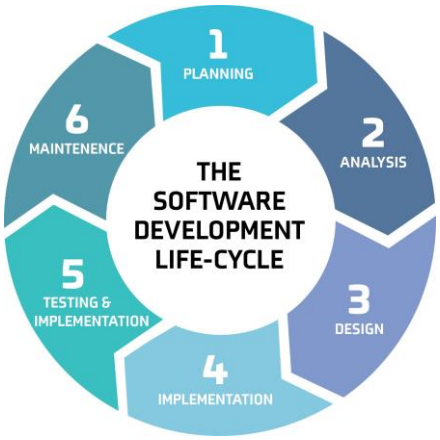
ZIMPERIUM®
MOBILE THREAT DEFENSE

Beschreibung der Lösung MAPS (Mobile Application Protection Suite)

HINDERNISSE BEZÜGLICH DER SICHERUNG MOBILER APPS

Unternehmen, die mobile Apps entwickeln, sind sich bewusst, dass sie diese auch sichern müssen. Mobile Apps werden immer ausgefeilter und verarbeiten sensiblere personen- bzw. unternehmensbezogene Daten in einem noch nie dagewesenen Umfang. Unternehmen sind sich auch der enormen Reputations- und Finanzrisiken bewusst – ob direkt in Form von Betrug oder indirekt als Geldbußen usw.–, die sich aus Verstößen im Zusammenhang mit der Verwendung von Mobilgeräten ergeben können.

Entwicklungs- und Sicherheitsteams benötigen Transparenz über den gesamten Softwareentwicklungslebenszyklus hinweg. Ihre Bemühungen wurden jedoch durch eine stark fragmentierte Reihe von Lösungen sowie einen Mangel an Sichtbarkeit von Bedrohungen auf Endbenutzergeräten erschwert. Mobile Apps haben das Potenzial, einen erheblichen Geschäftswert zu erzielen, jedoch nur, wenn die Hindernisse im Bereich der App-Sicherheit überwunden werden können. Dazu zählen:



Hindernis	Bedarf
Fragmentierte Risikobewertungslösungen	Unternehmen benötigen eine konsolidierte Sicht auf sämtliche Risiken, und zwar sowohl während der Entwicklung als auch kontinuierlich nach der Markteinführung der Anwendung.
Keine Sichtbarkeit von Bedrohungen auf Benutzergeräten	Unternehmen benötigen eine klare und kontinuierliche Übersicht über Bedrohungen auf Benutzergeräten, die zu Datenexfiltrationen sowie anderen Risiken führen können.

DIE MOBILE APPLICATION SUITE (MAPS) VON ZIMPERIUM

Um seinen Kunden eine Lösung für beide Probleme zu bieten, hat Zimperium das einzige vollständige Anwendungsschutzpaket für Mobilgeräte (Mobile Application Protection Suite/MAPS) entwickelt. Zimperium MAPS identifiziert Sicherheits-, Datenschutz- und Compliance-Risiken während der App-Entwicklung und überwacht bzw. schützt Apps vor Angriffen während der Verwendung. MAPS ist die einzige Sicherheitslösung für mobile Apps, die eine Risikoidentifizierung sowie Schutz über den gesamten Systementwicklungslebenszyklus hinweg bietet.

Das Paket besteht aus drei Lösungen, die jeweils die spezifischen Unternehmensanforderungen während den verschiedenen Phasen des Systementwicklungslebenszyklus erfüllen. Mit MAPS ist das Ganze tatsächlich größer als die Summe seiner Teile. Alle Lösungen verwenden dieselbe Backend- bzw. Verwaltungskonsole (zConsole), um eine umfassende und nahtlose Sichtbarkeit sowie Verwaltung von Risiken und Bedrohungen zu gewährleisten. Dank des in den gesamten Systementwicklungslebenszyklus integrierten Pakets liefert MAPS wertvolle Erkenntnisse, die nicht nur aktuelle Risiken erkennen lassen, sondern Entwicklern auch dabei helfen, Probleme zu identifizieren, die in zukünftigen Versionen gelöst werden können.

Die MAPS-Lösungen umfassen:

Unternehmenslösungen	MAPS-Lösung	Mehrwert
Konforme Gestaltung *Welche Probleme sollten wir vor der Markteinführung unserer App behoben haben?*	zSCAN™	Mithilfe von zScan können Unternehmen Compliance-, Datenschutz- und Sicherheitsprobleme in mobilen Apps erkennen und beheben, bevor diese im Rahmen des Entwicklungsprozesses auf den Markt gebracht werden.
Sichere Gestaltung *Wie können wir unsere App gegen Reverse Engineering oder Code-Manipulationen schützen?*	zSHIELD™	Die Funktionen der zShield-App zum Schutz vor Obfuskation und Manipulation bewahren die App vor möglichen Angriffen wie Reverse Engineering und Code-Manipulation.
Sicherer Betrieb *Wie können wir unsere App vor modernen Angriffen auf Endbenutzergeräte schützen?*	zDEFEND™	Das SDK zDefend wird in Apps eingebettet, um Angriffe auf Geräte und Netzwerke sowie böswillige Angriffe auf die App zu erkennen und abzuwehren.

ZIMPERIUM zSCAN ZUM AUFSPÜREN VON RISIKEN FÜR MOBILE APPS WÄHREND DER ENTWICKLUNG

Zimperium zScan hilft Entwicklern mobiler Apps, Reputations- und Finanzrisiken zu vermeiden, indem Datenschutz-, Sicherheits- und Compliance-Risiken im Entwicklungsprozess automatisch identifiziert werden, bevor Apps auf den Markt gebracht werden.

Während herkömmliche Code-Analyse-Tools die Bewertung der allgemeinen Qualität des Codes eines Entwicklers unterstützen, identifizieren die binären Analysefunktionen von zScan Risiken, die Angreifer sichtbar machen könnte, um die fertig entwickelte App zu beeinträchtigen. zScan ermöglicht eine sofortige Sichtbarkeit von Datenschutz- und Sicherheitsrisiken für die App, die von anderen Scannern nicht erkannt werden. Zudem deckt sie Vorfälle auf, die Probleme mit der Compliance im Zusammenhang mit der NIAP, der DSGVO sowie der OWASP Top 10 verursachen könnten. In zConsole, der Administratorkonsole von zScan, kümmern sich Compliance- und Sicherheitsteams darum, Richtlinien zu definieren und individuell anzupassen, sodass nur Probleme in Verbindung mit einer mangelnden Compliance an die Entwickler zur Behebung gesendet werden.

ZIMPERIUM zSHIELD ZUR VERHINDERUNG VON APP-MANIPULATIONSVERSUCHEN

Sobald eine mobile App auf den Markt gebracht wird, könnten potenzielle Angreifer versuchen, Codierungsfehler und Schwachstellen ausfindig zu machen, die für böswillige Zwecke ausgenutzt werden könnten. Die Funktionen zum Schutz vor Obfuskation und Manipulation von Zimperium zShield stärkt und schützt die App vor verschiedenen Angriffen. Dazu zählen beispielsweise Reverse Engineering, Piraterie, Entfernung von Anzeigen, Extrahierung von Vermögenswerten oder API-Schlüsseln sowie Einfügen von Malware. Im Gegensatz zu Obfuskationslösungen, die sich auf manuelle Penetrationstests verlassen, um die Effektivität zu beweisen, und keine aktive Berichterstattung umfassen, bietet zShield eine fortlaufende und sofortige Übersicht über App-Manipulationsversuche auf Endbenutzergeräten, indem die Vorfälle über zConsole, dem Verwaltungs- und Berichterstattungs-Dashboard von Zimperium gemeldet werden.

ZIMPERIUM zDEFEND ZUM SCHUTZ VON APPS VOR MOBILEN ANGRIFFEN

Das Software Development Kit (SDK) zDefend von Zimperium ermöglicht es Entwicklern, die führende Erkennungsengine z9 von Zimperium, die auf der Grundlage maschineller Lernverfahren arbeitet, schnell und problemlos direkt in jede mobile App einzubetten. Dank des eingebetteten SDK zDefend können mobile Apps sofort feststellen, ob

das Gerät des Benutzers kompromittiert ist, Netzwerkangriffe erfolgen und selbst ob schädliche Apps installiert sind. zDefend kann von App-Entwicklern vollständig konfiguriert werden, sodass sie wählen können, welche Abhilfemaßnahmen angewendet werden sollen, wenn eine bestimmte Bedrohung erkannt wird. Wenn ein Gerät angegriffen wird, informiert zDefend die App und leitet die festgelegten Maßnahmen zur Risikominderung ein.

MAPS IN AKTION ERLEBEN

Zimperium MAPS identifiziert Sicherheits-, Datenschutz- und Compliance-Risiken während der App-Entwicklung und überwacht bzw. schützt Apps vor Angriffen während der Verwendung. MAPS löst beide Hindernisse für die Sicherheit mobiler Apps, da es die einzige Lösung ist, die Folgendes bietet:

- Eine konsolidierte Sicht auf sämtliche Risiken, und zwar sowohl während der Entwicklung als auch kontinuierlich nach der Markteinführung der Anwendung
- Eine klare und kontinuierliche Übersicht über Bedrohungen auf Benutzergeräten in Unternehmen, die zu Datenexfiltrationen sowie anderen Risiken führen können

Wenn Ihr Unternehmen einer sofortigen, mühelosen und robusten Sicherheit für mobile Apps bedarf, ist MAPS von Zimperium genau das Richtige für Sie.

Um mehr über Zimperium MAPS zu erfahren oder eine Demo anzufordern, kontaktieren Sie uns am besten gleich heute.