Lookout®

WHITEPAPER

Wieso die proaktive Absicherung von Apps ein Muss für Finanzdienstleister ist

Finanzinstitute für Endverbraucher befinden sich mitten in einem digitalen Wandel, mit dem traditionelle persönliche Kundenkontakte zunehmend auf Mobilgeräte verlagert werden. Dreiundvierzig Prozent der Mobilfunkgerätebesitzer, die über ein Bankkonto verfügen, nutzen laut einer Studie der Federal Reserve mit dem Titel „Consumers and Mobile Financial Services" (Endverbraucher und mobile Finanzdienstleistungen) mobiles Banking. Mobiles Banking bringt völlig neuartige Annehmlichkeiten für Kunden mit sich, wie zum Beispiel die mobile Abfrage des Kontostands, nahezu sofortige Transfers von Konto zu Konto und Zugriff auf persönliche Konten ohne jegliche zeitliche Einschränkungen.

Dabei sehen Banken und andere Finanzdienstleister in mobilen Apps für Kunden die folgenden Hauptvorteile:

- Intensivere Interaktion mit Kunden. Durch die stärkere Einbindung der Kunden erkennen diese den von Dienstleistern erbrachten Wert. Eine Studie von J. D. Power and Associates hat eine um 84 Punkte höhere Kundenzufriedenheit aufgrund von mobilem Banking ergeben.
- Aufbau von Marken- und Imagebewusstsein. Der durchschnittliche Nutzer verbringt täglich mehr als vier Stunden mit einem Mobiltelefon. Selbst wenn die App eines Unternehmens nicht geöffnet ist, werden auf dem Gerät eines Nutzers Marke und Logo weiter als eine der installierten Apps angezeigt und sind so weiter für den Kunden präsent.
- Reduzierung der Kosten für die Servicebereitstellung. Mit der Automatisierung persönlicher Kontakte können Finanzdienstleistungsunternehmen die Kosten für die Kundenbetreuung senken und die Einsparungen in umsatzsteigernde Initiativen investieren.

Mit der fortwährenden Entwicklung mobiler Apps hat Sicherheit für App-Entwickler weiterhin eine hohe Priorität, um den Diebstahl von Kundenzugangsdaten durch böswillige Akteure zu verhindern.

Bedrohungen für Banking-Apps von Kunden

Es gibt vier Hauptwege, wie böswillige Akteure Zugangs- und andere Kundendaten in Apps ausspähen und manipulieren können:

1. **Infiziertes Gerät.** Über ein infiziertes Gerät (jailbroken oder gerootet) können Angreifer Sicherheitsfunktionen des Geräts ausschalten, die den Zugriff auf private App-Daten normalerweise verhindern, und können weiterhin auf dem Gerät ausgeführte Prozesse modifizieren, die mit der App interagieren, und sich somit Zugang zu den App-Daten verschaffen. Zusätzlich besteht die Möglichkeit der Installation von bösartigem Code, der neben weiteren die voranstehend genannten Aktionen ausführen kann.
2. **Malware.** Über eine auf dem Gerät installierbare bösartige App können Angreifer auf alle auf diesem Gerät ausgeführten Apps zugreifen. Dies gilt auch für Unternehmensanwendungen. Dadurch wird durch übermäßige Freizügigkeit oder durch den Einsatz eines Exploits zur Infizierung des Geräts Zugriff auf Daten gewährt.
3. **Mit einem Trojaner infizierte Version einer legitimen App.** Angreifer können eine legitime Version einer App aus Google Play oder dem App Store von Apple laden, diese modifizieren und sie dann in den App-Store eines Drittanbieters hochladen, der über einen weniger strengen Überprüfungsprozess für Apps verfügt. Angreifer können außerdem die App über Phishing direkt an einen Kunden schicken. In diesem Fall stünde dann eine gefälschte Version der App für den Download durch den Kunden zur Verfügung, die dann Zugangsinformationen und Daten an den Angreifer anstatt an das Unternehmen weiterleitet.
4. **Netzwerkangriff.** Angreifer können Verkehr entschlüsseln, anzeigen oder verändern, nachdem die Schwachstellen in verschlüsselten Kommunikationssystemen ausgenutzt wurden. Dies bezieht sich auch auf Zugangsdaten von Kunden. Diese Art der Ausnutzung wird als „Man-in-the-Middle-Angriff" bezeichnet.

Banking-Trojaner sind auf Kundengeräten aktiv

Anhand von Daten aus unserem einzigartigen Sensorennetzwerk mit über 150 Millionen Mobilgeräten weltweit hat Lookout 30.000 Mobilgeräte analysiert, auf der eine oder mehrere der bekannten Banking-Apps für Kunden installiert waren. Die Historie mobiler Bedrohungen dieser Geräte aus einer einjährigen Studie ergab, dass zehn Prozent der Kunden, die mobiles Banking nutzen, einer mobilen Bedrohung oder einem Risiko ausgesetzt waren.

Bild 1.1.: Gefundene Bedrohungen für Kunden

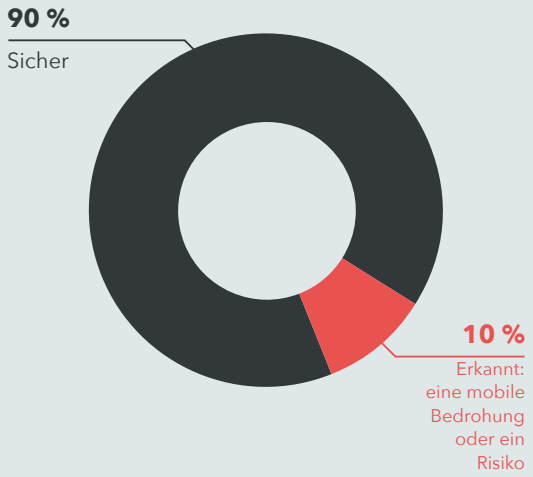
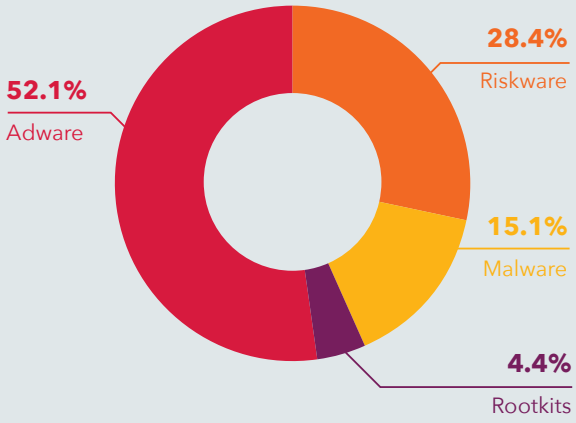


Bild 1.2.: Gefundene Bedrohungsarten



Im Rahmen dieser Studie entdeckte Lookout Geräte, auf denen sich ein oder mehrere gezielte Banking-Trojaner befanden, wie zum Beispiel BancaMarStealer, PlayBanker, Shunbad, SvPeng und TauSpy

Tabelle 1: Gefundene Banking-Trojaner

Trojaner-Familie	Beschreibung
BancaMarStealer	Einfacher Diebstahl von Zugangsdaten durch das Abfangen von Nachrichten mit mTANs bei SMS-Empfängern.
PlayBanker	Ein Trojaner, der Push-Benachrichtigungen generiert, um das Opfer dazu zu bewegen, unkontrollierte Versionen seriöser Banking-Apps herunterzuladen.
Shunbad	Ein Trojaner, der Banking-Apps entpersonalisiert und SMS- und Kontaktdaten stiehlt.
SvPeng	Ein Trojaner, der im Hintergrund schlummert und auf die Nutzung seriöser Banking-Apps wartet, um dann einen gefälschten Anmeldebildschirm überzublenden und die Bankdaten eines Opfers abzufangen.
TauSpy	Einfacher Diebstahl von Zugangsdaten durch das Abfangen von Nachrichten mit mTANs bei SMS-Empfängern.

Finanzinstitute müssen für eine proaktive Reduzierung von Übernahmen von Nutzerkonten, eine Steigerung des Kundenvertrauens und den Schutz vor mobilen Bedrohungen Kunden-Apps mit einer App Defense-Lösung schützen.

Interne App-Entwickler lassen die Sicherheit manchmal außer Acht

App-Entwickler befassen sich vorrangig mit dem Nutzererlebnis und mit der Optimierung der Funktionalität anstatt mit der Integration von Sicherheitsmaßnahmen zum Schutz vor mobilen Bedrohungen. Entwickler konzentrieren sich vielleicht noch darauf sicherzustellen, dass der App-Code keine Schwachstellen enthält, die Sicherheit des Gerätes an sich wird dabei jedoch häufig nicht bedacht.

Eine Zugangsdaten- oder Datensicherheitsverletzung hat verschiedene negative Konsequenzen für Unternehmen, einschließlich Umsatzverlust aufgrund von betrügerischen Handlungen, oder Kunden, die dem Unternehmen ihr Vertrauen entziehen. Weitere Konsequenzen können ein Imageverlust und Strafzahlungen aufgrund der Nichteinhaltung gesetzlicher Bestimmungen sein.

Eine App Defense-Lösung, auf die Sie sich verlassen können

Lookout App Defense stellt für Finanzdienstleister eine proaktive App-Sicherheit bereit, mit der Datensicherheitsverletzungen bei Kunden-Apps verhindert werden. Hierzu werden eine umfassende Transparenz in das Spektrum mobiler Risiken und erweiterter Schutz vor diesen Risiken geboten.

Lookout hat eine Matrix für mobile Risiken entwickelt, die Unternehmen einen Überblick über die Komponenten und Vektoren der gesamten Bandbreite mobiler Risiken vermittelt. Durch die Bereitstellung entsprechender Daten hilft Lookout ihnen außerdem, die Häufigkeit und Auswirkungen mobiler Bedrohungen und Schwachstellen besser zu verstehen.

Lookout App Defense nutzt die Leistungsstärke der Lookout Security Cloud zur Bereitstellung einer einfach zu implementierenden Lösung zum Schutz von Einzelpersonen vor Datensicherheitsverletzungen bei Transaktionen über mobile Apps.

Lookout App Defense weist vier ganz besondere einzigartige Merkmale auf:

Das umfangreiche globale Gerätenetzwerk von Lookout. Lookout Personal ist auf mehreren Millionen Mobilgeräten in über 150 Ländern installiert und nutzt dieselbe Basistechnologie wie Lookout App Defense. Dank dieser massiven Präsenz verfügt Lookout über einen frühzeitigen, exklusiven Einblick in neue und bereits bekannte mobile Bedrohungen. Mit diesem Gerätenetzwerk kann Lookout bestehende Akteure, die eine Bedrohung darstellen, besser nachverfolgen und Bedrohungen frühzeitig erkennen, um Kunden zu schützen und die Gefährdung sensibler Daten zu minimieren.

Lookout-Datensatz und Machine Learning (ML)-Technologie. Viele Anbieter von Sicherheitslösungen geben an, über Machine Learning-Funktionalität zu verfügen, doch nicht die Machine Learning-Algorithmen sondern die Daten sind der entscheidende Faktor. Ohne einen ausreichend großen Datensatz zum Trainieren von ML-Modellen wird sich eine Lösung nicht als wirklich effektiv erweisen. Lookout verfügt über den erforderlichen Datensatz und hat ML auf breiter Basis implementiert.

Eine cloudoptimierte, geräteunterstützte Architektur. Lookout hat seine Plattform für mobile Umgebungen entwickelt und optimiert. Das Sicherheitskonzept besteht darin, die eigene Cloud für die tiefgehende Analyse von Bedrohungen zu nutzen und nach Einführung der App für mobiles Arbeiten effiziente Prüfungen auf den jeweiligen Geräten durchzuführen.

Schnelle, reibungslose Implementierung. Lookout App Defense wurde dahingehend optimiert, dass auch nicht routinemäßig mit der Sicherheit befasste Mitarbeiter das SDK innerhalb weniger Minuten in Kunden-Apps implementieren können. App-Entwickler müssen keine Sicherheitsexperten sein, um die Daten und Funktionen von Kunden-Apps für den mobilen Einsatz zu schützen.

© 2020 Lookout, Inc. LOOKOUT®, das Lookout Shield Design®, LOOKOUT mit Shield Design®, SCREAM® und SIGNAL FLARE® sind eingetragene Marken von Lookout, Inc. in den USA und anderen Ländern. EVERYTHING IS OK®, LOOKOUT MOBILE SECURITY®, POWERED BY LOOKOUT® PROTECTED BY LOOKOUT® sind eingetragene Marken von Lookout, Inc. in den USA und anderen Ländern. POST PERIMETER SECURITY ALLIANCE™ and DAY OF SHECURITY™ sind auch Marken von Lookout, Inc. Alle anderen Logos und Markenzeichen sind Eigentum ihrer eingetragenen Besitzer. 20200203-Lookout-DEv1.1