Protection complète pour les applications mobiles

Les données et les transactions des utilisateurs mobiles sont mieux protégées lorsque les mécanismes de protection sont intégrés directement dans les applications. La technologie RASP de VASCO rend cela possible de manière simple.

Protéger les applications mobiles contre les cyberattaques n'est pas une tâche facile. Cela s'explique par le fait que les applications correspondantes sont souvent installées sur des périphériques en dehors de l'entreprise et sont utilisées en dehors du réseau sécurisé de l'entreprise. De plus, les systèmes d'exploitation et les applications sont souvent désuets et contiennent des failles. Les analystes de Gartner soulignent que la plupart des applications de certains magasins d'applications présentent des vulnérabilités qui peuvent être facilement exploitées par des pirates informatiques.

LES APPAREILS MOBILES ET LES APPLICATIONS DEVIENNENT DE PLUS EN PLUS IMPORTANTS; LEUR PROTECTION COMPLÈTE EST UNE NÉCESSITÉ.

Protection directement dans l'application

Les pare-feu périmétriques traditionnels à l'entrée du réseau local de l'entreprise ne suffisent pas pour assurer une protection complète des applications mobiles. Afin de sécuriser les données et les transactions des appareils mobiles de manière transparente, une protection complète des applications individuelles est nécessaire. Mais la protection des applications n'a pas bien fonctionné jusqu'à présent. Gartner estime que les entreprises investissent plus de 20 fois plus dans la sécurité périmétrique que dans la sécurisation des applications. Cela doit changer, souligne le spécialiste de la sécurité VASCO et présente VASCO RASP, une solution qui cible directement la protection de l'application individuelle.

La technologie RASP (Runtime Application Self-Protection) de VASCO s'enroule autour du code d'une application grâce à une intégration native et la protège des vecteurs d'attaque connus et inconnus. La solution offre une sécurité complète basée sur le principe «Protect – Detect – React»:

D'une part, les attaques par injection de code sont repoussées de manière fiable, ce qui, entre autres choses, bloque les tentatives de Reverse Engineering. D'autre part, RASP détecte plus de douze types de vulnérabilités et de méthodes d'attaque avancées – tels que les périphériques rootés et les «jailbreaks», les attaques Overlay et Repackaging, Screenreader et Keylogger. Cela protège les entrées d'utilisateur confidentielles telles que les ID utilisateur et les mots de passe contre le vol de données et les activités frauduleuses. Grâce à ces mesures de sécurité combinées, l'application sécurisée est dans une certaine mesure située dans un coffre-fort qui ne permet qu'un accès autorisé aux fonctions de l'application et protège ainsi de manière fiable les données et les transactions sensibles contre les cybercriminels.

De plus, la technologie RASP de VASCO réagit aux attaques. Si un risque élevé est détecté, RASP arrête complètement l'application. RASP enregistre dynamiquement toutes les activités détectées comme étant malveillantes ou suspectes et c'est la première solution de ce type à fournir un rapport centralisé sur la conformité des comportements à risque des applications mobiles.

Simple pour les développeurs, sûr pour les utilisateurs

RASP s'implémente dans les applications existantes et nouvellement développées. La technologie analyse la logique métier, les flux d'événements et de données de l'application à sauvegarder et se connecte automatiquement au code de l'application existante. De cette façon, les applications sécurisées RASP peuvent être lancées très rapidement et facilement. Cela n'affecte pas le développement de l'application. Ce qui profite non seulement aux départements de développement interne, mais aussi aux développeurs d'applications indépendants. En intégrant RASP, les développeurs peuvent fournir à leurs applications le plus haut niveau de sécurité sans pratiquement aucun effort, se concentrer sur la fonctionnalité de leurs applications et marquer des points avec leurs clients avec des applications particulièrement dignes de confiance.

VASCO RASP fait également partie de la suite de sécurité mobile «Digipass for Apps». La solution modulaire permet aux développeurs d'équiper les applications d'une grande variété de fonctions de sécurité en utilisant une API uniforme. Il s'agit notamment des méthodes d'authentification telles que CRONTO, la reconnaissance d'empreintes digitales et de visages, la liaison de dispositifs (l'application ne fonctionne que sur un dispositif spécifique), la géolocalisation et la fonctionnalité de QR Code.

VASCO RASP: Points forts

- Bloque les attaques: RASP protège contre les attaques de type «zero-day» et autres attaques ciblées.
- Détecte et bloque le code malveillant: Exécutez en toute sécurité des applications critiques, même sur des périphériques infectés.
- Enregistrement complet: Toutes les activités sont enregistrées dynamiquement – essentiel pour la conformité et la gestion des risques.
- Facile à mettre en œuvre: Se lie automatiquement au code des applications existantes ou nouvellement développées.
- Idéal pour les développeurs: la sécurité des applications sans effort de développement, la confiance des clients augmente.

BOLL
IT Security Distribution

BOLL Engineering SA

En Budron H15
1052 Le Mont-sur-Lausanne
Tél. 021 533 01 60
vente@boll.ch | www.boll.ch