PSD2

VORANTREIBEN DER ABSICHERUNG VON MOBILEN BANKING APPS.

Die Situation

Immer mehr Menschen kümmern sich vorrangig per Banking-App um ihre Finanzen: Sie tätigen Überweisungen, zahlen Rechnungen, reichen Schecks ein usw. Diesen Trend hat die Cyberkriminalität leider nicht verschlafen und hat ihre Bemühungen verstärkt, App-Nutzern zu schaden. Als Reaktion darauf werden immer mehr Vorschriften erlassen, die zusätzliche Sicherheit für Banking- und Zahlungs-Apps erzwingen sollen.

Die wichtigsten Fakten 2018

50%
MEHR MENSCHEN ERLEDIGEN BANKGESCHÄFTE NUR NOCH PER APP[1]

68%
DER MILLENNIALS ZIEHEN DAS SMARTPHONE DER GELDBÖRSE VOR[2]

600%
MEHR BETRÜGERISCHE APP-TRANSAKTIONEN IM ZEITRAUM 2015–2018[3]

65%
ALLER BETRÜGERISCHEN TRANSAKTIONEN FINDEN AUF MOBILGERÄTEN STATT[5]

87%
DER VERBRAUCHER FÜHREN IHRE BANKGESCHÄFTE BEVORZUGT PER MOBILGERÄT DURCH[3]

Wichtige Sicherheitsanforderungen der EBA an PSD2

MALWARE-ERKENNUNG

Banken müssen Überwachungsmechanismen für Transaktionen einführen, um Malware zum Zeitpunkt der Authentifizierung zu erkennen.

(PSD2, technischer Regulierungsstandard, Artikel 2)

SICHERE LAUFZEITUMGEBUNG

Banken müssen Sicherheitsmaßnahmen treffen, z. B. sichere Laufzeitumgebungen, um die Auswirkungen durch kompromittierte Geräte zu minimieren.

(PSD2, technischer Regulierungsstandard, Artikel 9)

Beispiele aus der Praxis[4]

15/100
GERÄTEN MIT APPS VON BEDEUTENDEN KREDITINSTITUTEN, DIE BEREITS EINMAL UNTER BEDROHUNG STANDEN

62%
DER BEVÖLKERUNG HÄLT DIE VENMO-APP FÜR NICHT SEHR SICHER

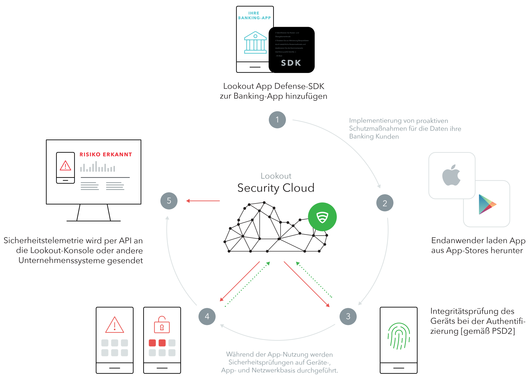
56.000
GERÄTE MIT APP EINER TOP-5-BANK SCHON EINMAL VON TROJANERN, SURVEILLANCEWARE ODER SPYWARE BEFALLEN

So werden Banking-Apps auf die Einhaltung von PSD2 vorbereitet

- Anwendung einer reibungslosen Bereitstellungsstrategie
- Zusätzlicher Schutz vor (un-)bekannten App-Bedrohungen
- Schnellerer Schutz
- Integration von Sicherheit auf App-Ebene
- Implementierung von Sicherheitsrichtlinien auf Basis eines umfangreichen Mobildatensatzes
- Gewährleistung von Sicherheit auf Kundenniveau

So schützt Lookout Banking-Apps

Sobald sich ein Anwender authentifiziert, überprüft Lookout App Defense, ob Malware vorhanden ist oder das Gerät kompromittiert wurde..



Lookout

1. Schiff, David, et al. „PwC's 2018 Digital Banking Consumer Survey: Mobile Users Set the Agenda". (PwC-Verbraucherumfrage zu digitalen Bankgeschäften: App-Nutzer geben den Ton an), PwC, Juni 2018, www.pwc.com/us/en/industries/financial-services/library/digital-banking-consumer-survey.html. Zugriff: Jan. 2019
2. „Mobile Banking One of Top Three Most Used Apps by Americans, 2018 Citi Mobile Banking Study Reveals" (2018er Citi-Studie zu Mobile Banking zeigt: In den USA zählen Banking-Apps zu den drei am häufigsten genutzten App-Arten). About | Citi | Timeline. 26. April 2018. Zugriff: Januar 2019. https://www.citigroup.com/citi/news/2018/180426a.htm
3. „Fraud Prevention | RSA Fraud & Risk Intelligence Suite" (Betrugsprävention | RSA Fraud & Risk Intelligence Suite). RSA FRAUD PREVENTION RSA® Fraud & Risk Intelligence Suite. 2018. Zugriff: Januar 2019. https://www.rsa.com/en-us/products/fraud-prevention.
4. „Lookout App Defense". Mobile Sicherheit. Zugriff: 14. Januar 2019. https://www.lookout.com/products/app-defense.
5. Orem, Tina. „65% of Fraud Transactions Happen on Mobile, Study Finds" (Umfrage ergibt, dass 65 % aller Betrugstransaktionen auf Mobilgeräten stattfinden). Credit Union Times. 31. Mai 2018.Zugriff: 19. Januar 2019. https://www.cutimes.com/2018/05/31/65-of-fraud-transactions-happen-on-mobile-study-fi/?slreturn=20190022141719.