ZIMPERIUM®

5 Schritte zur Sicherung von mobilen Banking-Apps

In den letzten Jahren ist die Nutzung von Mobilgeräten für Bankgeschäfte allgegenwärtig geworden. Egal, ob wir einen Scheck einreichen, eine Rechnung bezahlen, Geld überweisen oder einfach nur den Kontostand überprüfen möchten – wir greifen immer häufiger zum Telefon.

Infolgedessen werden mobile Banking-Apps zu immer beliebteren Zielen für Cyberkriminelle und sowohl App-Anbieter als auch Verbraucher sind gefährdet. Für die Anbieter ist es wettbewerbsentscheidend, den Verbrauchern ein leistungsstarkes und einfaches mobiles Bankerlebnis zu bieten. Aber diese mobilen Bankgeschäfte müssen auch sicher sein, um die Verbraucher zu schützen, teure Geldstrafen zu vermeiden und Betrug zu verhindern. Um diese Anforderungen zu erfüllen, müssen die Anbieter einen fünfstufigen Ansatz verfolgen. Durch diese Schritte können Teams die nötige Reife erlangen, um ihre Apps und die sensiblen Daten und Backend-Dienste, auf die diese Apps zugreifen, möglichst effektiv zu schützen.

Schritt 1
Kodierungsrisiken vermindern

Um starke Schutzmaßnahmen einzurichten, müssen die Teams zunächst die Risiken ihrer Apps einschließlich der Frage, wo und wie sie angegriffen werden könnten, verstehen. Allzu oft denken Unternehmen jedoch erst kurz vor einer Veröffentlichung über die Sicherheit nach. So kann es beispielsweise sein, dass Penetrationstests erst dann durchgeführt werden, wenn der Code in die Produktion gehen soll, wodurch eine große Anzahl von Schwachstellen aufgedeckt wird. Leider birgt dieser Last-Minute-Ansatz nicht nur Risiken, sondern es ist in der Regel auch viel teurer und zeitaufwändiger, Schwachstellen zu beheben, je später der Code in den Entwicklungszyklus gelangt.

Wie Sie Erfolg haben

Sicherheitsanforderungen müssen vor, während und nach der Erstellung des Codes berücksichtigt und behandelt werden. Durch kontinuierliches Testen können Teams Probleme erkennen und während des gesamten Entwicklungszyklus beheben, welches zur Rationalisierung von Prozessen beiträgt und gleichzeitig die Sicherheit verbessert. Darüber hinaus können Teams durch die sichere Entwicklung von Apps von Anfang an das Risiko verringern und die Kosten, den Aufwand und die Verzögerungen vermeiden, die mit der Behebung von Schwachstellen zu einem späteren Zeitpunkt im Softwarelebenszyklus verbunden sind. Im Folgenden finden Sie einige Schlüssel zum Erfolg:

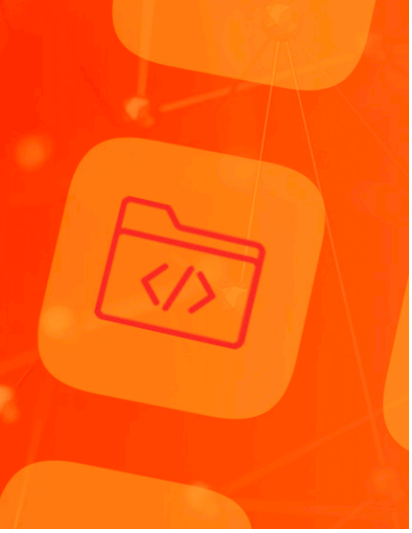
Nutzen Sie automatisierte Bewertungen. Wenn sich Teams ausschließlich auf manuelle Penetrationstests verlassen, wird die Entwicklung verlangsamt und die Effizienz der Mitarbeiter beeinträchtigt. Außerdem werden die Tests nicht so umfassend sein, wie sie sein müssten. Die Teams müssen automatisierte Funktionen nutzen, die sich in die Entwicklungsprozesse integrieren lassen, damit sie feststellen können, wo Risiken bestehen. Bei Verstößen gegen die Richtlinien sollte automatisch ein Ticket für die Entwickler erstellt werden, damit diese die Probleme beheben können.

Hüten Sie sich vor hybriden App-Entwicklungsansätzen und Drittanbieter-Komponenten. Immer mehr Teams verwenden Sprachen oder Programmier-Frameworks, um hybride Apps zu erstellen, d. h. eine Codebasis zu entwickeln, die sowohl auf iOS- als auch auf Android-Geräten funktioniert. Die Realität sieht jedoch so aus, dass diesen App-Frameworks viele der Sicherheitskontrollen fehlen, die in nativen Entwicklungsumgebungen verfügbar sind, sodass Teams diese Ansätze mit Bedacht einsetzen sollten. Auch Komponenten von Drittanbietern, egal ob sie proprietär oder Open Source sind, können Risiken bergen. Oftmals fehlt es den Entwicklern dieser Komponenten an den erforderlichen Fachkenntnissen und dem Fokus auf Sicherheit.

Wie Zimperium helfen kann

Zimperium's zScan kann Entwicklern helfen, Risiken in den Binärdateien ihrer mobilen Banking-App zu erkennen. Mit zScan können Teams Datenschutz-, Sicherheits- und Compliance-Risiken identifizieren, bevor Apps für die Öffentlichkeit freigegeben werden. Die statische und dynamische Analyse von zScan identifiziert die spezifischen Risiken, die ein Angreifer ausnutzen könnte, einschließlich des Codes von Erstanbietern, der von Drittanbietern erstellten Apps und aller Komponenten von Drittanbietern innerhalb der App.

zSCAN™



Schritt #2
Schützen Sie Ihren Code

Heutzutage ist es für böswillige Akteure ein Leichtes, eine App aus einem App-Store herunterzuladen, sie zurückzuentwickeln, ausnutzbare Fehler und Schwachstellen zu finden und böswillige Aktivitäten, einschließlich Code-Injection, Piraterie und mehr, durchzuführen. So können Kriminelle beispielsweise eine App umkonfigurieren und neu verpacken, um sie in einer Phishing-Kampagne, die darauf abzielt, die Zugangsdaten eines Opfers zu stehlen, zu verwenden. Die Anbieter von mobilen Banking-Apps können es sich nicht mehr erlauben, dass ihre Apps für diese Art von Bedrohung anfällig sind.

Wie Sie Erfolg haben

Entwickeln Sie keine internen Sicherheitstools. Oft wählen interne Teams den Ansatz, Anwendungsabschirmungsfunktionen zu entwickeln, anstatt bewährte kommerzielle Lösungen zu kaufen. Diese Bemühungen können sehr kostspielig und zeitaufwendig sein, wenn es um die Bereitstellung und Wartung geht. Interne Entwicklungsteams mögen zwar über eine gewisse Sicherheitserfahrung und einen internen Kontext verfügen, doch die Realität sieht so aus, dass sie nicht das Fachwissen und die Ressourcen besitzen, um die Sicherheit während der gesamten Lebensdauer einer App selbst zu verwalten. Darüber hinaus entwickeln sich die Sicherheitstechnologien und die Techniken der Angreifer rasant weiter. Um Schritt zu halten, ist es unerlässlich, sich auf Experten, die nur auf die Sicherheit fokussiert sind, zu verlassen.

Setzen Sie App-Verschleierung und -Abschirmung für mobile Apps ein. Um der Gefahr einer Code-Kompromittierung entgegenzuwirken, müssen die Teams mobile Apps verschleiern und abschirmen. Die Verschleierung von mobilen Apps ist eine der wichtigsten Waffen, die Entwicklern und Sicherheitsteams zur Verfügung stehen. Durch den Einsatz fortschrittlicher Quellcode-Verschleierung können Teams es schwer und zeitaufwändig für potenzielle Angreifer machen, herauszufinden, wie der Code funktioniert. Teams müssen außerdem robuste Funktionen zur Abschirmung von Apps einrichten, damit ein Angreifer, der die eingesetzten Verschleierungstechniken umgeht, die Geschäftslogik nicht manipulieren oder umgehen kann, um Zugriff auf sensible Daten zu erhalten oder den Code zu verändern.

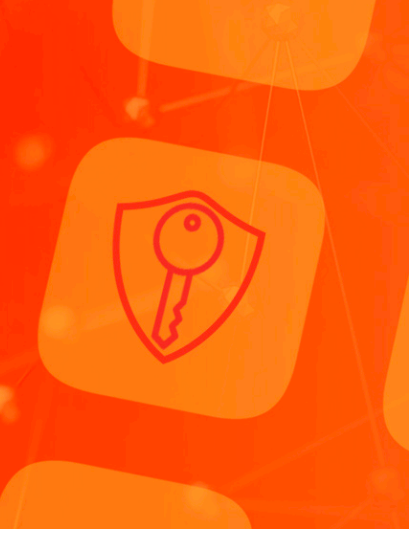
Verwenden Sie keine Open-Source- oder Freeware-Sicherheitstools. Diese grundlegenden Werkzeuge bieten einfach keinen ausreichenden Schutz, um Angreifern das Handwerk zu legen. So verfügen beispielsweise viele Open-Source-Tools über Schutzfunktionen, aber oft gibt es leicht zugängliche Gegenmaßnahmen, die diese Schutzmechanismen aushebeln, wie z. B. YouTube-Videos mit Schritt-für-Schritt-Anleitungen.

Verschaffen Sie sich einen Überblick über die Aktivitäten zur Bekämpfung von Manipulationen. Für die Teams ist es von entscheidender Bedeutung, dass sie feststellen können, ob der Schutz vor Manipulationen funktioniert. Allzu oft führen die Entwickler mobiler Banking-Apps jedoch lediglich Überprüfungen innerhalb der App durch, und wenn etwas Bösartiges entdeckt wird, wird eine voreingestellte Reaktion geliefert. So kann beispielsweise eine Transaktion einfach fehlschlagen oder dem Nutzer eine Nachricht anzeigen, dass die App aufgrund verdächtiger Aktivitäten nicht funktioniert. Leider bieten App-Anbieter mit diesen Ansätzen ein schlechtes Benutzererlebnis und haben keinen Überblick darüber, ob die Schutzmaßnahmen funktionieren. Daher ist es wichtig, die Aktivitäten zur Bekämpfung von Manipulationen zu überwachen, damit die Teams sicher sein können, dass die bestehenden Mechanismen funktionieren, oder die notwendigen Schritte unternehmen können, um zu reagieren, wenn dies nicht der Fall ist.

Wie Zimperium helfen kann

zShield von Zimperium bietet fortschrittliche Verschleierungs- und Anti-Manipulations-Funktionen, mit denen Teams ihren mobilen App-Code, ihr geistiges Eigentum und ihre privaten Daten abhärten und schützen können. Darüber hinaus bietet zShield Einblick in Manipulationsversuche.

zSHIELD™



Schritt #3
Sichern Sie Ihre Schlüssel

Die Verschlüsselung stellt eine wichtige Verteidigungslinie für Anbieter von mobilen Banking-Apps dar. Allzu oft sind kryptografische Schlüssel jedoch nicht vollständig gesichert, wodurch die Vorteile der Verschlüsselung geschwächt oder ganz aufgehoben werden können.

Wie Sie Erfolg haben

Nachfolgend sind einige kritische Ansätze und Überlegungen aufgeführt, um sicherzustellen, dass die Schlüssel ausreichend geschützt sind:

Verlassen Sie sich nicht auf einen intern entwickelten Schlüsselschutz. Um die Bereitstellung zu beschleunigen, können Teams einfach einen Hash über das Schlüsselmaterial laufen lassen, um es zu verbergen – aber dies reicht nicht aus. Alternativ können die Teams auch versuchen, ihre eigenen Kryptoalgorithmen zu verwenden. Bei diesen internen Ansätzen besteht die Gefahr, dass die Schlüssel von Malware oder Angreifern missbraucht werden, wodurch wichtige Daten und Dienste ungeschützt bleiben.

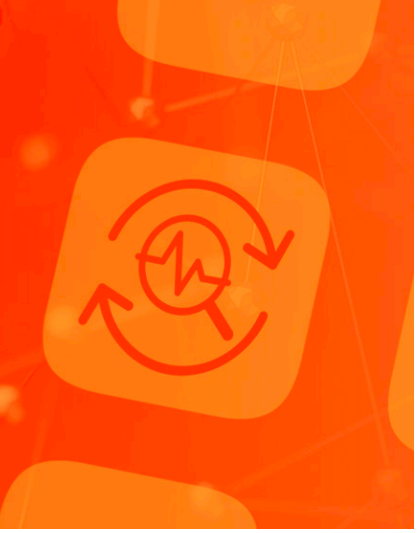
Setzen Sie keine hardwarebasierte Schlüsselsicherheit ein. Diese Ansätze sind mit verschiedenen Problemen verbunden, wie z. B. der fehlenden Unterstützung für bestimmte kryptografische Algorithmen oder Operationen, den unregelmäßigen (Sicherheits-)Aktualisierungszyklen und der Fragmentierung der Lösungen auf verschiedenen mobilen Plattformen. In den meisten Fällen können App-Entwickler von Drittanbietern nicht auf die hardwarebasierten Trusted Execution Environments oder Secure Enclave zugreifen, da diese vom Smartphone-Hersteller eingeschränkt werden. Standardmäßige Krypto-APIs, die in den mobilen Betriebssystemen verfügbar sind, machen Ihre Schlüssel ebenfalls angreifbar und ungeschützt, wenn das Gerät gerootet oder jailbroken ist oder einfach keine Sicherheitsupdates mehr erhält.

Verwenden Sie White-Box-Kryptographie. Um starke, widerstandsfähige und effiziente Schutzmechanismen für kryptografische Schlüssel einzurichten, müssen Entwickler von mobilen Banking-Apps White-Box-Kryptografie einsetzen. Mit dieser softwarebasierten Technologie werden kryptografische Algorithmen umgewandelt und verschleiert, so dass die Schlüssel nie im Klartext erscheinen und die Ausführungslogik nicht ausspioniert werden kann. Folglich können die Schlüssel nicht extrahiert werden, selbst wenn das Gerät kompromittiert wurde.

Wie Zimperium helfen kann

Mit Zimperium's zKeyBox können Teams eine starke Sicherheit für kryptografische Schlüssel einrichten, ohne sich mit den Herausforderungen interner oder hardwarebasierter Schutzansätze herumschlagen zu müssen. zKeyBox stellt sicher, dass Schlüssel verschleiert und verborgen werden und niemals im Klartext angezeigt werden, selbst wenn ein Angreifer die Kontrolle über die Ausführungsumgebung erlangt.

zKEYBOX™



Schritt #4
Laufzeit aktivieren Sichtbarkeit

Die Realität ist, dass es nahezu unendlich viele Geräte gibt, auf denen eine mobile Banking-App ausgeführt werden kann. Selbst die am sichersten konzipierte und codierte Anwendung kann durch anfällige Betriebssysteme, ungesicherte Netzwerke und Malware gefährdet sein.

Wie Sie Erfolg haben

Um Apps, die auf Benutzergeräten ausgeführt werden, erfolgreich zu schützen, müssen die Teams die folgenden Funktionen nutzen:

Aktivieren Sie Laufzeitsichtbarkeit. Es ist wichtig, Angriffe zu erkennen und zu stoppen, wenn sie stattfinden. Dies bedeutet, dass diese Angriffe auf dem Gerät des Endbenutzers während der Laufzeit erkannt werden müssen. In der Tat müssen Teams Stolperdrähte einrichten, die anzeigen, wenn eine App angegriffen oder manipuliert wird.

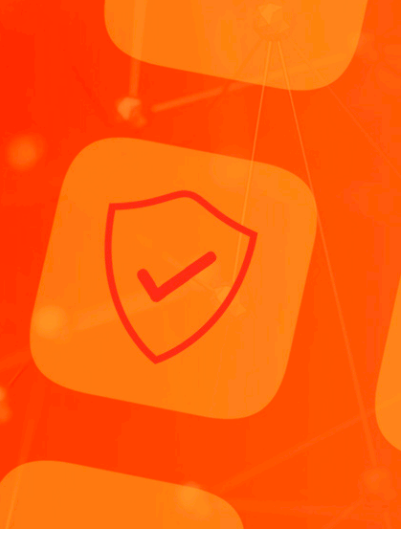
Kontinuierliche Modellierung von Bedrohungen. Es ist von entscheidender Bedeutung, dass die Teams die nötige Transparenz herstellen, um die Art der Umgebung, in der ein Gerät arbeitet, zu erkennen und diese Informationen kontinuierlich in die Bedrohungsmodellierung einfließen zu lassen. Dies ist wichtig, um die optimale Vorgehensweise zu bestimmen und die Sicherheit über den gesamten Lebenszyklus der Anwendung hinweg zu optimieren.

Aktivieren Sie Over-The-Air (OTA)-Updates. Entwickler von mobilen Banking-Apps benötigen eine Lösung, mit der sie ihre Sicherheitslage in Echtzeit aktualisieren können, um mit den sich entwickelnden Bedrohungen und Zero-Day-Angriffen Schritt zu halten. Ohne diese Möglichkeit müssen die Teams jedoch die Anwendung neu kompilieren und ihre Nutzer dazu bringen, ihre Apps ständig neu zu installieren oder zu aktualisieren, welches zeitaufwändig und unbequem sein kann.

Wie Zimperium helfen kann

zDefend von Zimperium bietet kontinuierliche Überwachung und Schutz und liefert effektive Funktionen zur Bedrohungsmodellierung. Mit dieser Lösung erhalten Teams die effektive Laufzeittransparenz, die sie benötigen, um Bedrohungen zu erkennen und zu stoppen, bevor es zu spät ist.

zDEFEND™



Schritt #5
Selbstschutz etablieren Apps

Um das ultimative Reifestadium zu erreichen, müssen Teams selbstschützende Apps einrichten. In erster Linie geht es darum, zwei potenziellen Bedrohungen zu begegnen:

Wie Sie Erfolg haben

Bei der Entwicklung ihrer mobilen Anwendungen müssen die Teams sicherstellen, dass sie die folgenden potenziellen Hindernisse vermeiden:

- **Ausschließliches Verlassen auf Anti-Malware-Schutzmaßnahmen.** Für viele Sicherheitsteams in Unternehmen ist der Schutz von Apps vor Malware heute ein wichtiger Schwerpunktbereich. Die Einrichtung einer starken Anti-Malware-Abwehr ist ein guter Anfang, reicht aber nicht aus. Die Ausnutzung mobiler Banking-Apps kann auf viele andere Arten erfolgen. Mit Anti-Malware-Funktionen allein können Teams in der Tat die Vordertür schützen und die Hintertür offenlassen.

- **Verlassen Sie sich auf signaturbasierte Verteidigungsmaßnahmen.** Angesichts der vielen verschiedenen Banking-Trojaner, die entdeckt werden, und der Geschwindigkeit, mit der sie sich weiterentwickeln, können es sich die Teams nicht leisten, sich auf signaturbasierte Ansätze zu verlassen. Diese Tools bieten statische Mechanismen, die einfach nicht das erforderliche Maß an Sicherheit bieten können. Darüber hinaus sind diese Ansätze in der Regel mit erheblichen zusätzlichen Verarbeitungsanforderungen für Apps verbunden, welches die Leistung und das Nutzererlebnis beeinträchtigen kann. Ferner sind signaturbasierte Tools oft auf ständige Cloud-basierte Suchvorgänge angewiesen, welches die Leistung weiter beeinträchtigen kann.

Zur Sicherstellung, dass mobile Apps sich selbst schützen können, müssen Teams die oben genannten Schritte ausführen, um echte Defense-in-Depth-Funktionen zu etablieren. Um erfolgreich zu sein, muss die Ausnutzung auf dem Gerät in nicht vertrauenswürdigen Umgebungen verhindert werden. Darüber hinaus müssen die Teams die Abfolge der Ereignisse, die erforderlich sind, um die Anwendung und die Daten in Gefahr zu bringen, verstehen. Ferner ist es wichtig, die Bedrohungen in der Umgebung zu verstehen, damit die Teams fundierte Maßnahmen in Bezug auf das Verhalten innerhalb von Apps ergreifen können.

Um die kontinuierliche Intelligenz zu schaffen, die die dynamischen Umgebungen von heute erfordern, muss eine große Menge an Daten verfolgt und analysiert werden. Um zeitnahe und verwertbare Informationen zu erhalten, müssen Teams das maschinelle Lernen nutzen. Eine effektive Lösung muss in der Lage sein, eine enorme Menge an Ereignissen zu analysieren und diese nach ihrer Kritikalität zu priorisieren. Durch maschinelles Lernen können Sicherheitsteams Fehlalarme reduzieren und ihre Arbeit rationalisieren. Auf diese Weise können die Teams ihre Erkennungsfähigkeiten verbessern und bessere Entscheidungen darüber treffen, wie sie reagieren sollen.

Wie Zimperium helfen kann

Entwickler können jetzt mit zDefend von Zimperium Risiken effizienter erkennen und eindämmen. zDefend ist ein in die mobile Anwendung eingebettetes SDK, das der Host-Anwendung gestattet, das Gerät zu prüfen, Bedrohungen zu erkennen und sich proaktiv zu schützen. zDefend nutzt z9, die patentierte, auf maschinellem Lernen basierende Bedrohungserkennungs-Engine von Zimperium, um fortschrittlichen Schutz für Apps zu bieten.

Schlussfolgerung

Mit den oben beschriebenen fünf Schritten können Teams damit beginnen, mobile Banking-Apps ganzheitlich und kontinuierlich zu sichern. Durch die Minderung von Kodierungsrisiken, den Schutz von Code und Schlüsseln, die Transparenz zur Laufzeit und die Einrichtung von Selbstschutzfunktionen können Teams eine umfassende App-Sicherheit realisieren. Folglich können Anbieter von mobilen Banking-Apps ihre Apps, Kundendaten und ihr gesamtes Geschäft effektiv schützen.

Glücklicherweise bietet Zimperium Lösungen an, die Kunden dabei helfen können, diese fünf Schritte mit maximaler Geschwindigkeit und Effizienz zu durchlaufen. Zimperium's Mobile Application Protection Suite (MAPS) bietet die umfassenden Funktionen, die Teams benötigen, um die Sicherheit ihrer mobilen Banking-Apps zu erhöhen. Die Suite kombiniert umfassenden In-App-Schutz mit zentraler Bedrohungsübersicht. MAPS umfasst Funktionen für automatisiertes Anwendungs-Scanning, White-Box-Kryptografie, Anti-Manipulations- und Code-Hardening-Funktionen sowie fortschrittliche, auf maschinellem Lernen basierende Erkennung, Bescheinigung und Überwachung von Bedrohungen.

Kontaktieren Sie uns noch heute, um mehr darüber zu erfahren, wie Zimperium Ihre mobile Banking-Anwendung effektiv und effizient sichern kann.