Directive sur les services de paiement (PSD2)

Les nouvelles exigences de sécurité pour les applications bancaires sur mobile en UE

Quel est l'impact de la DSP2 pour les applications bancaires sur mobile ?

La DSP2 (en anglais PSD2) ou Directive sur les services de paiement 2 est une directive européenne qui imposera aux prestataires de services financiers de contribuer à un écosystème de paiement plus intégré, plus sûr et plus efficace. Parmi les éléments clés de la directive DSP2 figurent les exigences fixées par l'Autorité bancaire européenne pour garantir la sécurité des paiements. Cette directive entrera en vigueur en septembre 2019 et s'appliquera à tous les services de paiement au sein de l'UE. En ce qui concerne les applications bancaires sur mobile, les exigences de sécurité définies par la DSP2 soulignent la nécessité de les protéger contre les attaques à la fois connues et inconnues.

La nécessité de sécuriser l'authentification sur mobile

En termes de sécurité, les objectifs de la DSP2 sont d'assurer la protection des consommateurs et de rendre l'utilisation des services de paiement plus sûre. Ainsi, les normes techniques de réglementation de la DSP2 fixent comme priorité la capacité de détecter les logiciels malveillants et de sécuriser les appareils des utilisateurs pour réduire les risques. Pour satisfaire à ces exigences, les institutions financières doivent doter leurs applications mobiles de fonctionnalités de sécurité pour faire face aux menaces connues et inconnues sur les appareils des utilisateurs. Les applications bancaires sur mobile doivent également être capables de détecter si elles sont installées sur un appareil à risque et bloquer l'accès aux services bancaires tant que le danger n'a pas été écarté.

Exigences de sécurité de la DSP2

Normes techniques de réglementation

L'Autorité bancaire européenne a élaboré des normes techniques de réglementation afin de garantir un niveau de sécurité suffisant aux utilisateurs de services de paiement. Ces normes exigent notamment des mécanismes de surveillance des logiciels malveillants et des mesures de sécurité pour réduire les risques pour les utilisateurs d'appareils mobiles :

Détecter les logiciels malveillants

Les banques doivent appliquer des mécanismes de suivi des opérations pour détecter tout signe d'infection par des logiciels malveillants à n'importe quelle étape de la procédure d'authentification. *(DSP2, Normes techniques de réglementation, Article 2-3)*

Sécuriser les environnements d'exécution

Afin de réduire les risques lorsque l'appareil d'un utilisateur est compromis, les banques doivent mettre en place des mesures de sécurité telles que la sécurisation des environnements d'exécution. *(DSP2, Normes techniques de réglementation, Article 9-3)*

Lookout App Defense

La réponse à la Directive sur les Services de Paiement (DSP2)

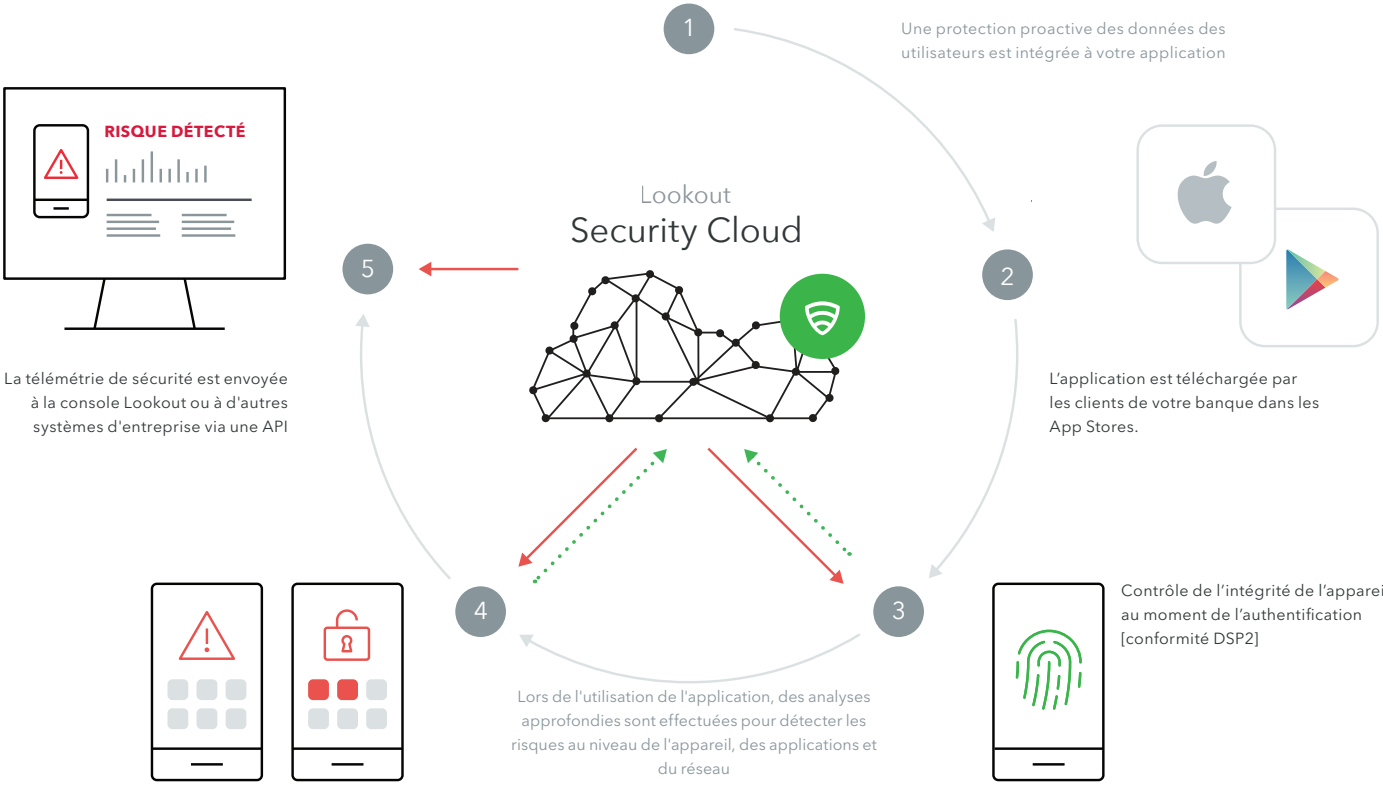
Fonctionnement

Durant la phase de développement d'une application, les développeurs au sein d'institutions financières intègrent simplement le SDK Lookout App Defense au process de développement. Une fois en place, celui-ci exploite directement les données de Lookout Threat Intelligence pour empêcher une compromission des données lors de transactions réalisées depuis une application bancaire.

Pour accéder à la télémétrie de sécurité générée par Lookout App Defense et l'utiliser, les entreprises ont deux possibilités :

- La console de développement Lookout App Defense est une application web qui donne aux administrateurs la visibilité sur les événements de sécurité d'un appareil mobile, grâce à des évaluations de risque et des alertes d'événement de sécurité réglables
- Lookout Event Feed API est un flux de télémétrie et d'événements de sécurité que les entreprises peuvent intégrer à leurs systèmes SIEM, de gestion de la fraude ou aux services back-end propriétaires

Ajout du kit de développement logiciel Lookout App Defense à votre application bancaire sur mobile



Ce qui rend Lookout différent

- Grâce à notre présence mondiale et à l'importance que nous accordons au mobile, Lookout a réuni l'ensemble de données sur la sécurité mobile le plus important au monde. Lookout a ainsi collecté les données de sécurité de plus de 175 millions d'appareils à travers le monde et de plus de 80 millions d'applications, avec jusqu'à 90 000 nouvelles applications ajoutées chaque jour.
- Ce réseau de capteurs mondial intègre la notion de prédiction à notre plate-forme en utilisant l'intelligence artificielle pour identifier des modèles d'attaques complexes, modèles qui autrement échapperaient aux analystes humains.
- La mobilité a fait entrer l'informatique dans une nouvelle ère et nécessite une nouvelle solution de sécurité conçue exclusivement pour ses besoins. Lookout sécurise les appareils mobiles depuis 2007 et possède une solide expérience en la matière.

Lookout permet à votre entreprise d'offrir des services mobiles sécurisés en bénéficiant d'une visibilité inégalée sur les risques applicatifs. Pour savoir dès aujourd'hui comment sécuriser vos expériences utilisateurs mobiles, rendez-vous sur www.lookout.com.

.