



OWASP

Open Web Application  
Security Project

# Why Organisations should rely on Mobile AppTesting

Dr. Michael Spreitzenbarth & Jennifer  
Bombien

Siemens CERT

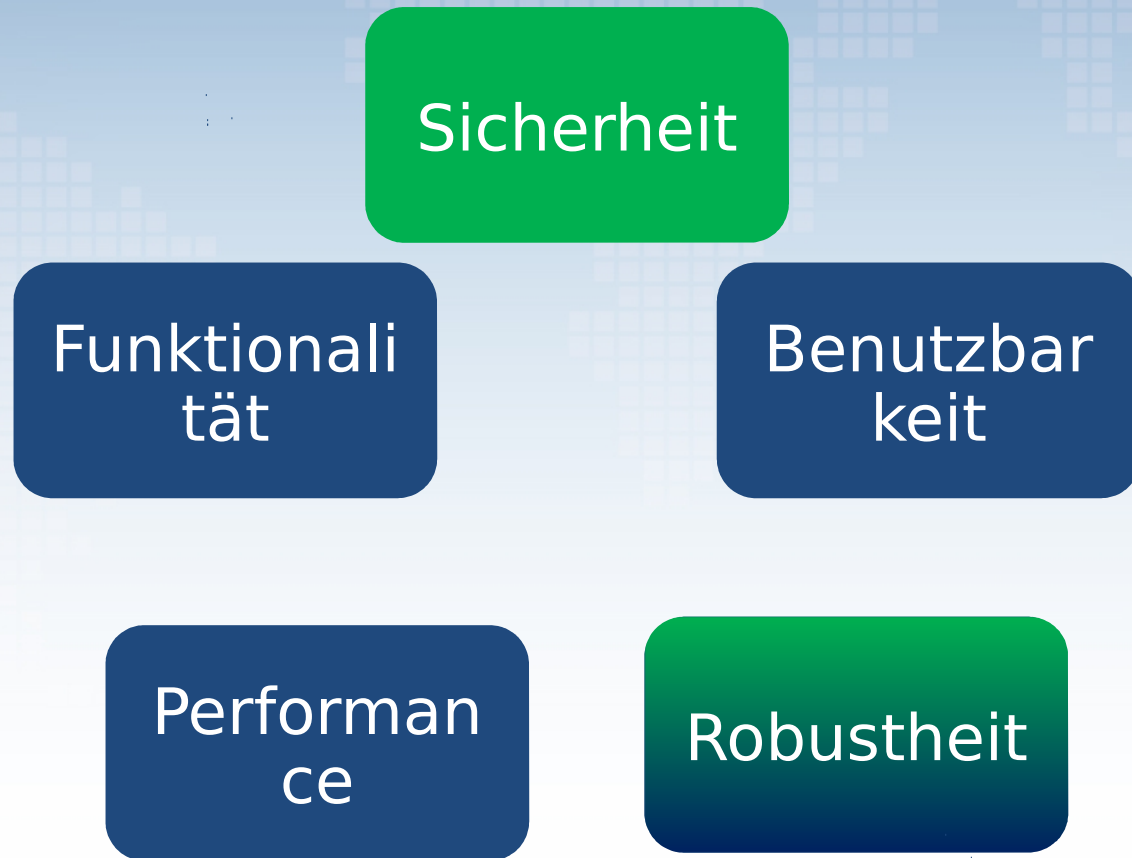
# Agenda

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

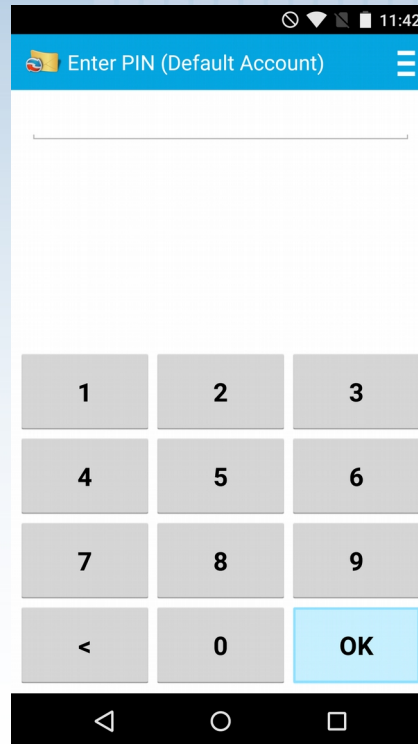
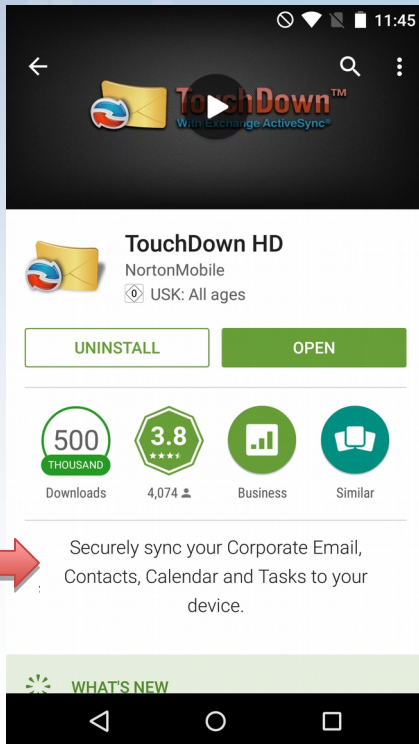
Welche Möglichkeiten zum Testen von Apps gibt es?

# **VERIFIZIEREN MOBILER APPS**

# Testmöglichkeiten mobiler Apps



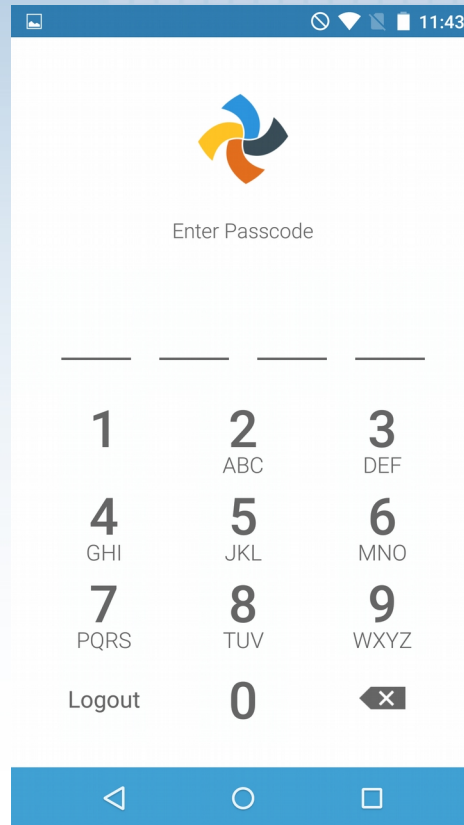
# Praxisbeispiel: TouchDown



```
.....
ASVersions=Versions:Microsoft-IIS/7.5
AccountID=Exchange Mail
.....
Domain=#EFT1.7#I0VGVD*****
FailedLoginAttemptCount=0
FolderSyncKey=1
LastPINPromptTime=1421767231987
LastPinChangeTime=1421766891980
LastPolicyGet=0
.....
PasswordHistory=14141414
PasswordHistory=#EFT1.7#I0VG*****
PasswordRecoveryEnabled=false
PolicyKey=814518012
.....
```



# Praxisbeispiel: Syncplicity



```
<?xml version='1.0' encoding='utf-8'
standalone='yes' ?>

<map>
.....
<string
name="passcode">ICPNS*****</string
>
</map>
```

# 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 Infrastruktur-richtlinien 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	ooo
Snoop-it	iOS	dynamisch	(X)	X	manuell	oo
Cycrypt	iOS	dynamisch	---	X	manuell	ooooo
MobileSandbox-NG	Android	beides	X	---	automatisiert	oo
Androguard	Android	statisch	X	X	manuell	oooo
Drozer	Android	beides	(X)	X	beides	ooooo
DroidBox	Android	dynamisch	X	---	automatisiert	oo
CuckooDroid	Android	dynamisch	X	(X)	automatisiert	ooo
AuditDroid	Android	beides	---	X	beides	oooo
NowSecure Lab	beides	beides	X	X	beides	oooo




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

# **APPTESTING KONZEPT ALS UNTERNEHMENSLÖSUNG**

# 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

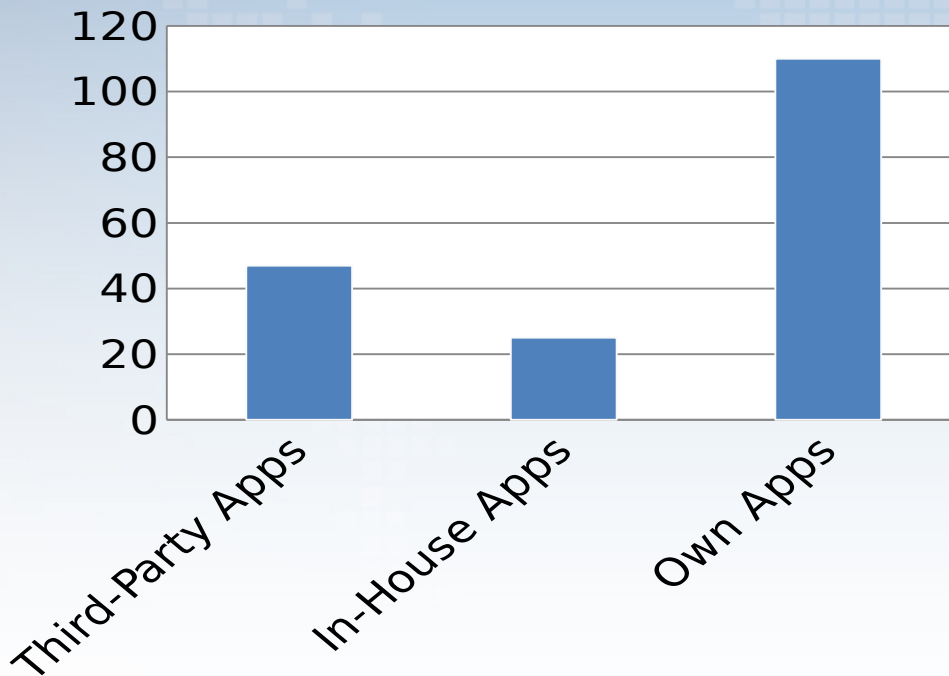
- 20% automatisiert
- 80% manuell
- Privacy / Datenschutz
- Schwachstellen im Code
- Schwachstellen im Design
- Ausführlicher Report mit Unterstützung für den Entwickler

- Aufwand nach Absprache
-  Noch tiefere und ausgereifere Tests (>5 Tage)

Was sind die Resultate?

# **EIN JAHR APPTESTING IM RÜCKBLICK**

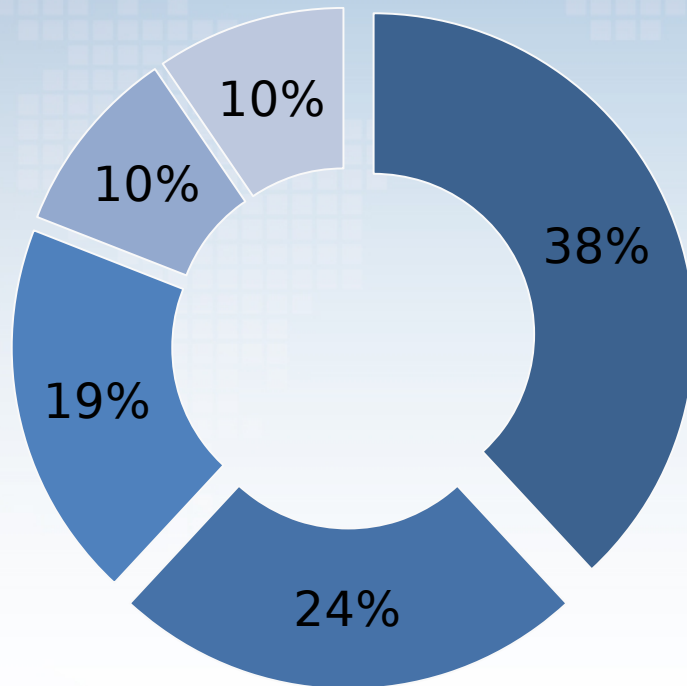
# Ein Jahr AppTesting im Rückblick



- Rund 180 getestete Apps
- Über 340 kritische Schwachstellen aufgedeckt
- 9 Apps der Third-Party Apps für Benutzung im Unternehmen verboten
- 15 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						Auswirkung		
	Wissen 	Zeit 			SSL	Backup-Flag	NS File Protection	Datenablage	Zugangsschutz	Keychain	   Risiko
voll-automatisiert											
teil-automatisiert											
manuell											
				manuell				X	X		OWASP Open Web Application Security Project
				automatisiert	X	X	X	(X)		X	

# Vielen Dank für Ihre Aufmerksamkeit!



Dr. Michael Spreitzenbarth  
Siemens CERT  
Email:  
[michael.spreitzenbarth@siemens.com](mailto:michael.spreitzenbarth@siemens.com)  
m

Jennifer Bombien  
Siemens CERT  
Email:  
[jenifer.bombien@siemens.com](mailto:jenifer.bombien@siemens.com)