



OWASP

Open Web Application
Security Project

Why Organisations should rely on Mobile AppTesting

Dr. Michael Spreitzenbarth & Jennifer Bombien

Siemens CERT

Über mich

- Wifo-Studium an der Universität Mannheim mit Schwerpunkt IT-Sicherheit und Forensik
- PhD an der FAU mit Schwerpunkten in den Bereichen Forensik und Malware-Analyse auf Android Endgeräten und dessen Applikationen
- Teamleiter im Siemens CERT
- Schwerpunkte im Bereich Forensik, Incident Handling und AppTesting auf mobilen Plattformen (Android, BB10, iOS und WP10)



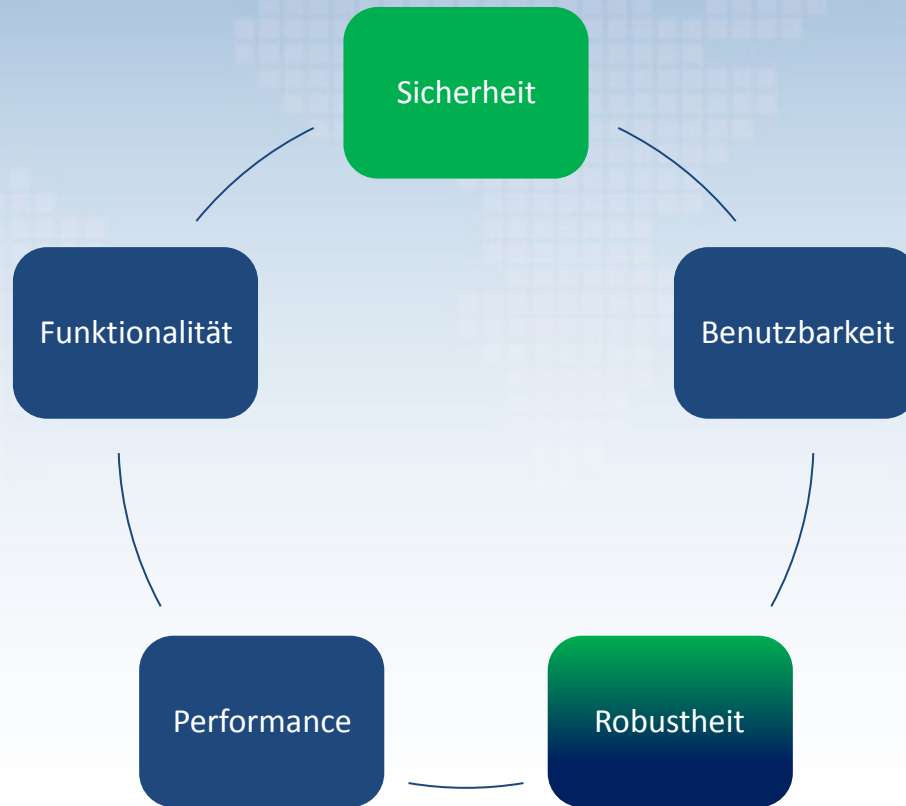
Agenda

- ❖ Verifizieren und Testen mobiler Apps
- ❖ Potential verfügbarer App-Test Lösungen
- ❖ Vorstellung unseres AppTesting Konzepts
- ❖ Ein Jahr AppTesting im Rückblick
- ❖ Mobile AppTesting Matrix

Welche Möglichkeiten zum Testen von Apps gibt es?

VERIFIZIEREN MOBILER APPS

Testmöglichkeiten mobiler Apps



Schlussfolgerungen

- Vertrauen in die „Marketing-Slides“ der Hersteller oft keine gute Idee wenn es um sensible Inhalte / Usecases geht
- Der Schutz sensibler Daten kann ohne Überprüfung nicht gewährleistet werden
- Einhalten von internen Policy-Vorgaben und Infrastrukturrichtlinien ist wichtig und für externe Tester nur schwer zu prüfen

Schlussfolgerungen

- Vertrauen in die „Marketing-Slides“ der Hersteller oft keine gute Idee wenn es um sensible Inhalte / Usecases geht
- Der Schutz sensibler Daten kann ohne Überprüfung nicht gewährleistet werden
- Einhalten von internen Policy-Vorgaben und Infrastrukturrichtlinien ist wichtig und für externe Tester nur schwer zu prüfen

→ **Organisationen und große Firmen müssen ihre Apps testen !**

Welche Lösungen gibt es auf dem Markt und was leisten sie?

POTENTIAL VERFÜGBARER APP- TESTING LÖSUNGEN

Übersicht über verfügbare Lösungen

Lösung	Plattform	Statisch / Dynamisch	Privacy	Security	Manuell / Automatisiert	Nötiges Wissen
DiOS	iOS	beides	X	---	automatisiert	0
iNalyzer	iOS	dynamisch	(X)	X	manuell	000
Snoop-it	iOS	dynamisch	(X)	X	manuell	00
Cycrypt	iOS	dynamisch	---	X	manuell	00000
MobileSandbox-NG	Android	beides	X	---	automatisiert	00
Androguard	Android	statisch	X	X	manuell	0000
Drozer	Android	beides	(X)	X	beides	00000
DroidBox	Android	dynamisch	X	---	automatisiert	00
CuckooDroid	Android	dynamisch	X	(X)	automatisiert	000
AuditDroid	Android	beides	---	X	beides	0000
NowSecure Lab	beides	beides	X	X	beides	0000
Introspsy	beides	dynamisch	(X)	X	manuell	000

Und noch einige (~100) mehr ...

Wie sieht unser Konzept als App Testing Lösung für Unternehmen aus?

APPTESTING KONZEPT ALS UNTERNEHMENSLÖSUNG

Unser Lösungsansatz

Unser Lösungsansatz

Simple Check

- 90% automatisiert
- 10% manuell
- Privacy / Datenschutz
- Einfacher Report in Ampelfarben
- 1 Tag Aufwand

✓ Schnell und günstig

✓ Fokus auf Privacy und Datenschutz

✗ Kein Security-Testing

Unser Lösungsansatz

Simple Check

- 90% automatisiert
- 10% manuell

- Privacy / Datenschutz

- Einfacher Report in Ampelfarben

- 1 Tag Aufwand

- ✓ Schnell und günstig
- ✓ Fokus auf Privacy und Datenschutz
- ✗ Kein Security-Testing

In-Depth Check

- 50% automatisiert
- 50% manuell

- Privacy / Datenschutz
- Schwachstellen im Code
- Schwachstellen im Design

- Ausführlicher Report mit Unterstützung für den Entwickler

- 2-3 Tage Aufwand

- ✓ Deutlich mehr Details und Tests
- ✓ Security-Testing
- ✓ Detaillierter Report der den Entwicklern beim Lernprozess hilft

Unser Lösungsansatz

Simple Check

- 90% automatisiert
- 10% manuell

- Privacy / Datenschutz

- Einfacher Report in Ampelfarben

- 1 Tag Aufwand

- ✓ Schnell und günstig
- ✓ Fokus auf Privacy und Datenschutz
- ✗ Kein Security-Testing

In-Depth Check

- 50% automatisiert
- 50% manuell

- Privacy / Datenschutz
- Schwachstellen im Code
- Schwachstellen im Design

- Ausführlicher Report mit Unterstützung für den Entwickler

- 2-3 Tage Aufwand

- ✓ Deutlich mehr Details und Tests
- ✓ Security-Testing
- ✓ Detaillierter Report der den Entwicklern beim Lernprozess hilft

Assessment

- 20% automatisiert
- 80% manuell

- Privacy / Datenschutz
- Schwachstellen im Code
- Schwachstellen im Design

- Ausführlicher Report mit Unterstützung für den Entwickler

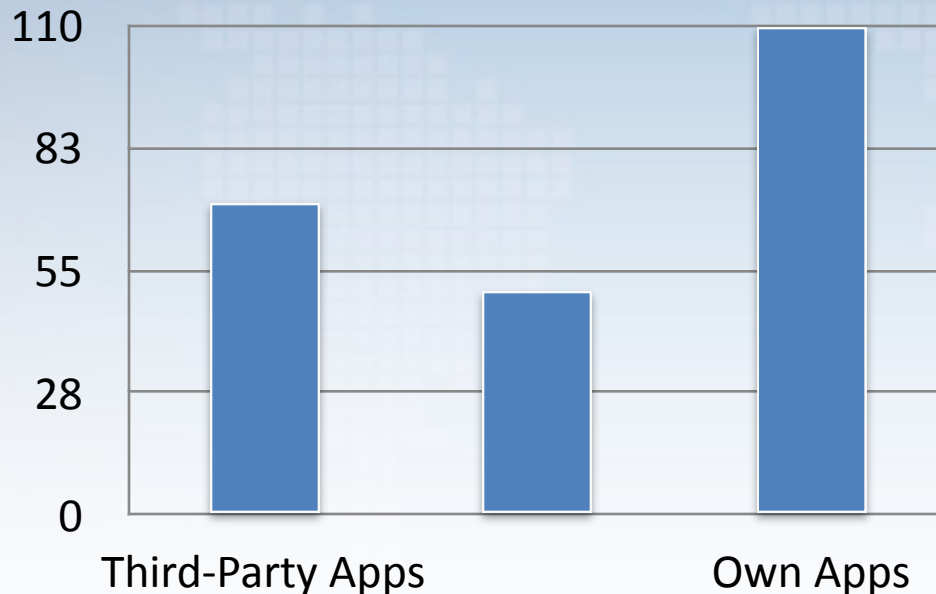
- Aufwand nach Absprache (>5 Tage)

- ✓ Noch tiefere und ausgereifere Tests

Was sind die Resultate?

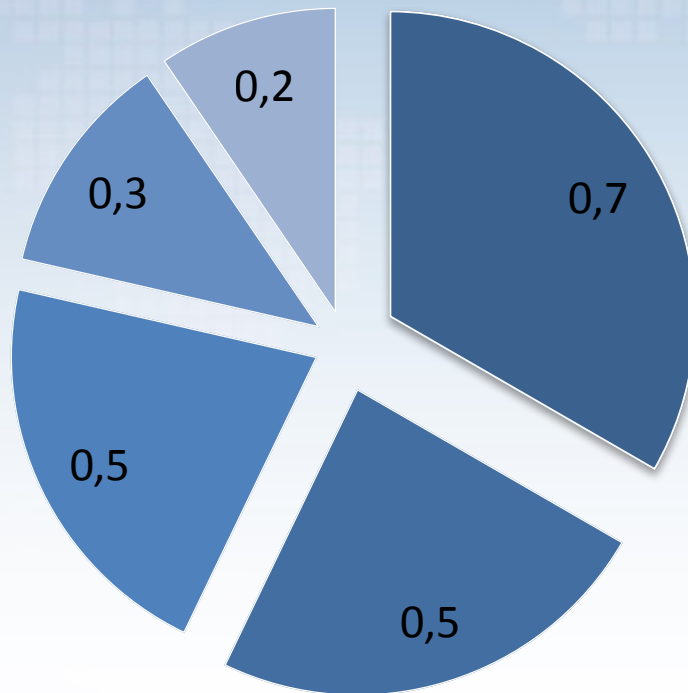
EIN JAHR APPTESTING IM RÜCKBLICK

Ein Jahr AppTesting im Rückblick



- Rund 220 getestete Apps
- Über 400 kritische Schwachstellen aufgedeckt
- 12 Apps der Third-Party Apps für Benutzung im Unternehmen verboten
- 24 Apps der Third-Party Apps für Benutzung im Unternehmen eingeschränkt
- Rund $\frac{3}{4}$ der getesteten Apps mussten nachgebessert werden

Prozentualer Anteil der Schwachstellen in den getesteten Apps





















- Insufficient Transport Layer Protection
- Lack of Binary Protections
- Insecure Data Storage
- Poor Authorization and Authentication
- Other Issues



















Kosten < - > Ergebnis

MOBILE APPT TESTING MATRIX

Mobile AppTesting Matrix

	Kosten		Anzahl erkannter Schwachstellen			Auswirkung
	Wissen	Zeit	Code	Design	Privacy	Risiko
voll-automatisiert						
teil-automatisiert						
manuell						

Mobile AppTesting Matrix

	Kosten		Anzahl erkannter Schwachstellen			Auswirkung
	Wissen	Zeit	Code	Design	Privacy	Risiko
voll-automatisiert						
teil-automatisiert						
manuell						

	SSL	Backup-Flag	NSFile Protection	Daten-ablage	Zugangs-schutz	Keychain
manuell	X			X	X	
automatisiert		X	X	(X)		X

Vielen Dank für Ihre Aufmerksamkeit!

Dr. Michael Spreitzenbarth
Siemens CERT
Email: michael.spreitzenbarth@siemens.com

Jennifer Bombien
Siemens CERT
Email: jennifer.bombien@siemens.com

