# Umfassender Schutz für mobile Anwendungen

Daten und Transaktionen mobiler Anwender sind am besten geschützt, wenn die Schutzmechanismen direkt in die einzelnen Apps integriert sind. Die RASP-Technologie von VASCO macht dies auf einfache Art und Weise möglich.

Mobile Anwendungen gegen Cyberangriffe zu schützen, ist kein einfaches Unterfangen. Denn die entsprechenden Apps sind oft auf firmenfremden Geräten installiert und kommen ausserhalb des abgesicherten Unternehmensnetzwerks zum Einsatz. Zudem sind Betriebssysteme und Apps oft nicht auf dem neuesten Stand und bergen Fehler. So betonen Analysten von Gartner, dass sich in manchen App-Stores mehrheitlich Apps mit Schwachstellen tummeln, die von Hackern einfach ausgenutzt werden können.

**MOBILE GERÄTE UND ANWENDUNGEN WERDEN IMMER BEDEUTSAMER; DEREN UMFASSENDER SCHUTZ IST EINE NOTWENDIGKEIT.**


### Schutz direkt in der App

Klassische Perimeter-Firewalls am Eingang zum Firmen-LAN reichen nicht aus, um mobilen Anwendungen einen umfassenden Schutz zu gewähren. Um Daten und Transaktionen mobiler Devices nahtlos zu sichern, ist vielmehr ein umfassender Schutz der einzelnen Apps notwendig. Doch bisher stand es mit dem App-Schutz nicht zum Besten. So schätzt Gartner, dass Unternehmen über 20-mal mehr in die Perimeter-Security investieren als in die Sicherung von Apps. Dies muss sich ändern, betont der Security-Spezialist VASCO und präsentiert mit VASCO RASP eine Lösung, die direkt auf den Schutz der einzelnen App abzielt.

Die RASP-Technologie (Runtime Application Self-Protection) von VASCO hüllt sich durch eine native Integration um den Code einer App und schützt diese vor bekannten und unbekannten Angriffsvektoren. Die Lösung bietet eine umfassende Sicherheit nach dem Prinzip «Protect – Detect – React»:

Einerseits werden Code-Injection-Angriffe zuverlässig abgewehrt, was unter anderem Reverse-Engineering-Versuche abblockt. Andererseits erkennt RASP mehr als zwölf Typen von Schwachstellen und fortgeschrittenen Angriffsmethoden – so beispielsweise gerootete Geräte und Jailbreaks, Overlay- und Repackaging-Attacken, Screenreader und Keylogger. Dadurch bleiben vertrauliche Nutzereingaben wie User-IDs und Passwörter vor Datenklau geschützt und betrügerische Aktivitäten werden im Keim erstickt. Dank dieser kombinierten Schutzmassnahmen liegt die gesicherte App gewissermassen in einem Tresor, der nur einen autorisierten Zugang auf die App-Funktionen erlaubt und damit sensitive Daten und Transaktionen zuverlässig vor Cyberkriminellen schützt.

Zudem reagiert die RASP-Technologie von VASCO auf Angriffe. Wird ein hohes Risiko erkannt, stoppt RASP die Ausführung der App vollständig. Sämtliche Aktivitäten, die als bösartig oder verdächtig erkannt werden, hält RASP dynamisch fest und legt damit als erste Lösung ihrer Art die Basis für eine zentrale, Compliance-konforme Protokollierung des Risikoverhaltens mobiler Anwendungen.

### Unkompliziert für Entwickler, sicher für Anwender

RASP implementiert sich selbst in bestehende und neu entwickelte Apps. Dabei durchsucht die Technologie die Geschäftslogik, die Ereignis- und Datenflüsse der zu sichernden App und bindet sich automatisch an den vorhandenen App-Code an. Auf diese Weise können RASP-gesicherte Apps sehr schnell und unkompliziert lanciert werden. Die primäre App-Entwicklung wird dadurch nicht beeinflusst. Dies kommt nicht nur unternehmensinternen Entwicklungsabteilungen, sondern auch unabhängigen App-Entwicklern zugute. So können Entwickler durch die Integration von RASP ihre Apps praktisch ohne Aufwand mit Sicherheit auf höchstem Niveau ausstatten, sich auf die Funktionalität ihrer Apps konzentrieren und bei ihren Kunden mit besonders vertrauenswürdigen Apps punkten.

VASCO RASP ist überdies Teil der Mobile-Security-Suite «Digipass for Apps». Die modular aufgebaute Lösung ermöglicht Entwicklern, Apps unter einem einheitlichen API mit unterschiedlichsten Sicherheitsfunktionen auszurüsten. Dazu gehören Authentifizierungsverfahren wie CRONTO, Fingerabdruck- und Gesichtserkennung, Device-Binding (App läuft nur auf einem bestimmten Gerät), Geolocation und QR-Code-Funktionalität.

### VASCO RASP – die Highlights:

- Wehrt Angriffe ab: RASP schützt vor Zero-Day- und anderen gezielten Angriffen
- Erkennt und blockiert Schadcode: Selbst auf infizierten Geräten können geschäftskritische Apps sicher ausgeführt werden
- Protokolliert umfassend: Alle Aktivitäten werden dynamisch aufgezeichnet – essenziell für Compliance und Risikomanagement
- Einfach zu implementieren: Bindet sich automatisch an den Code bestehender oder neu entwickelter Apps an
- Ideal für Entwickler: App-Sicherheit ohne Entwicklungsaufwand, Kundenvertrauen steigt

BOLL
IT Security Distribution

**BOLL Engineering AG**

Jurastrasse 58
5430 Wettingen
Tel. 056 437 60 60
info@boll.ch | www.boll.ch