Secure App

Immer mehr Anbieter stellen Apps zur Verfügung, um über die mobilen Applikationen eine übersichtliche und vereinfachte Nutzung ihrer Dienste anbieten zu können. Für viele Verbraucher ist es zunehmend schwierig, vertrauenswürdige Apps zu erkennen, bei denen sie ihre Daten in Sicherheit wissen.

Wir machen Ihre App sicher

Um die Sicherheit Ihrer App für Ihre Nutzer sichtbar machen zu können, prüfen unsere Sicherheitsexperten Ihre Applikation manuell oder toolbasiert auf mehrere Faktoren und stellen Ihnen einen umfassenden Prüfbericht inklusive Maßnahmenkatalog, ein persönliches Zertifikat sowie das Siegel der usd zur Verfügung.

Zertifizierung Ihrer App

Die Zertifizierung Ihrer App erfolgt auf Grundlage und nach Vorgaben des NIST SP800-163. Die Anforderungen des internationalen Sicherheitsstandards der Kreditkartenindustrie (PCI DSS) sowie die Handlungsempfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) sowie des Open Web Application Security Project (OWASP) werden vollständig bei der Überprüfung Ihrer Applikation berücksichtigt.

Unsere Verfahren

Ein Großteil der Sicherheitsprobleme entsteht durch kritische Schwachstellen in den Applikationen. Besonders im Feld der mobilen Anwendungen werden Sicherheitsrisiken gerne unterschätzt, da die Möglichkeiten der Eingaben begrenzt erscheinen. Wir kombinieren statische mit dynamischen Analyseverfahren in einem sogenannten „Whitebox"-Ansatz für Ihre Android- oder iOS-App. Unsere Sicherheitsexperten identifizieren die Schwachstellen während der Benutzung Ihrer Anwendung. Die Daten sowie der Quellcode der Applikation stehen ihnen hierbei zur Verfügung. Wir überprüfen die Einhaltung von anerkannten Secure Coding Guidelines und Best Practices. Unsere Verfahren unterstützen Anwendungen für die Android- und iOS-Plattform und damit einhergehend für Java, Objective-C und Swift.

Mobile App Pentest

usd Pentests bieten Ihnen die Möglichkeit, Ihre Anwendung individuell von einem unserer Sicherheitsexperten überprüfen zu lassen. Zur Informationsbeschaffung nutzt er professionelle Werkzeuge und versucht gezielt, individuell und erfinderisch, Schwachstellen über die mobile Anwendung auszunutzen. Dadurch erlangt der Sicherheitsexperte tiefere Einblicke in die Entwicklersicht und erkennt effizient Schwachstellen in der Applikation. Mithilfe des Whitebox Pentests liefern wir Ihnen zuverlässige Ergebnisse, die wir gemeinsam mit konkreten Verbesserungsvorschlägen für Sie in Berichtsform übergeben.

Code-Analyse

Die Analyse des Quellcodes wird unterstützend zum Mobile App Pentest durchgeführt. Wir betrachten Teilbereiche Ihrer Applikation und untersuchen den Code auf Schwachstellen. Die Überprüfung wird anhand des anerkannten Vorgehensmodells von OWASP durchgeführt.

Unser Vorgehensmodell

Kick-Off

Die Vorbereitung der Überprüfung erfolgt im Rahmen eines Kick-off Meetings remote per Telefon- oder Webkonferenz oder auf Wunsch bei Ihnen vor Ort mit den technischen und organisatorischen Verantwortlichen Ihres Unternehmens. Hierbei wird die zu prüfende Applikation spezifiziert, notwendige Zugriffswege abgestimmt, Ansprechpartner und Eskalationswege definiert, sowie der Ablauf der Überprüfung im Detail gemeinsam besprochen.

Manual Research

Die im Vorfeld zur Verfügung gestellte Anwendung und der Quellcode werden mit statischen und dynamischen Analyseverfahren auf potentielle Schwachstellen untersucht. Dabei werden unterschiedliche Facetten einer mobilen Anwendung, wie zum Beispiel der Anwendungsserver, die lokal auf dem Gerät gespeicherten Daten und Seitenkanalangriffe, betrachtet.

Exploitation

In dieser Phase wird versucht, die identifizierten Schwachstellen auszunutzen, um reale Angriffsszenarien zu entwickeln oder auf sensible Daten zuzugreifen. Eine potentielle Schwachstelle kann sich hier als falsch-positiv herausstellen - d.h. dass bei erneuter Betrachtung keine Schwachstelle festgestellt werden kann. Nur verifizierte Schwachstellen werden in den abschließenden Bericht aufgenommen und entsprechend ihrer Kritikalität eingestuft.

Report

Sie erhalten einen umfassenden Bericht bestehend aus einer Executive Summary und einem Technical Report. Kritikalität von Findings und Eintrittsrisiken werden bewertet und die Schwachstellen anhand eines Angriffsbeispiels oder durch Code-Ausschnitte erläutert. Eine entsprechende Maßnahmenempfehlung wird ebenfalls ausgesprochen.

Remediation

In dieser Phase erfolgt die Beseitigung der identifizierten Abweichungen bzw. Schwachstellen durch Ihr Unternehmen. Bei Bedarf werden Sie hier durch unsere erfahrenen Berater unterstützt.

Optionale Nachprüfung

Sie haben die Möglichkeit, nach Durchführung der Remediation eine Nachprüfung durch uns durchführen zu lassen. Hierbei überprüfen wir die Wirksamkeit Ihrer Maßnahmen und passen den Ergebnisbericht entsprechend an.

Preis/Umfang

Der Umfang dieser Leistung wird individuell bestimmt. Er ist beispielsweise abhängig vom jeweiligen Untersuchungsobjekt. Kontaktieren Sie uns! Gerne erstellen wir Ihnen ein individuelles Angebot.

Mit starkem Partner usd

Experten kennen die usd AG als einen der führenden Anbieter von technischen Sicherheitsanalysen in Deutschland. Das Sicherheitsteam der usd AG führt jährlich tausende automatisierte Schwachstellen-Scans sowie hunderte manuelle Pentests von IT-Systemen und Anwendungen durch. Die Sicherheitsexperten der usd AG sind dem Code of Ethics des EC-Councils verpflichtet, verfügen über zahlreiche Sicherheitszertifizierungen und umfangreiche Erfahrungen aus internationalen Projekten. Die usd AG ist eines der wenigen deutschen Unternehmen, das durch das PCI Security Standards Council (PCI SSC) autorisiert ist, europaweit Sicherheitsprüfungen gemäß den Standards PCI DSS, PCI PA-DSS, PCI P2PE und PCI 3DS durchzuführen.

Ihr persönliches Zertifikat

Wir orientieren uns bei der Bewertung Ihres Pentestergebnisses an den Sicherheitsvorgaben des Open Web Application Security Projects (OWASP). Erfüllen Sie mit Ihrem Pentestergebnis die Anforderungen, bestätigen wir Ihnen dies gerne in einem persönlichen Zertifikat. So können Sie auch Dritten Ihren Anspruch an Sicherheit demonstrieren.

Dieses Produktblatt hat Gültigkeit, sofern keine aktuellere Version veröffentlicht wurde. *Erstellungsdatum: 14.01.2020*

usd AG
Frankfurter Straße 233, Haus C1 | 63263 Neu-Isenburg
www.usd.de
Telefon: +49 6102 8631-190 | E-Mail: vertrieb@usd.de
PGP oder S/MIME für verschlüsselte Kommunikation.