Zahlungsdienstrichtlinie 2 (PSD2)

Neue Sicherheitsanforderungen für Banking-Apps in der EU

Was bedeutet die PSD2 für Banking-Apps?

Die Zahlungsdienstrichtlinie 2, oder abgekürzt PSD2, ist eine neue EU-Richtlinie mit dem Ziel, Zahlungsdienstleister stärker in den europäischen Binnenmarkt für den Zahlungsverkehr zu integrieren. Das Ziel ist, Zahlungsvorgänge sicherer und effizienter zu gestalten. Ein wichtiger Bestandteil von PSD2 sind Auflagen der Europäischen Bankenaufsichtsbehörde, die die Sicherheit des Zahlungsverkehrs gewährleisten sollen. Ab September 2019 gelten diese für sämtliche Zahlungsdienste innerhalb der EU. Für Banking-Apps bedeuten die höheren Sicherheitsanforderungen der PSD2, dass sie stärker vor bekannten wie unbekannten Cyberangriffen geschützt werden müssen.

Sichere Authentifizierung auf Mobilgeräten ist ein Muss

Die Sicherheitsauflagen der PSD2 sollen den Verbraucher besser schützen und elektronische Zahlungsvorgänge sicherer machen. Die wichtigsten Sicherheitsziele, die die technischen Regulierungsstandards für die PSD2 aufstellen, sind die Erkennung von Malware und das Vorhandensein von Sicherheitsmechanismen, die Risiken auf Anwendergeräten senken sollen. Um diese Vorgaben zu erfüllen, müssen Finanzinstitute Sicherheitsfunktionen in ihre Apps integrieren, die Endgeräte vor bekannten als auch unbekannten Bedrohungen schützen. Gleichzeitig sollten Banking-Apps erkennen können, wenn sie auf einem risikobehafteten Gerät installiert werden, und den Zugriff auf die Bankendienste blockieren, bis die Risiken beseitigt wurden.

Sicherheitsvorgaben der PSD2

Technische Regulierungsstandards

Die Europäische Bankenaufsichtsbehörde hat technische Regulierungsstandards erarbeitet, die ein angemessenes Maß an Sicherheit für die Nutzer von Zahlungsdiensten sicherstellen sollen. Zwei Sicherheitsanforderungen stehen dabei im Mittelpunkt: Malware-Überwachungsmechanismen und Sicherheitsmaßnahmen zur Senkung des Risikos für Mobilgerätenutzer.

Malware-Erkennung

Banken müssen Überwachungsmechanismen für Transaktionen einführen, um Anzeichen einer Malware-Infektion bei jeder Authentifizierungssitzung zu erkennen. *(PSD2, technischer Regulierungsstandard, Artikel 2-3)*

Sichere Laufzeitumgebung

Banken erfordern Sicherheitsmaßnahmen, z. B. sichere Laufzeitumgebungen, um die Gefahren, die von einer Manipulation von Endgeräten ausgehen, zu minimieren. *(PSD2, technischer Regulierungsstandard, Artikel 9-3)*

Lookout App Defense

So unterstützt es die PSD2

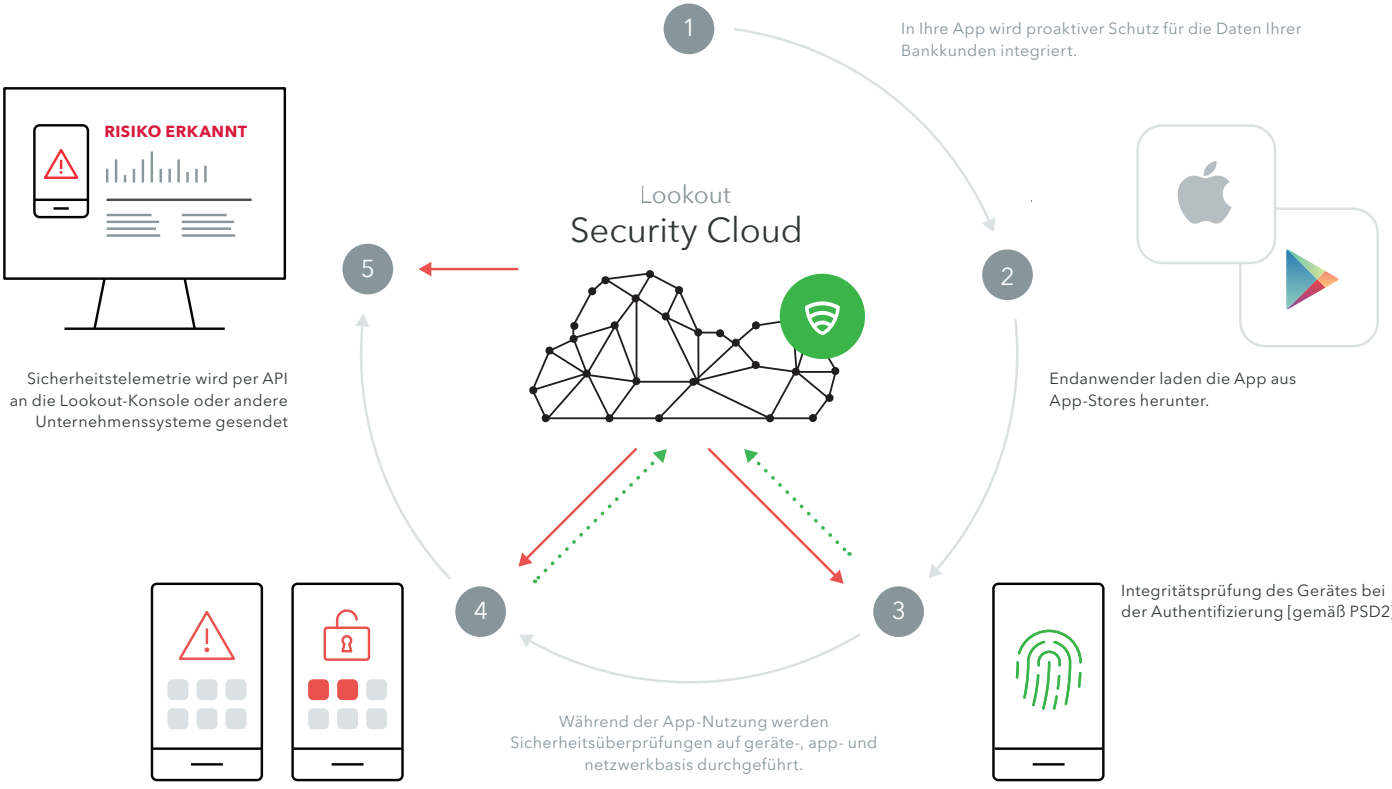
So funktioniert es

App-Entwickler bei Finanzinstituten können das Software-Development-Kit (SDK) von Lookout App Defense ganz einfach während der App-Entwicklung nutzen. Mithilfe dieser Integration ist die App in der Lage auf alle Bedrohungsdaten aus der Lookout Security Cloud zuzugreifen und so Einzelpersonen und Unternehmen vor Datensicherheitsverletzungen bei Transaktionen zu schützen.

Unternehmen können auf die von Lookout App Defense generierte Sicherheitstelemetrie auf zwei Arten zugreifen und diese nutzen:

- Die Entwicklerkonsole von Lookout App Defense ist eine Web-App, über die Administratoren Transparenz bezüglich des Status von Sicherheitsereignissen auf einem Mobilgerät erhalten. Sie bietet außerdem konfigurierbare Risikobewertungen und Warnungen bei Sicherheitsereignissen.
- Die Lookout Event Feed API liefert Informationen über Sicherheitsereignisse, die Unternehmen in SIEM-Systeme, Betrugsmanagementsysteme oder unternehmenseigene Backend-Services integrieren können.

Lookout App Defense-SDK zur Banking-App hinzufügen



Lookout – der feine Unterschied

- Dank unserer globalen Ausrichtung und unserer Konzentration auf Mobilgeräte verfügt Lookout über die weltweit größten Datensätze zur mobilen Sicherheit. Lookout hat Sicherheitsdaten von über 170 Millionen Geräten weltweit erfasst sowie über 70 Millionen Apps überprüft. Täglich kommen bis zu 90.000 neue Apps hinzu.
- Dank dieses globalen Sensorennetzwerks kann unsere Plattform Bedrohungen im Voraus erkennen. Wir setzen dafür maschinelle Intelligenz ein, um komplexe Muster zu identifizieren, die auf Risiken hindeuten. Diese Muster wären für menschliche Analysten nicht erkennbar.
- Die Mobilität hat eine neue Ära der Datenverarbeitung eingeläutet. Benötigt wird eine neue Generation von Sicherheitslösungen, die speziell für diese Plattform entwickelt wurden. Lookout spezialisiert sich bereits seit 2007 auf mobile Sicherheit und verfügt über das nötige Expertenwissen in diesem Bereich.

Mit Lookout ist Ihr Unternehmen in der Lage, sichere Services für Mobilgeräte mit erstklassigen Einblicken in die Anwendungsrisiken bereitzustellen. Um zu erfahren, wie Sie das Anwendererlebnis für Mobilgeräte noch heute besser absichern können, kontaktieren Sie uns unter www.lookout.com/de.