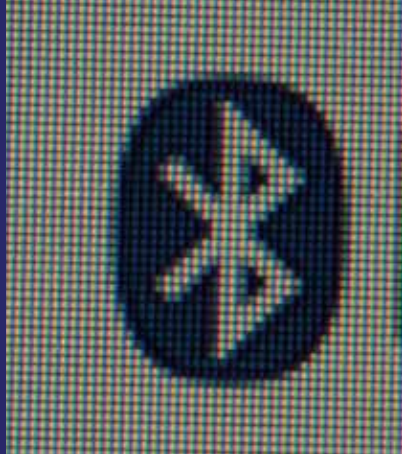
Fraunhofer
SIT

FRAUNHOFER-INSTITUT FÜR SICHERE INFORMATIONSTECHNOLOGIE

# MOBILE SYSTEMS

## TECHNISCHE BERATUNG, TESTS & LÖSUNGEN

# SECURITY FÜR SMARTPHONES & TABLETS



## TRENDS

**Consumerisation of IT**

IT-Trends gehen heute vom Massenmarkt aus. Besonders deutlich ist dies bei den Smartphones und Tablet-PCs. Sie wurden zwar nicht für den professionellen Arbeitseinsatz entwickelt, kommen jetzt jedoch verstärkt in Unternehmen zum Einsatz. Mitarbeiter nutzen diese Smart Devices oft sowohl privat als auch geschäftlich. Unternehmen suchen deshalb nach Lösungen, die unternehmenskritische Daten und Dienste schützen und ein effizientes Management der mobilen Geräte ermöglichen.

**Mobile Malware**

Laut Mobile Threat Report von F-Secure ist die Menge an mobiler Malware im ersten Halbjahr 2012 um 64 Prozent gestiegen. Den größten Zuwachs verzeichnet Schadsoftware für das mobile Betriebssystem Android. Oft nutzen Malware-Programme Hintertüren, die in scheinbar harmlose Apps einprogrammiert wurden. Bei Installation einer solchen App können Angreifer die Kontrolle über das Gerät übernehmen, auf sensible Daten und Dienste zugreifen oder Gespräche über das Mikrophon belauschen.

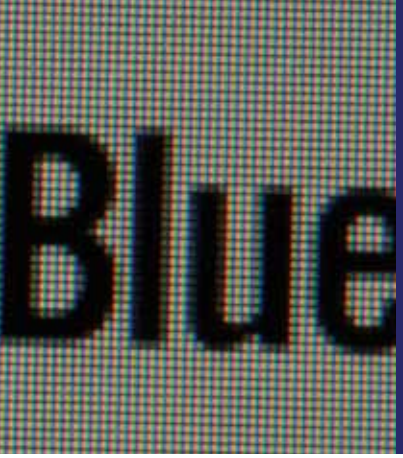
**Advanced Persistent Threats**

Jüngste Schadensfälle zeigen, dass Angreifer immer professioneller vorgehen. Gegen diese gezielten Angriffe, die teils mit großem Aufwand und Sachverstand durchgeführt werden, helfen Standardschutzmaßnahmen nicht.

## HERAUSFORDERUNGEN

Beim Einsatz mobiler Geräte sollten Unternehmen die Schwächen in Betriebssystemen und drahtlosen Schnittstellen beachten. Eine zusätzliche Herausforderung bildet die gemischte Nutzung von mobilen Geräten für geschäftliche und private Zwecke. Was geschieht wenn das Gerät verloren geht oder sensible Geschäftsdaten ungewollt das Unternehmen verlassen? Was wenn Angreifer über das mobile Gerät auf kritische Unternehmensdienste zugreifen? Wie lassen sich die Geräte einfach und flexibel verwalten (Mobile Device Management), und dürfen Unternehmen dabei private Daten sichern?

Wer gutes Personal gewinnen möchte, sollte die Freiheitsgrade der Mitarbeiter entsprechend ausweiten, ohne die IT-Risiken zu vernachlässigen. Noch gibt es keine etablierten Methoden, wie sich Konzepte des Dual Use oder Bring-your-own-device verantwortungsvoll und zugleich einfach realisieren lassen. Zentrale Herausforderungen bleiben die Sensibilisierung der Nutzer sowie das Management mobiler Geräte und der auf ihnen genutzten Daten über den gesamten Lebenszyklus hinweg. Fraunhofer SIT besitzt Erfahrung mit iOS, Android und weiteren gängigen Betriebssystemen. Die Mitarbeiter des Instituts härten mobile Systeme, entwickeln innovative Anwendungen und Sicherheitsmodule, bewerten existierende Produkte und unterstützen Unternehmen und Behörden mit umfangreichem Know-how und Herstellerneutralität.



## ANGEBOTE

**Security for Smart Devices / Dual Use / BYOD:**

- Technische Beratung zu iOS, Android und anderen OS
- Bewertung existierender Lösungen
- Integration geschützter mobiler Endgeräte
- Konzepte für sicheres Mobile-Device-Management
- Sichere Konfiguration von Smart Device-Lösungen
- Anpassung bestehender Systeme
- Awareness-Workshops für Mitarbeiter und Management

**Testlabor Mobile Security:** Sicherheitsanalysen mobiler Plattformen und Infrastrukturen, praktische Tests von Smartphone-Lösungen, Apps, etc. – mit/ohne Testat

## KUNDENNUTZEN

- Zeitvorteil durch herstellerneutrales Know-How, das sofort nutzbar ist
- Investitionssicherheit und Risiko-Minimierung durch belastbare Sicherheitsbewertungen von Technologien, Prozessen und Produkten
- Benutzerfreundliche Sicherheit
- Erhöhung der Mitarbeitereffizienz durch Mobilisierung von Geschäftsprozessen bei abschätzbarem unternehmerischem Risiko
- Etablierung von sicheren und hochsicheren Netzen auch in komplexen Einsatzszenarien wie Femtozellen oder kritischen Infrastrukturen

## REFERENZEN

**Sicherheitsanforderungen für den iPAD-Einsatz**

Die Lufthansa AG beabsichtigt, seinen Kabinenbesatzungen iPads als neue Arbeitsgeräte zur Verfügung zu stellen. Die vielseitigen Geräte sollen auch privat von den Mitarbeitern genutzt werden dürfen. Da in der dienstlichen Nutzung zum Teil personenbezogene Daten von Mitarbeitern und Kunden verarbeitet werden, hat die Lufthansa AG umfängliche Anforderungen zum Schutz der Daten vorgegeben. Wichtigste Anforderung ist die Vertraulichkeit der Daten durch strikte Trennung der dienstlichen und privaten Nutzung sowie das Durchsetzen einer sicheren Konfiguration. Fraunhofer SIT hat für diesen Anwendungsfall einen Katalog zu berücksichtigender Aspekte der IT-Sicherheit von iOS-Geräten zusammengestellt und spezifische Maßnahmen zur Implementierung und Konfiguration sowie angepasste organisatorische Prozesse entwickelt, mit denen die Sicherheitsanforderungen eingehalten werden können.

**Sicherheitsanalyse für Gerätemanagment unter iOS**

Fraunhofer SIT hat gemeinsam mit der Datev mehrere Projekte durchgeführt, in denen die mobilen Geräte auf Basis iOS (Apple) auf ihre Sicherheit gegen externe und interne Angreffe hin getestet wurden. Fraunhofer SIT hat Techniken des Reverse Engineering eingesetzt, um mögliche Schwächen und Bedrohungen des iOS-Betriebssystems und der Mobile Device Management Strategie aufzudecken.

## LÖSUNGEN

**BizzTrust for Android**

Fraunhofer SIT hat eine Smartphone-Lösung entwickelt, die geschäftliche Daten und Anwendungen auf Smartphones schützt, ohne die private Nutzung des Geräts einzuschränken. Die Lösung unterstützt die sichere Kommunikation mit dem Unternehmen per VPN und bietet die Möglichkeit für Remote Update und automatisches Policy Enforcement.

www.bizztrust.de

**MobileSitter/iMobileSitter**

Zum sicheren Umgang mit Passwörtern hat Fraunhofer SIT mit MobileSitter und iMobileSitter eine Software für Handys bzw. iPhones erstellt, die einen Schutz der Passwörter auch dann gewährleistet, wenn das Handy gestohlen oder verloren wird. Fraunhofer SIT hat dazu ein patentiertes kryptographisches Verfahren entwickelt.

www.imobilesitter.com

## DAS INSTITUT

Die Informationstechnologie hat bereits weite Teile unseres Alltags durchdrungen: Ob Auto, Telefon oder Heizung – ohne IT-Einsatz sind die meisten Geräte und Anlagen heute nicht mehr denkbar. Insbesondere Unternehmen nutzen IT-Systeme zur effektiven Gestaltung ihrer Arbeitsprozesse. Fraunhofer SIT beschäftigt sich mit dem Schutz dieser Systeme vor Ausfällen, Angriffen und Manipulationen.

Fraunhofer SIT ist für Unternehmen aller Branchen tätig. Viele erfolgreiche Projekte mit internationalen Partnern sind eindrucksvoller Beweis für eine vertrauensvolle Zusammenarbeit. Zu unseren Kunden zählen unter anderem HP, die Software AG, SAP, Lufthansa und das Bundesamt für Sicherheit in der Informationstechnik.

## KONTAKT

*Oliver Küch*
*Telefon 06151 869-213*
*Fax 06151 869-224*
*oliver.kuech@sit.fraunhofer.de*

**Fraunhofer-Institut für Sichere Informationstechnologie**
*Rheinstraße 75*
*64295 Darmstadt*
*www.sit.fraunhofer.de*