Smartphones im Unternehmen

Philipp Schaumann
Dipl. Physiker
Erste Group Bank AG
Group Security Management
philipp.schaumann@erstegroup.com

Agenda

- Smartphones an sich
- Cloud und Games
- Privat vs. Business
- Lösungsoptionen (heute und in der Zukunft)

Smartphones sind unsicher – oder ?

- Jede Menge Privatsphäre-Verletzungen durch Benutzer-Apps
- App-Entwickler „opfern“ Sicherheitsfeatures wie Verschlüsselung dem schnellen Time-to-Market
- Betrügerische Apps (Mehrwertnummer-SMS, u.ä.) sind im Umlauf
- Falsche Banken-Apps verwirren die Kunden und fangen Passworte ab
- Aber der (von einigen) erwartete Zusammenbruch der Sicherheit ist ausgeblieben – der Bedarf für Anti-Malware hält sich in Grenzen

Panikmeldungen in 2011

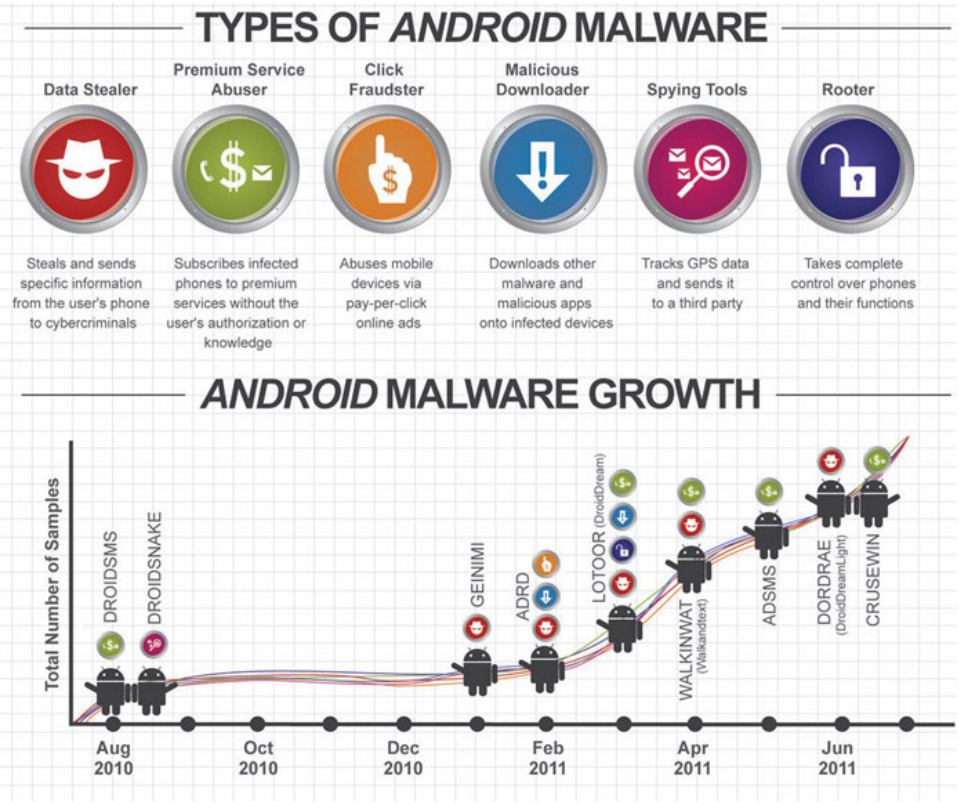
Thema Android

- Mit einem Anstieg um 76 Prozent ist Android das am häufigsten angegriffene mobile Betriebssystem und hat damit Symbian abgelöst.
- Bis zu 55.000 neue Formen von Malware, die auf Googles Software abzielen, würden pro Tag registriert werden. Die meisten Schad-Programme würden in Apps eingeschleust werden, etwa über gefälschte Updates für Spiele wie "Angry Birds".

55.000 neue Malware-Samples pro Tag, stimmt das wirklich?

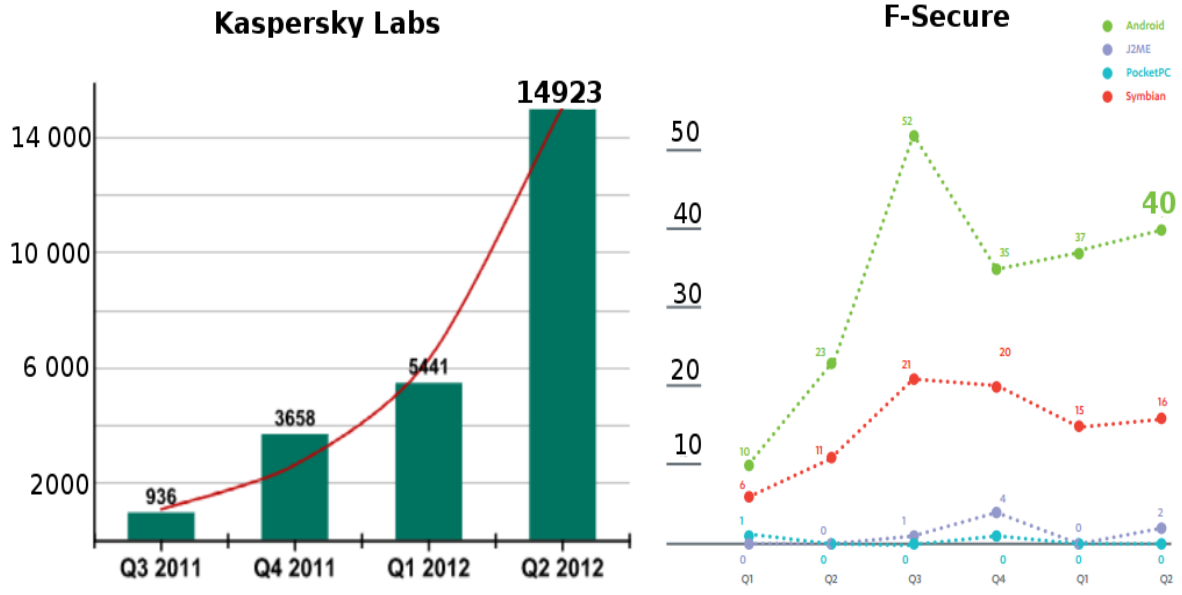
http://www.mcafee.com/us/about/news/2011/q3/20110823-01.aspx

Android Malware (Okt. 2011)



 Quelle: http://blog.trendmicro.com/snapshot-of-android-threats

Korrektur 2012: Kaspersky vs. F-Secure



Kaspersky zählt jede neue Erkennungs-Signatur als neue Malware

Smartphones
Stärken und Schwächen

Stärken

- Sandboxes zur Isolierung von benutzer-installierten Prozessen – wichtigste Sicherheitsfeature
  Dadurch deutlich höhere Sicherheit verglichen mit MS Windows und MacOS

- Trend zu hardware-basierter Speicherverschlüsselung

Behauptung:
Smartphones, von der Technologie her, sind sicherer als die meisten heutigen Computer

Fraunhofer März 2011:
http://www.dfn.de/fileadmin/3Beratung/Betriebstagungen/bt54/forum-mobileit-heider.pdf

Sicher - wären da nicht Cloud und der menschliche Spieltrieb

- Smartphones werden IMMER in Verbindung mit der Cloud genutzt
- Die Zahl der wirklich sicheren Cloud-Lösungen liegt sehr nahe bei Null
- „User Experience“ schlägt Sicherheitsbedürfniss jederzeit

Smartphones
Stärken und Schwächen (2)

ERSTE
ERSTE GROUP

Schwächen

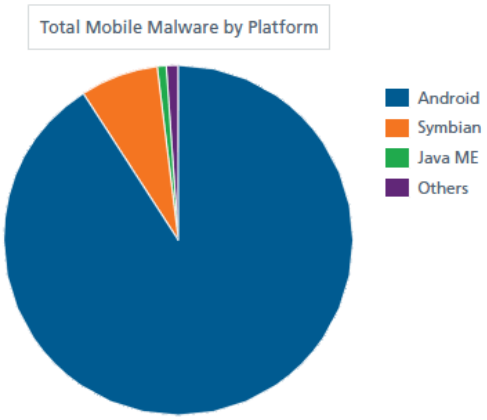
- Die größte Achilles Ferse bei beiden sind jailbreaking / rooting

- Privatsphäre-Probleme durch oft unkontrollierte Zugriffe der Apps auf Benutzerdaten und/oder Systemfunktionenen (Telefon, GPS, Adressbücher, etc.)
  → theoretisch in der Zukunft lösbar

- Sehr begrenzte Virtualisierungsmöglichkeiten
  → praktisch lösbar in der Zukunft

Smartphones
Stärken und Schwächen (3)

Spezielle Schwächen des Android

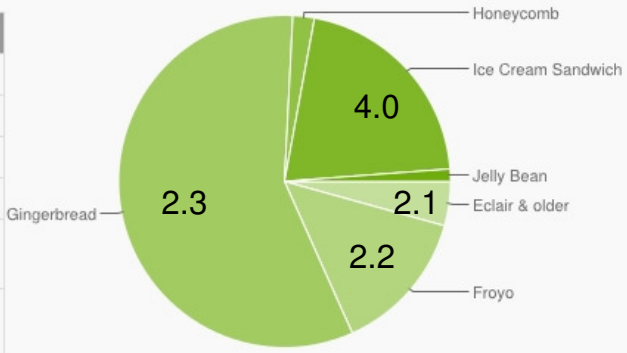


- Die größten Probleme von Android sind die Apps
  - Leichtes Re-engineering (Java Byte-Code), dadurch viele „Fake Apps“, mit oder ohne bösen „Zusatzfunktionen“
  - Unkontrollierbare „alternate markets“
  - Keine trusted digital signature

- Viele OS-Versionen – komplizierte oder fehlende Software-Updates durch Hersteller plus Netzbetreiber (falls überhaupt) – 2-fach Branding

50% aller Android Geräte liegen 2 Hauptupdates zurück

Version	Codename	API	Distribution
1.5	Cupcake	3	0.2%
1.6	Donut	4	0.4%
2.1	Eclair	7	3.7%
2.2	Froyo	8	14%
2.3 - 2.3.2	Gingerbread	9	0.3%
2.3.3 - 2.3.7		10	57.2%
3.1	Honeycomb	12	0.5%
3.2		13	1.6%
4.0 - 4.0.2	Ice Cream Sandwich	14	0.1%
4.0.3 - 4.0.4		15	20.8%
4.1	Jelly Bean	16	1.2%



Data collected during a 14-day period ending on September 4, 2012

http://www.techrepublic.com/blog/security/the-problem-with-android-updates-playing-the-blame-game/8474

iPhone vs. Android Quelle: Symantec 2011

Table 1
Resisting attack types

Resistance to:	Apple iOS	Google Android
Web-based attacks		
Malware attacks		
Social Engineering attacks		
Resource Abuse/ Service attacks		
Data Loss (Malicious and Unintentional)		
Data Integrity attacks		

Table 2
Security feature implementation

Security Pillar	Apple iOS	Google Android
Access Control		
Application Provenance		
Encryption		
Isolation		
Permission-based Access Control		

Legend
- Full Protection
- Good Protection
- Moderate Protection
- Little Protection
- Little or No Protection

http://www.symantec.com/content/en/us/about/media/pdfs/symc_mobile_device_security_june2011.pdf

Heute: „Coolness“ ist gefragt

ERSTE GROUP

„Out“

„In“ weil „cool“

Resultat: Die Smartphone-Herausforderung für Firmen

ERSTE GROUP

- Ein Arbeitsplatz-Gerät
  - auf dem der Anwender beliebige Software installieren kann
  - der Anwender volle Administrationsrechte hat
  - das in einem Öko-System genutzt wird, dass außerhalb unserer Kontrolle liegt (z.B. iCloud, DropBox, etc.)

  hätten die Security Abteilungen einer Bank früher nicht akzeptiert

Privat oder Business

Seit wann sind die Privatgeräte der Mitarbeiter und Kunden ein Thema für uns?

- **Kunden** erwarten, dass sie ihre Bankgeschäfte auch auf den mobilen Geräten erledigen können – dann wenn sie z.B. in der U-Bahn Zeit dafür haben

- **Mitarbeiter** erwarten heute, dass ihre Privatgeräte von der Firmen-IT unterstützt werden, zumindest dass die Mitarbeiter die Emails, Termine, Kontakte synchronisieren können

Privat oder Business

Seit wann sind die Privatgeräte der Mitarbeiter und Kunden ein Thema für uns?

- **Kunder**
  den Mo
  der U-B

- **Mitarbe**
  Firmen-
  Mitarbei
  können

Kontrollverlust bei der Firmen-IT

Kübler-Ross Modell - Five Stages of Grief
http://en.wikipedia.org/wiki/K%C3%BCbler-Ross_model

Acceptance:
„Bring Your Own Device“ B.Y.O.

ERSTE GROUP

September 22, 2011 The New York Times

More Offices Let Workers Choose Their Own Devices

By VERNE G. KOPYTOFF

SAN FRANCISCO — Throughout the information age, the corporate I.T. department has stood at the chokepoint of office technology with a firm hand on what equipment and software employees use in the workplace.

They are now in retreat. Employees are bringing in the technology they use at home and demanding the I.T. department accommodate them. The I.T. department often complies.

Some companies have even surrendered to what is being called the consumerization of I.T. At Kraft Foods, the I.T. department's involvement in choosing technology for employees is limited to handing out a stipend. Employees use the money to buy whatever laptop they want from Best Buy, Amazon.com or the local Apple store.

I.T. Departments Lose Their Clout Over Phone Choices

By VERNE G. KOPYTOFF

http://bits.blogs.nytimes.com/2011/09/22/i-t-departments-lose-their-clout-over-phone-choices/
http://www.nytimes.com/2011/09/23/technology/workers-own-cellphones-and-ipads-find-a-role-at-the-office.html

Acceptance:
„Bring Your Own Device“ B.Y.O.

ERSTE GROUP

CISCO PRESS RELEASE

SAN JOSE, Calif. – Jan. 24, 2012

Global IT Survey Highlights Enthusiasm over Tablets in the Enterprise, Shows Customization, Collaboration and Virtualization as Key Features

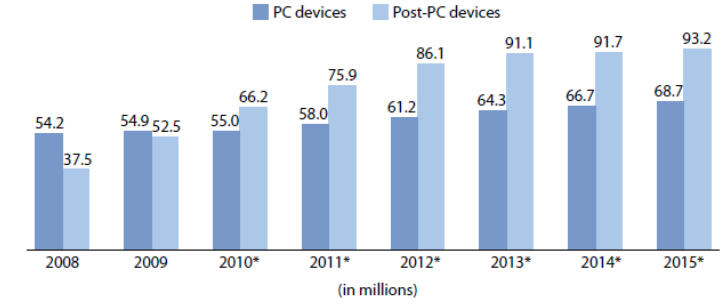
Zitat:
Globally, 48% said their company would never authorize employees to bring their own devices (BYOD), yet 57% agreed that some employees use personal devices without consent.

http://newsroom.cisco.com/press-release-content?type=webcontent&articleId=658006

Security In The Post-PC Era: Controlled Chaos - Forrester Research

ERSTE GROUP

- Devices are pocketable – data-on-the-move un-encrypted
- They run stripped-down operating systems
- Customers add „apps“, IT doesn‘t install „applications“
- Vendors own the security of the platform incl. user experience (d.h. auch Security Experience)



Source: Forrester Research eReader Forecast, 2010 To 2015 (US)
*Forrester forecast

57025

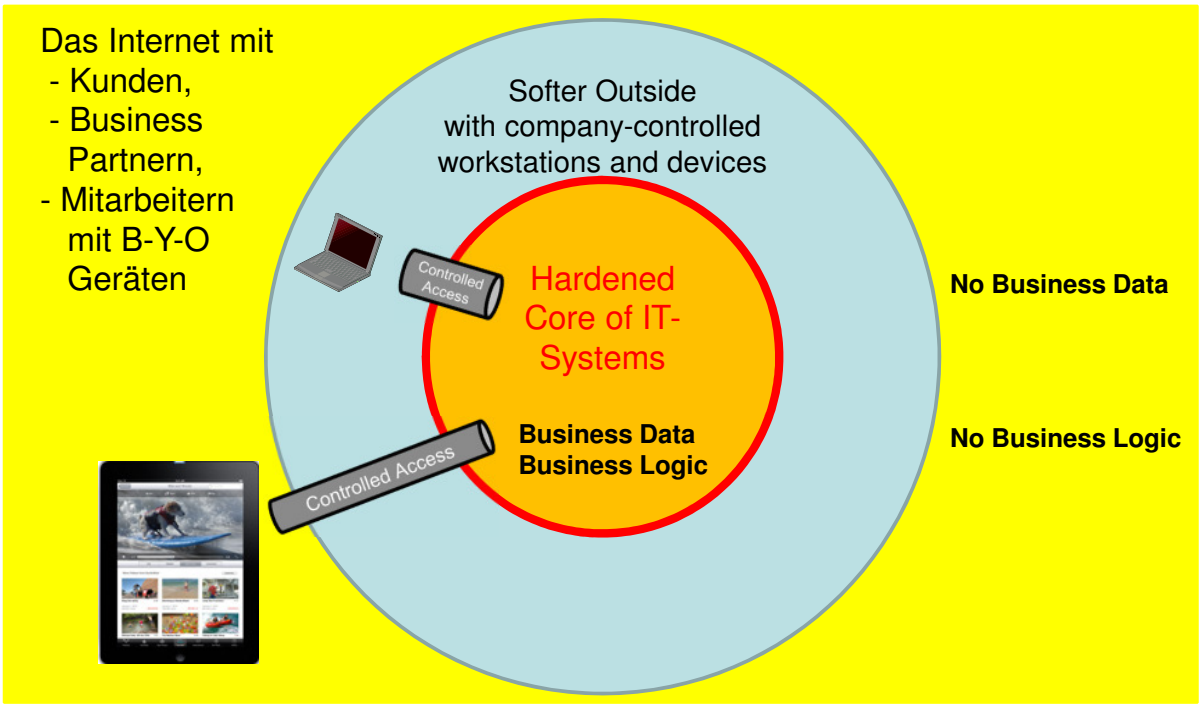
Source: Forrester Research, Inc.

Consumerization of Business Devices - And the Winner is . . . .

ERSTE GROUP

Und vielleicht auch die Information Security ????

Das Jericho Konzept – De-Perimeterisation



http://en.wikipedia.org/wiki/Jericho_Forum
http://www.opengroup.org/jericho/commandments_v1.2.pdf

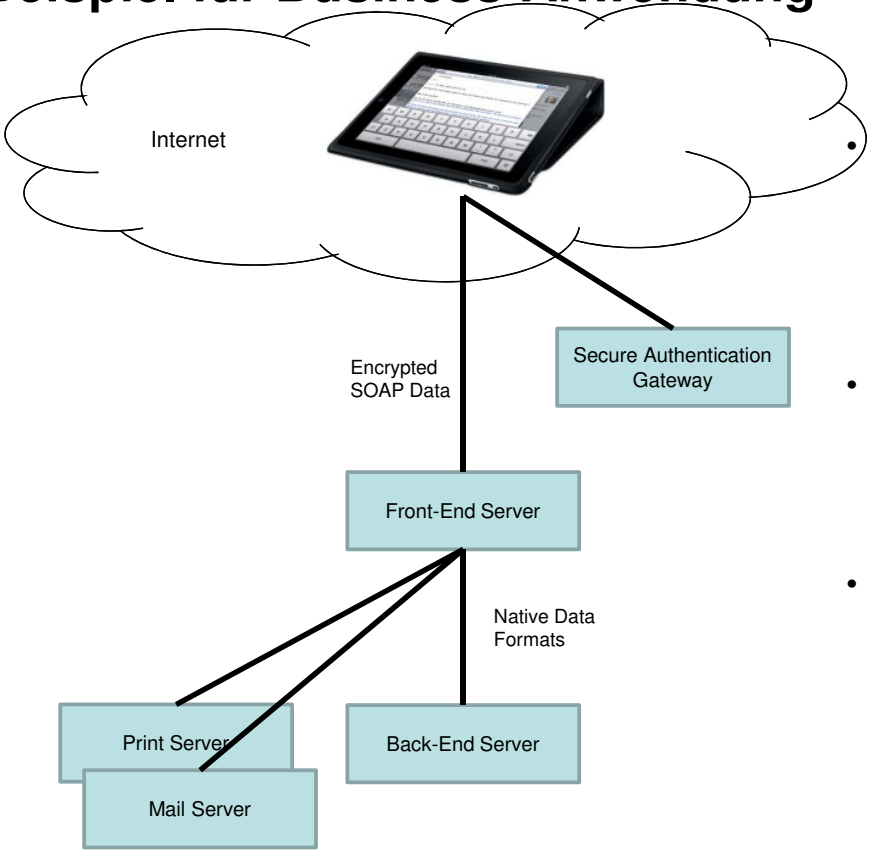
Ein Beispiel aus dem Kundenbereich

- **Keine Daten auf dem Gerät**
- **Kein Caching, kein Auto-Complete**
- **Programm läuft in einer „ausreichend sicheren“ Sandbox**
- **Ausreichender Schutz gegen Fake-Apps**
- **Proprietäre Software**
  → keine Browser-Plugins möglich

Beispiel für Business-Anwendung

- Keine Daten auf dem Gerät, alle Daten kommen von den Servern des inneren Bereichs
- Gut kontrollierter Zugang, 2-Faktor Authentifizierung
- Nutzungsmöglichkeit wo immer Internet-Zugang ist

Beispiel für Business-Anwendung



- Keine Daten auf dem Gerät, alle Daten kommen von den Servern des inneren Bereichs
- Gut kontrollierter Zugang, 2-Faktor Authentifizierung
- Nutzungsmöglichkeit überall wo Internet-Zugang ist

Aktuelle Herausforderung E-Mail

ERSTE GROUP

- Starke Anforderung nach Offline Arbeit, d.h. Businessdaten auf dem Gerät
- Apple: Email ist einzige App von Apple die „enhanced security“ verwendet, aber Weitergabe von Anhängen an andere Apps, z.B. ebook-reader erstellt ungeschützte Kopien
- Lösungsansätze können in der Sicherheit einer „enhanced security“ App und dem Sandbox-Konzept liegen
- Produkte liegen für iOS und Android vor, bzw. sind in Arbeit

- Aber: Jailbreaking / Rooting

Wie kann ein mobile Device zum Business Tool werden? – 2 Anforderungen

ERSTE GROUP

Virtualisierung der Geräte

Aus 1 mach 2

Der “Fun-Factor” der Geräte bleibt erhalten – die Business Daten sind geschützt

Plus MDM:

Kontrolle (zumindest des Business-Phones) und die Verfügbarkeit eines Not-Aus-Knopfes mittels Mobile Device Management

Zweite Forderung:
MDM – Mobile Device Management

Mobile device Management (MDM) gibt zentrales Management und Kontrolle aber alle Smartphones.

Die wichtigsten Funktionen:

- Verwaltung der Geräte und Status-Übersicht (OS-Level, etc.)
- Verteilung und Kontrolle von vielen lokalen Einstellungen
- Erzwingung von Security Policies
- Löschen von Daten, Verteilung von Security Zertifikaten
- Kontrolle über die Active Sync Settings, Möglichkeit der Löschung der Firmen-Mails
- Kontrolle der Security Settings und rules, z.B. jailbreak Erkennung, etc.
- Begrenzte Kontrolle über die installierten Apps
- Unterstützung von Remote Support durch Bildschirmübernahme

Smartphone-Virtualisierung wird von immer mehr Firmen als Opportunity gesehen

4 Virtualisierungsoptionen

ERSTE GROUP

Work in Progress

Lokal auf dem Gerät

Komplettes virtuelles Phone in Corporate Sandbox

1 Anwendung z.B. Mail in Corporate Sandbox

Anforderungen:
- Getrennte Wipes
- Getrennte Passcode/ Passwords

Remote über Netzzugriff

Remote Zugriff auf einen Remote Desktop

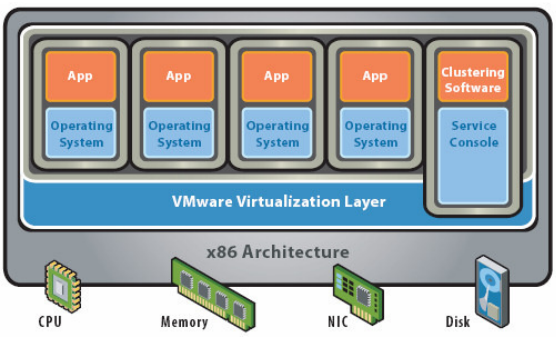
Remote Zugriff auf eine Anwendung

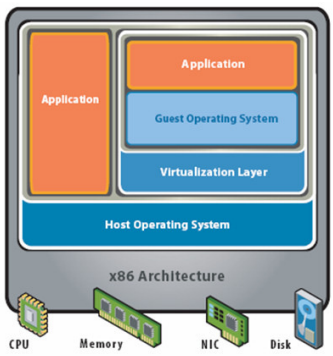
Stand der Technik 2012

Siehe auch: IBM X-Force
http://public.dhe.ibm.com/ DF

Two conceptual Approaches

ERSTE





Virtualisation Layer kontrolliert die Hardware

Virtualisation Layer ist „guest“ des Operating Systems

Die wirklich sichere Implementierung ist nur die Kontrolle über die Hardware

Theoretisch kann das Guest-System anders sein als der Host, z.B. Android auf iOS

Stand 2012
Virtualisierung Smartphone OS

ERSTE GROUP

– Option 1 –
Virtualisierungslayer als unterste Schicht ist für Mobile Devices (derzeit) nicht umsetzbar

– Option 2 –
Guest System über dem Host System ist bei infiziertem / rooted / jail-broken nicht sicher
(Beispiel Vmware Mobile Horizon für Android)

Conclusio 2012:
Work in Progress – aber der Weg in die Zukunft

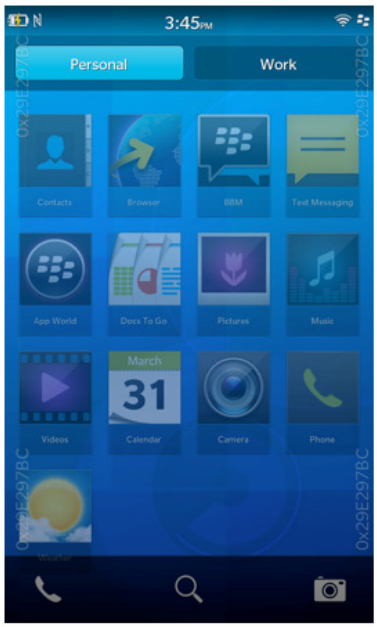
Herausforderungen bei der Virtualisierung des Geräts selbst

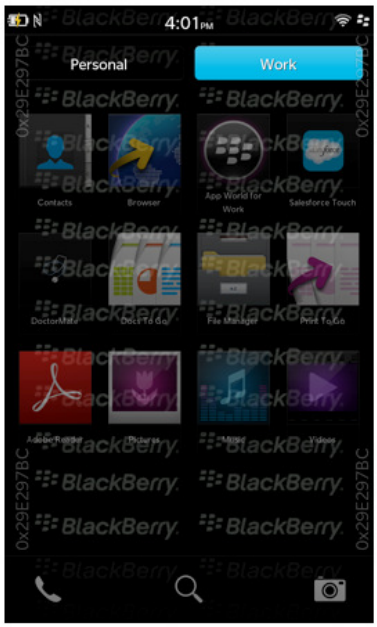
ERSTE GROUP

- **Virtualisierung von iOS benötigt die Unterstützung von Apple. Hauptthema für Apple ist aber „User Experience“**
  (Lösungen daher nur auf App-Basis)
- **Virtualisierung von Android ist vergleichsweise einfach, die (fast unendliche) Vielfalt von Hardware und (Provider-)Versionen verhindert aber die sichere Implementierung auf der Hardware-Ebene**
- **Virtualisierung durch Remote Zugriff erfordert Entscheidung über sichere Authentisierung**

Blackberry BB10

- Separate Apps (kompatibel mit Android)
- separate Termine (gemeinsam angezeigt)
- separate Adressbücher (gemeinsam angezeigt)
- Separate Filespaces
- Kein Copy & Paste zwischen Work und Personal
- USB nur in Personal Mode





http://bizblog.blackberry.com/2012/09/blackberry-balance-on-blackberry-10/?CPID=E020C072&Date=101112

Alternative Lösung statt Virtualisierung: Corporate E-mail in der App Sandbox (1)

„Good Technology“

Durch eine Trennung der Email-Funktionalität in einer separate „App“ kann eine Separierung zwischen Privat und Business erreicht werden

•Probleme:

- Wenn Anhänge aus der Umgebung entfernt werden, so entfällt die erhöhte Sicherheit
- D.h. begrenzte Funktionalität oder Einschränkung der Sicherheit
- Keinen direkten Support für Active Sync, erfordert separaten Server

http://www.good.com/

Alternative Lösung statt Virtualisierung: Corporate E-mail in der App Sandbox (2)

ERSTE GROUP

Excitor DME (Dynamic Mobile Exchange)

- **Excitor DME is a 'One App' Enterprise Mobility solution for your employees to securely access Corporate email and Business Applications on their favourite mobile device**

Wmware: Mobile Horizon für iOS

- **Apps werden automatisiert für Ausführung in einer extra Sandbox vorbereitet (wie bei ThinApp)**

Alternative Lösung statt Virtualisierung: Corporate E-mail in der App Sandbox (3)

ERSTE GROUP

Für Android: Touchdown E-Mail Client von Nitrodesk

Touchdown

- Secure Corporate Email auf Android
- Integration mit Active Sync und Exchange
- Gute Integration mit MDM