e.biz-Veranstaltung

Veranstaltungsreihe: „Die Mittelstandsoffensive erklärt IT“

Lösungen und Sicherheit von mobilen Lösungen

Prof. Dr.-Ing. Kai-Oliver Detken
Geschäftsführer
DECOIT GmbH
URL: http://www.decoit.de
E-Mail: detken@decoit.de

Partner der Mittelstands-offensive

Eine Initiative der WFB Wirtschaftsförderung Bremen GmbH

Consultancy & Internet Technologies

Kurzvorstellung der DECOIT GmbH

- Gründung am 01.01.2001 als reines Consulting-Unternehmen
- Fokus: Herstellerneutrale, ganzheitliche Beratung
- Zielsetzung: akademische Lösungsansätze in kommerzielle Marktprodukte/Lösungen umsetzen
- 2002: Hinzunahmen des Systemmanagements, um Herstellerlösungen oder stabile Open-Source-Lösungen anzubieten
- 2003: Hinzunahme der Software-Entwicklung, um im Individualbereich innovative eigene Lösungen zu entwickeln oder Herstellerlösungen zu ergänzen
- Heute: Full-Service-Anbieter im IT-Bereich
- Sitz im Technologiepark an der Universität Bremen
- Enge Kooperationen zu Herstellern, Anbietern und Hochschulen bzw. Universitäten
- Aktueller Mitarbeiterstand: 15

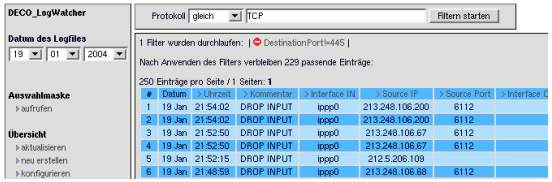
Dienstleistungen / Portfolio

- **Technologie- und Markttrends**, um strategische Entscheidungen für und mit dem Kunden vor einer Projektrealisierung treffen zu können
- **Solutions (Lösungen)** zur Identifizierung der Probleme und Angebot einer Lösung für die Umsetzung eines Projekts
- Kundenorientierte **Workshops, Coaching, Schulungen** zur Projektvorbereitung und -begleitung
- **Software-Entwicklung** zur Anpassung von Schnittstellen und Entwicklung von IT-Projekten
- Schaffung innovativer eigener **Produkte**
- Nationale und internationale **Förderprojekte** auf Basis neuer Technologien, um neues Know-how aufzubauen oder Fördermöglichkeiten aufzuzeigen

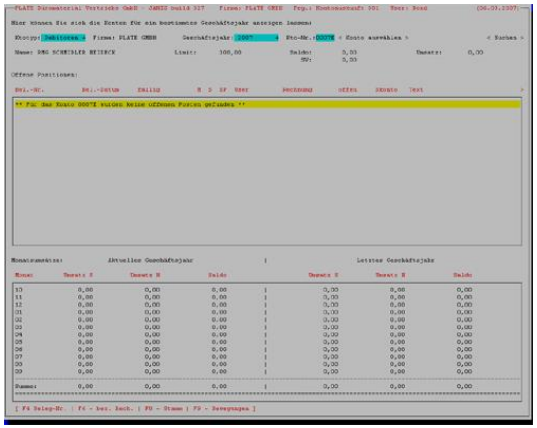
Innovative eigene Produkte

DECO_eShop

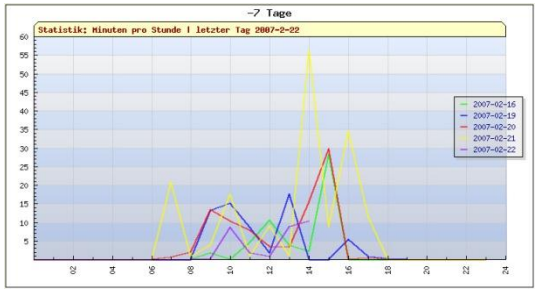
DECO_LogWatcher



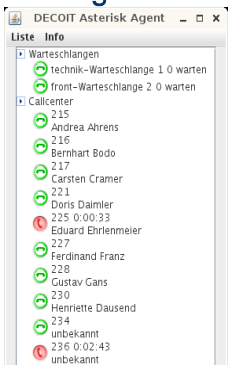
JANIS ERP-Software



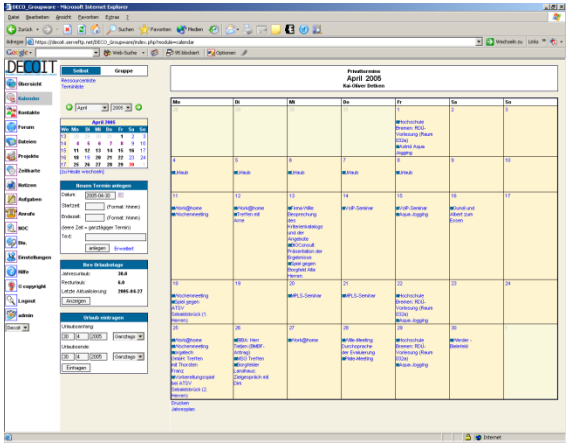
Asterisk Call Detail Records



Asterisk Agent Desktop



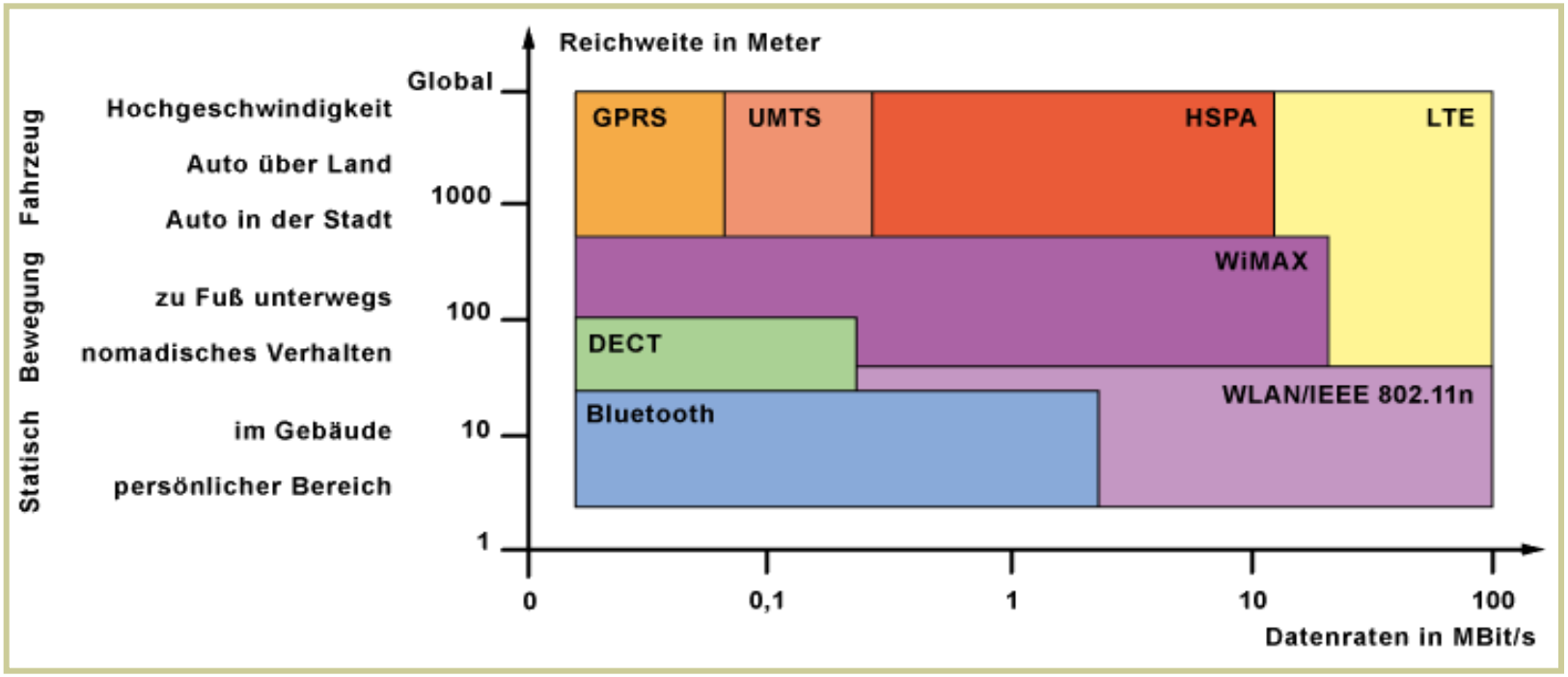
OSGA - Groupware



Übertragungstechnologien & Endgeräte

- Übertragungstechnologien
  - GSM, GPRS, UMTS, HSPA
  - LTE, WiMAX
  - WLAN 802.11b/a/g/h/n
  - Bluetooth, DECT
- Mobilfunkgeräte
  - Handys
  - Smartphones
  - Tablet PCs
  - Notebooks
  - Netbooks

Reichweiten verschiedener Mobilfunktechnologien



Arbeitsteilung der Technologien

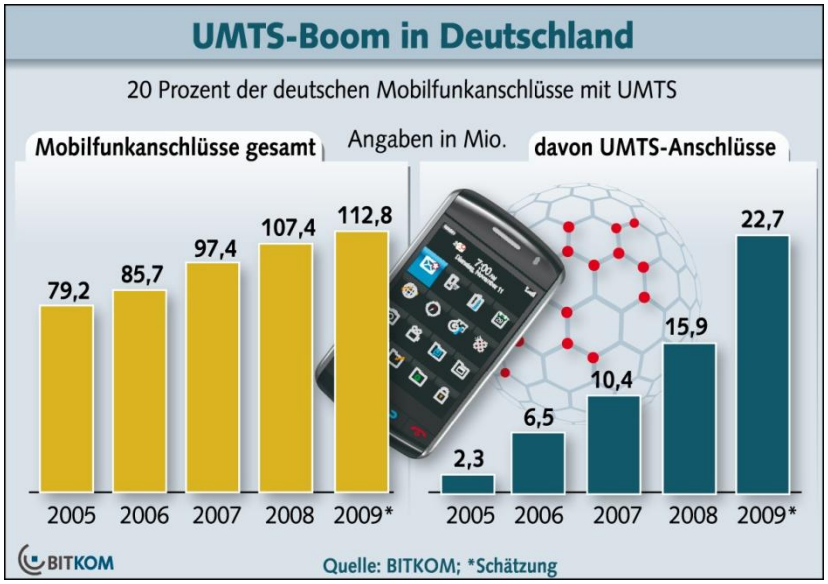
- Bluetooth
  - Private Area Network (PAN)
  - Anbindung von Peripheriegeräten
- WLAN
  - Local Area Network (LAN)
  - WLAN ist ein „quasi-stationärer Dienst“
  - WLANs könnten Orte entlasten, an denen viel Internet-Bedarf besteht (Flughäfen, Hotels)
- UMTS
  - Wide Area Network (WAN)
  - UMTS ermöglicht eine problemlose Verbindungsübergabe (Handover)
  - Flächendeckende Erreichbarkeit
  - LTE und WiMAX werden weitere Alternativen bereitstellen

Mobile Anwendungen

- Mobile Arbeitsplätze
- Schulungseinrichtungen
- Vernetzung von Home Offices
- Vernetzung von geschützten Gebäuden
- Mobile Datenerfassung
- Hot-Spots
- Externe Vernetzung
- Ad-hoc-Networking
- Mobiles VoIP
- Wearable Computing

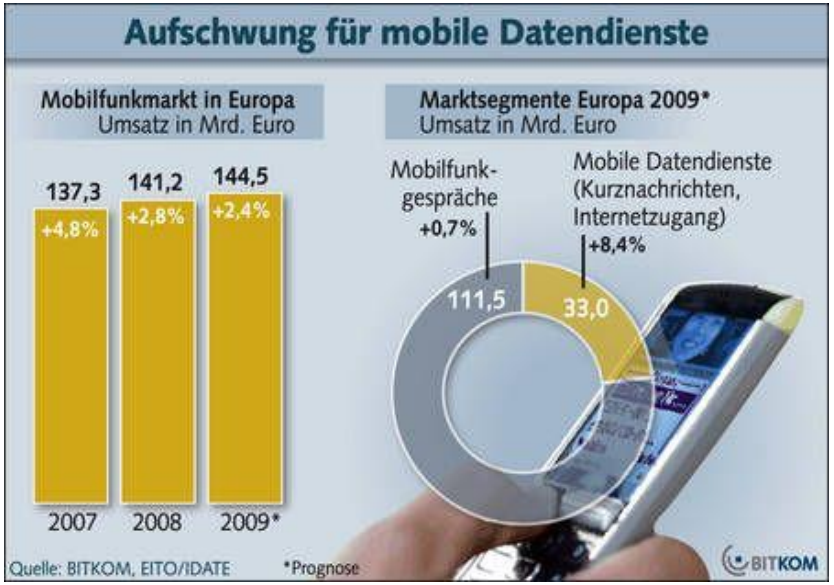
UMTS-Anschlüsse in Deutschland

- Schnelle Internetverbindungen boomen im Mobilfunk
- Einen Schub bei den UMTS-Teilnehmerzahlen bringen die neue Generation der Smartphones und Netbooks
- Datendienste sind damit der neue Treiber der Telekommunikation



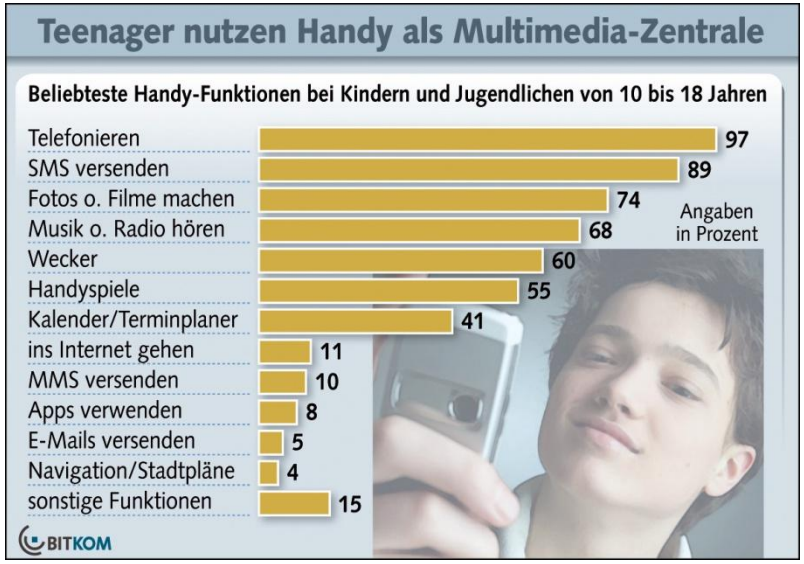
Mobile Datendienste

- Mit Handy-Telefonaten lässt sich kaum noch Geld verdienen
- Daher setzen Europas Mobilfunk-Service-Provider verstärkt auf mobile Datendienste
- Carrier lassen sich daher immer neue Dienste einfallen, die den Umsatz mit Datenservices in die Höhe treiben sollen



Handy als Multimedia-Zentrale

- 92 Prozent der 10- bis 18-Jährigen haben eigenes Mobiltelefon
- Mädchen sind besser ausgestattet als Jungs
- Jugendliche setzen das Handy wesentlich vielseitiger ein als die meisten Erwachsenen, die es nur zum Telefonieren nutzen oder SMS versenden

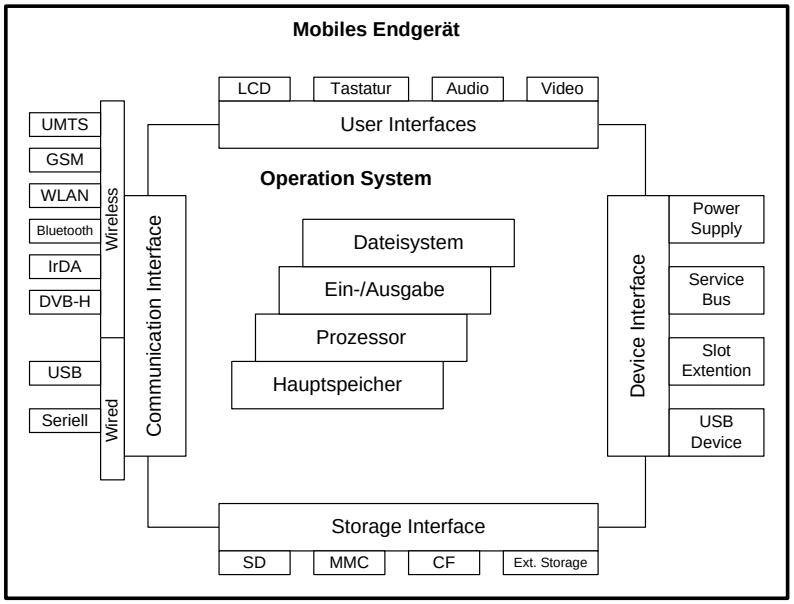


Smartphone-Vielfalt

- Google hat mit dem Android-Betriebssystem Nokia als Marktführer abgelöst
- Apple und Blackberry folgen auf den nachfolgenden Plätzen
- Der Smartphone-Markt wuchs um 88,6% weltweit (Android sogar um 600%)
- Verlierer im Smartphone-Markt im Vergleich zum Vorjahr ist Microsoft mit nur noch 3,1% Marktanteil
- Der Handy-Kampf um den Verbraucher wird von Plattformen beherrscht und nicht mehr von Gerätefunktionen dominiert

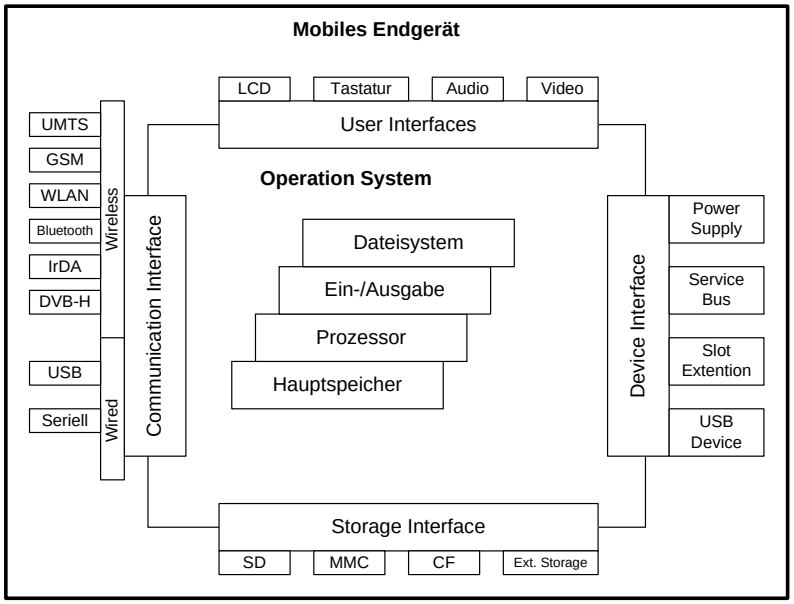
Eigenschaften mobiler Endgeräte (1)

- Mobile Endgeräte:
  - Zunehmende Integration von Funktionalitäten und Schnittstellen in mobile Endgeräte
  - Zusammenführung ursprünglich verschiedener Geräteklassen (Handy und PDA)
  - Leistungsfähigere Endgeräte
  - Mobile Endgeräte werden zudem als digitale Assistenten eingesetzt



Eigenschaften mobiler Endgeräte (2)

- Dienste:
  - Verstärkte Verbreitung von echten mobilen Diensten
  - Spezifischen Eigenschaften und Fähigkeiten der mobilen Endgeräte werden genutzt
  - Neue Benutzungsparadigmen wie „Digital Lifestyle“ oder „Ubiquitous Computing“ verändern die Anforderungen an mobile Dienste
  - Bedienbarkeit und Kommunikationsfähigkeit ist wichtig
  - Der Wunsch nach aktuellen und ständig verfügbaren Informationen führt zum mobilen Internet



Mobile Betriebssystemkonzepte (1)

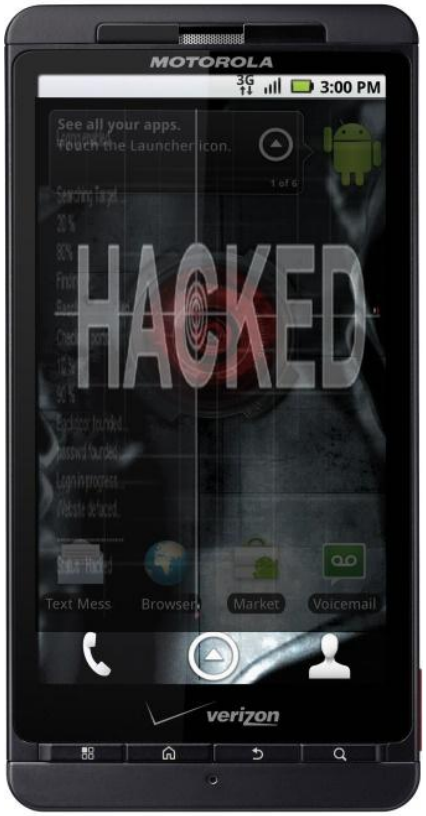
- Virtuelle Speicherverwaltung:
  - Zuordnung von Speicherbereichen zu Applikationen und Diensten
  - Stellt sicher, dass mehrere aktive Anwendungen sich nicht gegenseitig negativ beeinflussen können
  - Dies betrifft z.B. die Daten anderer Programme oder deren Speicher
- Java-Einsatz:
  - Eigenes Java-Speicherschutzkonzept
  - Java sichert die Anwendungen zueinander ab, ohne auf die virtuelle Speicherverwaltung zurückgreifen zu müssen
- Dateisysteme:
  - Persistente Speicher werden verwaltet
  - Sind nach Neustart weiterhin verfügbar (Benutzerdaten)
  - Speicher wird durch Dateisysteme organisiert
  - Kontrolle von Dateizugriffen notwendig, um nur bestimmten Benutzern den Zugriff zu gestatten

Mobile Betriebssystemkonzepte (2)

- Kryptografische Verfahren:
  - Verschiedene Verschlüsselungsverfahren sind im Einsatz je nach Gerät
  - Implementierung hängt davon ab, wie sicher diese Verfahren angewendet werden können
  - Handhabung kann Konfiguration erschweren, wodurch Sicherheitslücken entstehen
- Zugangskontrollen:
  - Authentifizieren des Benutzers für den Zugriff auf seine persönlichen Daten
  - Unterscheidung der Zugriffskontrolle bei verschiedenen Benutzern
- Erweiterbarkeit:
  - Hersteller haben Interesse an der kontrollierten Erweiterbarkeit vorhandener Gerätebasen
  - Ermöglicht eine höhere Flexibilität des Benutzers, der das Endgerät auch mit anderer Hardware nutzen möchte

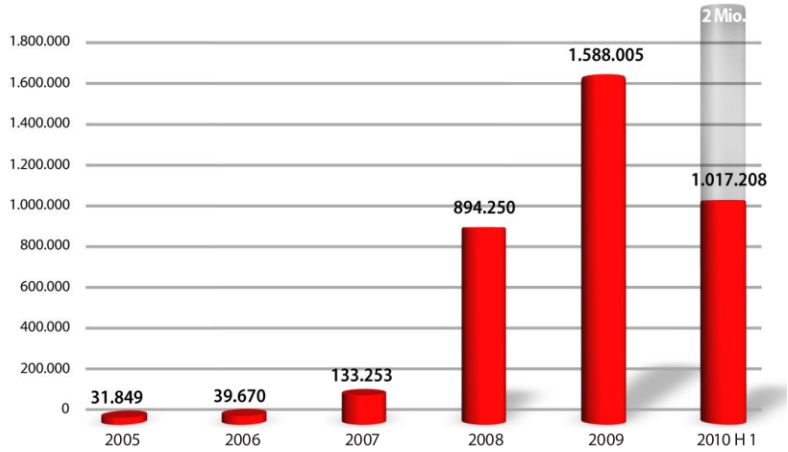
Neue Sicherheitsrisiken

- Fehlerhafte Konfiguration
  - Fehlkonfigurationen in Sicherheitskomponenten wie Firewalls, VPN-Gateways etc.
  - Betriebssystemfehler der Handys
- Offene mobile Endpunkte
  - Zugriff und Verwaltung von kritischen Geschäftsdaten
  - Keine Integritätsüberprüfung der Hardware ist möglich
  - Wachsender Malware-Markt für Smartphones
  - Verwendung von mobilen Endgeräten in unsicheren Netzen



Anstieg von Malware

- Laut den Prognosen von Sicherheitsexperten wird es in den kommenden Jahren zu einem sprunghaften Anstieg von Schadsoftware (Malware) kommen
- Dabei rücken vor allem Smartphones und andere mobile Endgeräte (z.B. Tablet-PCs) zunehmend in den Fokus der Angreifer



GData Malware Report 2010

Anforderungen bei der Implementierung im Unternehmen

- Absicherung des mobilen Unternehmensnetzes (z.B. WLAN) gegenüber externen Angreifern
- Verwaltung aller mobilen Endgeräte ist notwendig
- Sichere Authentifizierung der Hardware und Teilnehmer
- Kontinuierliche Aktualisierung der Software-Betriebszustände
- Überprüfung der IT-Sicherheit, bevor der Zugriff auf das Unternehmensnetz erfolgt
- Kompromittierung der Endgeräte muss erkannt werden können

Forschungsprojekte

- Da aktuell keine Herstellerlösung besteht, die alle Anforderungen gleichermaßen berücksichtigt, beschäftigen sich verschiedene F&E-Projekte mit dieser Thematik
  - VOGUE
  - ESUKOM
  - tNAC
  - SumoDacs
  - TNC@FHH
  - SIMOIT

VOGUE (www.vogue-project.de)

- Das VOGUE-Projekt ist ein nationales BMBF-Projekt
- Es startete im Oktober 2009 und wird im September 2011 enden
- Folgende Partner sind in diesem Projekt involviert:
  - DECOIT GmbH (Konsortialführer)
  - Fraunhofer SIT (Darmstadt)
  - Mobile Research Center (Bremen)
  - NCP engineering GmbH (Nürnberg)
  - OTARIS (Bremen)

Anforderungen mittels Trusted Computing bei VOGUE

- Eindeutige Erkennung von Zugangsversuchen und die Identifizierung der Endgeräte
- Vergleich mit den Policys und das Umsetzen von Sicherheitsrichtlinien
- Isolierung und im besten Fall die automatische Korrektur bei fest gestellten Richtlinienverletzungen
- Erstellung und Verwaltung der Richtlinien sowie die Auswertung der Ereignisse und gesammelten Daten

  → kleine Demonstration: animiertes Szenario

Fazit und Ausblick

- Mobile Endgeräte erweitern die vorhandene IT-Infrastruktur von Unternehmen
- Sie müssen deshalb in die vorhandenen IT-Sicherheitsrichtlinien bzw. das Sicherheitskonzept integriert werden
- Das BSI gibt aufgrund der wachsenden Malware-Probleme inzwischen die Empfehlung heraus Smartphones (speziell iPhone und Blackberry) nicht mehr im Unternehmen einzusetzen
- Ausnahmen sollten nur zugelassen werden, wenn die Endgeräte Simko-2-Verschlüsselungstechniken nutzen können
- Simko 2 beinhaltet: digitale Identität, sichere Authentifizierung, Verschlüsselung der Daten, sichere Datenkommunikation, abgesicherter Boot-Prozess, kontrollierter Prozess für Zusatzsoftware
- Grundsätzlich sollten mobile Endgeräte wie vollwertige Rechnersysteme behandelt und eingesetzt werden

DECOIT

Vielen Dank für ihre Aufmerksamkeit

DECOIT GmbH
Fahrenheitstraße 9
D-28359 Bremen
http://www.decoit.de
info@decoit.de