mit Hilfe von manuellen und automatisierten Tests wird die mobile Applikation im zeitlichen Rahmen der Analyse strukturiert auf Schwachstellen hin untersucht. Gefundene Schwachstellen werden in einem TÜV Rheinland-Bericht dokumentiert und Empfehlungen zur Behebung der Schwachstellen gegeben.

In einem Vorgespräch wird der Untersuchungsbereich der Sicherheitsanalyse der mobilen Applikation näher spezifiziert und ggf. Schwerpunkte definiert. Hierzu gehören sowohl die zu untersuchende mobile Applikation in einer definierten Version als auch relevante Benutzerzugänge und die Kommunikation mit API-Endpunkten zur Interaktion mit der mobilen Applikation. Anschließend wird die mobile Applikation auf Basis des OWASP Mobile Application Security Testing Guide hin untersucht. Allgemein lässt sich das Vorgehen in eine passive und eine aktive Phase untereilen.

! Kommuniziert die mobile Applikation mit einer Webapplikation/Web-API, ist der Penetrationstest der Webapplikation nicht im Umfang enthalten. Soll die Webapplikation mit untersucht werden, empfehlen wir ihnen zusätzlich das Pentest M-Paket unter Webapplikationen zu bestellen.

Im Folgenden werden die einzelnen Arbeitsschritte der passiven (Informationssammlung) sowie aktiven (Identifizierung von Schwachstellen und Ausnutzung von Schwachstellen) Phasen beschrieben.

Schritt 1: Passive Phase

Innerhalb der passiven Phase interagiert TÜV Rheinland mit der zu untersuchende mobile Applikation. Hierbei gewinnt TÜV Rheinland einen Überblick über die bereitgestellten fachlichen und technischen Funktionen der mobilen Applikation. Die passive Phase wird durch den Einsatz von speziell vorbereiteten (gerooteten/gejailbreakten) mobilen Endgeräten sowie Tools, wie z. B. Intercepting-Proxies oder Tools zum Enumerieren von Informationen unterstützt.

Das Ziel der passiven Phase ist die Ermittlung von möglichst vielen und detaillierten Informationen, die TÜV Rheinland helfen, die Angriffsfläche besser einzuschätzen, um in der folgenden aktiven Phase die mobile Applikation möglichst effizient angreifen zu können.

Schritt 2: Aktive Phase

In dem zweiten Schritt, der aktiven Phase, wird die im Geltungsbereich befindliche mobile Applikation unter anderem auf Schwachstellen untersucht, die den OWASP Mobile Top 10 zuzuordnen sind:

- M01:2016 – Falsche Nutzung Plattform-spezifischer Merkmale (Improper Platform Usage)
- M02:2016 – Unsichere lokalen Datenspeicherung (Insecure Storage Data)
- M03:2016 – Unsichere Kommunikationsprotokolle (Insecure Communication)
- M04:2016 – Unsichere Authentifizierungsverfahren (Insecure Authentication)
- M05:2016 – Unsichere kryptographische Verfahren (Insufficient Cryptography)
- M06:2016 – Unsicheres Berechtigungsmanagement (Insecure Authorization)
- M07:2016 – Unzureichende Qualität des Quellcodes (Client Code Quality)
- M08:2016 – Unzureichender Schutz gegen Programmflussänderungen (Code Tampering)
- M09:2016 – Unzureichender Schutz gegen Reverse Engineering (Reverse Engineering)
- M10:2016 – Überflüssige Funktionalitäten (Extraneous Functionality)

Bei der Sicherheitsanalyse untersucht TÜV Rheinland die mobile Applikation während der Laufzeit auf entsprechenden Testgeräten, z. B. iPhone oder Android-basiertem Smartphone, welche ebenfalls über einen Jailbreak verfügen können. Bei dieser Analyse werden sowohl automatisierte Verfahren als auch manuelle Analysen angewendet. Hierbei können exemplarisch folgende Schwachstellen identifiziert werden:

- Manipulation von übertragenen Daten über eine Man-in-the-Middle-Position zwischen mobiler Applikation und Kommunikationspartner aufgrund einer fehlenden oder unzureichenden Authentifizierung.
- Identifikation und Extraktion von vertraulichen, z. B. personenbezogenen Daten aufgrund der unsicheren Speicherung auf dem lokalen Dateisystem.
- Umgehen von Authentifizierungs- oder Autorisierungsüberprüfungen aufgrund einer unzureichenden Validierung von Benutzereingaben.
- Externes Auslösen von Funktionen der untersuchten mobilen Applikation aufgrund von lokalen exponierten Diensten aus Sicht einer weiteren installierten schadhaften mobilen Applikation.

Des Weiteren untersucht TÜV Rheinland die mobile Applikation mit Hilfe von Reverse-Engineering auf Schwachstellen bei der Datenverarbeitung, z. B. unzureichender Überprüfung von Benutzereingaben oder Schwachstellen im Authentifizierungs- und Autorisierungsmanagement.

Die identifizierten Schwachstellen werden innerhalb des TÜV Rheinland Berichts dokumentiert.

! Die Testabdeckung hängt von der Komplexität der mobilen Applikation und dem investierten Aufwand für den Test ab. Je höher die Anzahl der Testtage, desto mehr Tests und Angriffsvarianten können berücksichtigt werden und desto größer ist die Abdeckung der getesteten Funktionen innerhalb der mobilen Applikation(en).