Workshop an der Hochschule Bremen

BYOD und Informationssicherheit:

Mobile Endgeräte sicher in die Unternehmensnetze einbinden

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

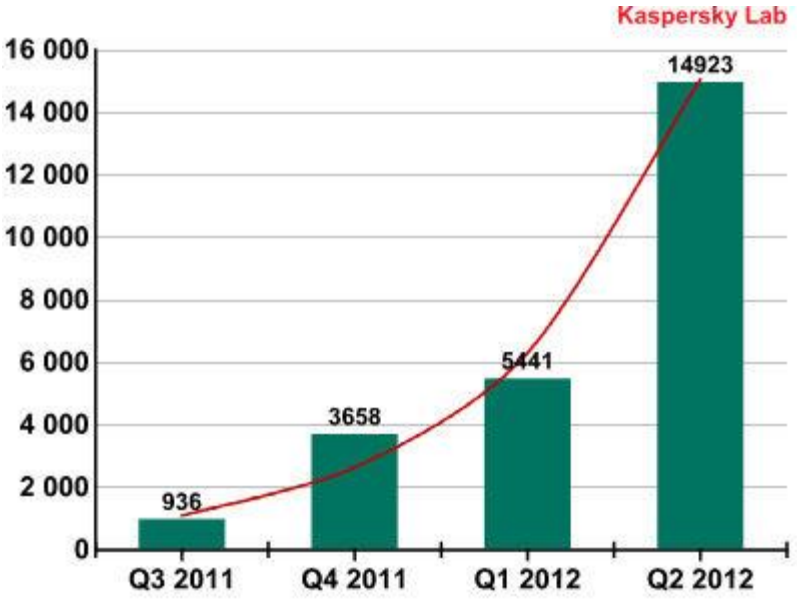
Consultancy & Internet Technologies

Kurzvorstellung der DECOIT GmbH

- Fokus: Herstellerneutrale, ganzheitliche Beratung
- Zielsetzung: akademische Lösungsansätze in kommerzielle Marktprodukte/Lösungen umsetzen
- Bereich Systemmanagement: Anbieten von Herstellerlösungen oder stabilen Open-Source-Lösungen
- Bereich Software-Entwicklung: Anbieten von selbst entwickelten Individuallösungen mit hohem Innovationscharakter oder Herstellerlösungen
- Sitz: Technologiepark an der Universität Bremen
- Heute: Full-Service-Anbieter im IT-Umfeld
- Enge Kooperationen zu Herstellern, Anbietern und Hochschulen bzw. Universitäten
- Zur Know-how-Bildung: regelmäßige Teilnahme an Forschungsprojekten

Anstieg von Malware

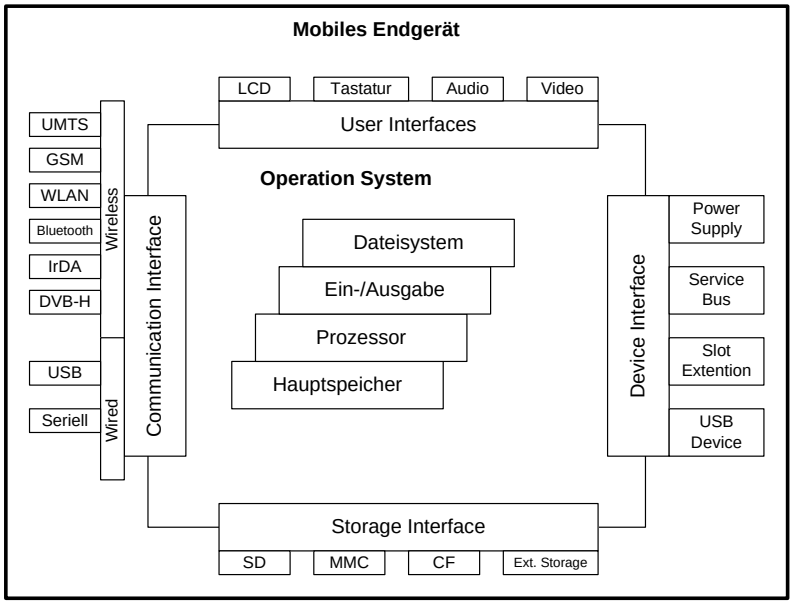
- Die Anzahl von mobilen Schädlingen gegen Android hat sich im zweiten Quartal 2012 im Vergleich zum Vorquartal verdreifacht
- Allein zwischen April und Juni 2012 wurden 14.900 neue Android-Schadprogramme entdeckt
- Zusätzlich nimmt die Qualität der Schadprogramme beständig zu
- Hauptverbreitung geschieht durch: inoffizielle App-Shops und Partnerprogramme
- Hauptziel ist es, vertrauliche Daten über Kreditkartendetails zu stehlen



Malware-Report 2012 von Kaspersky

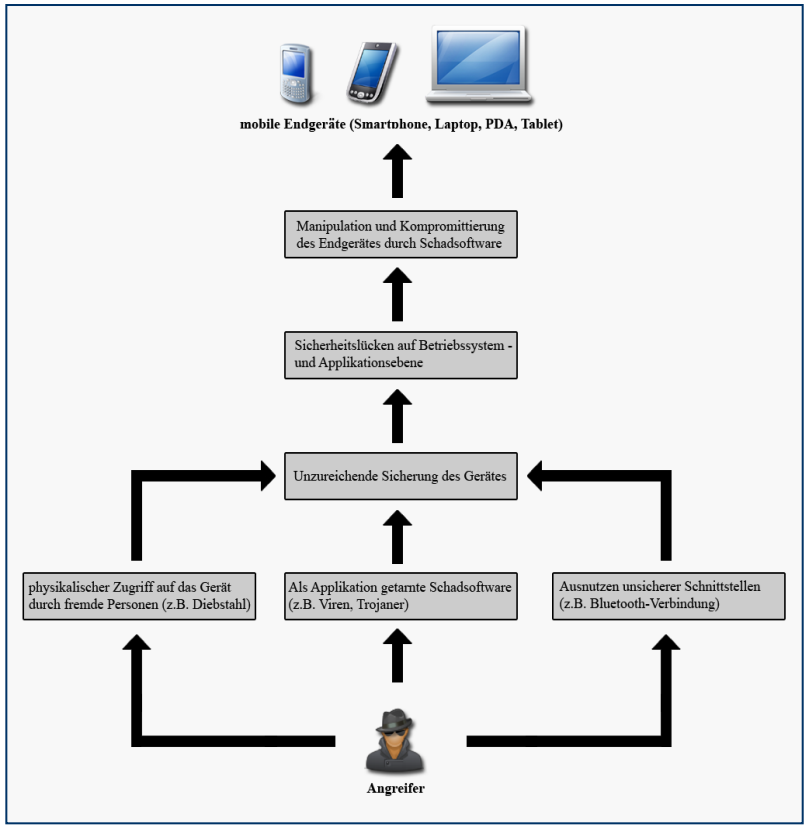
Eigenschaften mobiler Endgeräte

- Mobile Endgeräte:
  - Zunehmende Integration von Funktionalitäten und Schnittstellen in mobile Endgeräte
  - Zusammenführung ursprünglich verschiedener Geräteklassen (Handy und PDA)
  - Leistungsfähigere Endgeräte (Dual-/Quad-Core CPUs)
  - Mobile Endgeräte werden zudem als digitale Assistenten eingesetzt
- Dienste
  - Spezifischen Eigenschaften und Fähigkeiten der mobilen Endgeräte werden genutzt
  - Der Wunsch nach aktuellen und ständig verfügbaren Informationen führt zum mobilen Internet
  - Bedienbarkeit und Kommunikationsfähigkeit ist wichtig



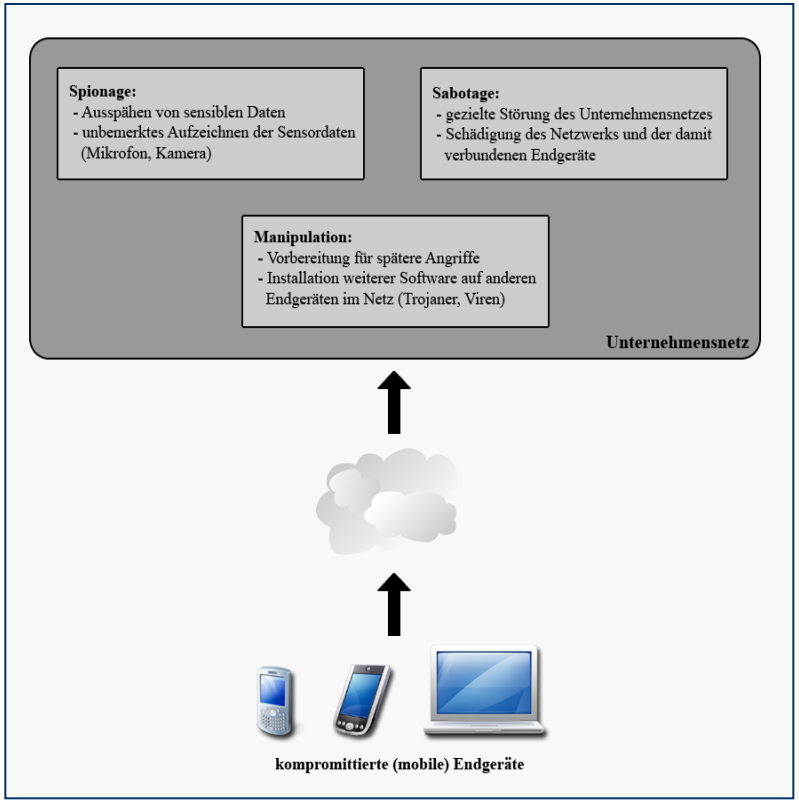
Kompromittieren mobiler Endgeräte

- Durch die Mobilität der Endgeräte erhöht sich auch gleichzeitig das Risiko des Verlustes oder des Zugriffs bzw. Diebstahls des Gerätes durch unbefugte Personen
- Unzureichende Sicherheitsvorkehrungen durch den eigentlichen Besitzer des Endgerätes (z.B. Einsatz von „schwachen" PIN-Codes) ermöglichen Daten auszuspähen oder sich mit Hilfe des Endgerätes selbst Zugang in das Netz des Unternehmens zu verschaffen
- Unbemerkten Manipulation des Gerätes (z.B. durch die Installation von Schadsoftware)
- Sicherheitslücken der Betriebssysteme ermöglichen weitere Hacking-Varianten



Gefahren kompromittierter Endgeräte

- Ausspähen von sensiblen Daten
  - Nutzerdaten (Kontakte, Kalender etc.)
  - Interne Unternehmensdaten
- Gefahren durch Sensoren und Schnittstellen heutiger mobiler Endgeräte
  - z.B. Bewegungsprofile erstellen
  - Hacking über Hardware-Interface
- Mobiles Endgerät kann als Überträger von Schadsoftware eingesetzt werden, um einen Angriff vorzubereiten
  - Trojaner
  - Viren
- Schädigung des Unternehmensnetzes oder der damit verbundenen Endgeräte



DECOIT

Mobile Sicherheitsrisiken

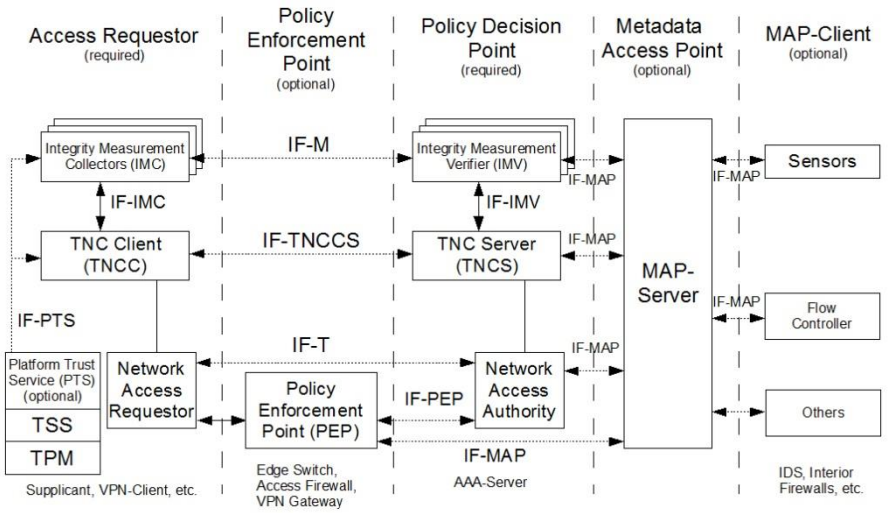
- Folgendes Sicherheitsniveau haben wir heute:
  - Keine Sicherheitsüberprüfung der Software (Patches)
  - Keine Hardware-Kontrolle verfügbar
  - Kein Support für verschiedene Security Policys
  - Sicherheitslöcher in den Betriebssystemen
  - Unzureichende Kontrolle der Apps in den AppStores der Hersteller
- Die Ausrichtung der Smartphone-Hersteller ist eindeutig der Massenmarkt!
- Es lässt sich über die Hardware-Schnittstelle eines Smartphones jedes mobile Standard-Betriebssystem hacken

Trusted Network Connect (TNC)

- TNC ist eine offene Architektur für Network Access Control (NAC), standardisiert durch die Trusted Network Connect Working Group (TNC-WG) von der Trusted Computing Group (TCG)
- Die Spezifikation stellt die „Reinheit“ von Endpunkten sicher: es kann durch Authentifizierungs- und Autorisierungsinformationen eine Zustandsprüfung („Health Check“) erfolgen, die sicherstellt, dass das Endgerät den IT-Sicherheitsregeln des Unternehmens entspricht
- Die TNC-Architektur ist somit die Entwicklung einer offenen und herstellerunabhängigen Spezifikation zur Überprüfung der Integrität von Endpunkten, die einen Verbindungsaufbau starten
- Die Architektur bezieht dabei schon bestehende Sicherheitsaspekte mit ein, wie Virtual Private Network (VPN), IEEE 802.1x (802.1x), Extensible Authentication Protocol (EAP), Transport Layer Security (TLS), Hyper-Text Transfer Protocol Security (HTTPS)

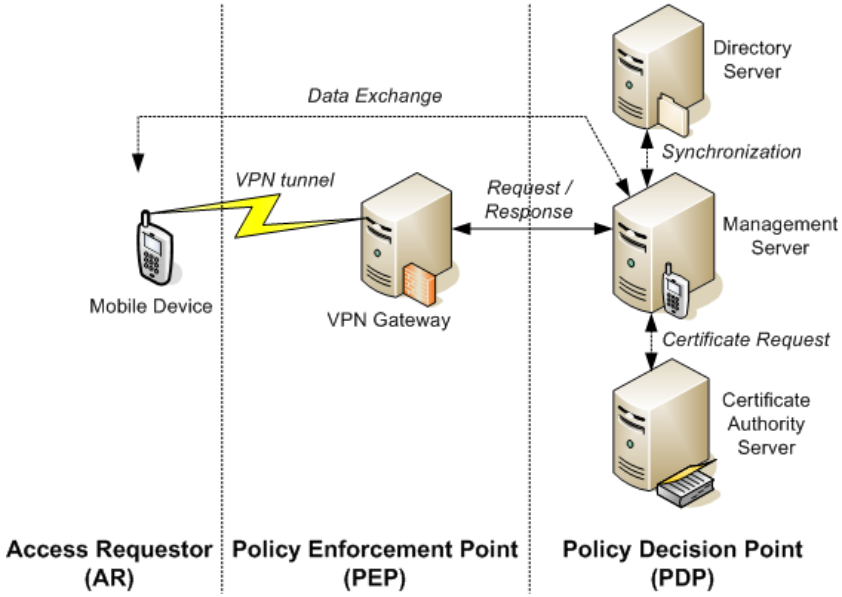
Architektur des TNC-Ansatzes

- Richtlinien-abhängige Zugriffssteuerung für Netzwerke
  - **Integritätsprüfung:** Messen des Systemzustands (Konfiguration der Endgeräte) und Überprüfung dieser Zustände gemäß Richtlinien (Assessment-Phase)
  - **Isolation** von potentiell gefährlichen Rechnersystemen bei Nichterfüllung der Richtlinien (Isolation-Phase)
  - **Wiedereingliederung** nach Wiederherstellung der Integrität (Remediation-Phase)
- Erweiterter Integritätscheck möglich (z.B. Binden von Zugangsdaten an ein bestimmtes Rechnersystem, Signierung von Messwerten)



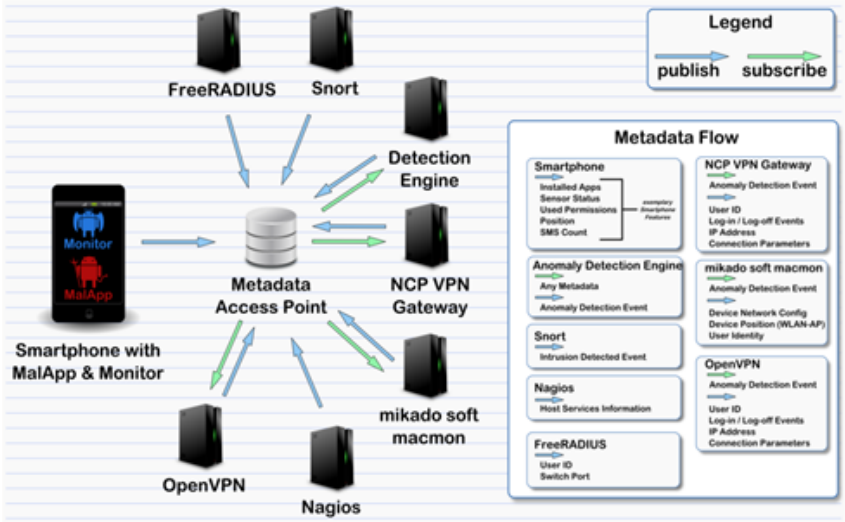
TNC-Aufgaben

- 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
- Herausforderung: wie lassen sich Anomalien am Endgerät ausmachen?



Anomalie-Erkennung

- Das Metadaten-Protokoll IF-MAP der TNC-Architektur muss zusätzlich eingeführt werden
- Ansatz:
  - Es werden möglichst viele Informationen gesammelt
  - Normalverhalten und Grenzverhalten muss erkannt werden können (Trainingsdaten)
- Die Stärke von IF-MAP gegenüber einer IDS Anomalie-Erkennung liegt in der Diversität der Daten
- Anomalie-Erkennung kann auf verschiedene Metadaten angewandt werden
- Metadaten könnten sein: Login-Count, User Account, MAC-/IP-Adresse, Zeit im System



Smartphone Awareness

- Ein IF-MAP-Client für Android wurde deshalb von der DECOIT GmbH entwickelt (Open Source)
- Erkennen von Angriffen auf Unternehmensnetze und die Einleitung entsprechender Gegenmaßnahmen über IF-MAP
- Auch andere Sicherheitskomponenten können mit IF-MAP ausgerüstet werden (IDS, Proxy, VPN-Gateway etc.)
- MAP-Server ist zur Konsolidierung der Daten notwendig
- Somit lassen sich Angriffe erkennen, die mit den Standardsystemen unentdeckt bleiben würden

Hindernisse der Softwareverteilung

- Der übliche Weg auf einem Android-Smartphone Software zu installieren, führt über den Google Market
- Bevor Zugriff auf den Google Market gewährt wird, müssen die Lizenzbedingungen akzeptiert werden
- Diese beinhalten u.a. eine Klausel, nach der Google bestimmte Apps wieder vom Endgerät entfernen kann
- Android Apps können aber auch direkt genutzt werden, was das Risiko schadhafter Software aber erhöht
- Softwareverteilung kann auf unterschiedliche Art realisiert werden:
  - Angepasste Firmware zur Behebung von Sicherheitslücken (hoher Wartungs- und Entwicklungsaufwand)
  - Automatische Updates des Herstellers (Gerät muss jedes Mal neu geroutet werden)
  - Eigener AppStore wird intern zur Verfügung gestellt und mit einer Policy versehen (kein BYOD-Szenario möglich bzw. sehr aufwändig)

Produktbeispiele

- ubi-Suite Android Mobile Management (www.ubitexx.com)
  - Zentrale Verteilung und Management von Benutzer- und Geräte-Zertifikaten
  - Gruppenbasierte Benutzerverwaltung mit LDAP-/AD-Synchronisation
  - Zentrale Softwareverteilung und Konfiguration mit Benutzerinteraktion
  - Sicherheit: Einhaltung der Passwortrichtlinien und Remote-Kill
  - Sicherung aller automatisch ausgelesenen Gerätedaten auf dem ubi-Suite Server
- MobileIron (iron-dev.com)
  - Software-Rollout mittels eigenem AppStore
  - Policy für Apps/Inventur aller Apps
  - Erkennung vorhandener oder installierter Anwendungen auf dem Gerät
- Weitere Produktbeispiele: Symantec Mobile Management, Sybase SAP-Afaria, Datomo Mobile Device Management, ISEC7 B*Nator

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 laut BSI nur zugelassen werden, wenn die Endgeräte mindestens SiMKo-2-Verschlüsselungstechniken nutzen können
- Grundsätzlich sollten mobile Endgeräte wie vollwertige Rechnersysteme behandelt und eingesetzt werden
- Eine Softwareverteilungslösung zum Monitoring und Management ist daher zumindest anzustreben

Sichere Mobile Kommunikation (SiMKo)

- SiMKo2 beinhaltet:
  - Digitale Identität (Zertifikat)
  - Sichere 2-Faktor-Authentifizierung (Karte + PIN)
  - Verschlüsselung der lokalen Daten (nur über PIN lesbar)
  - Sichere Datenkommunikation mittels VPN-Technik
  - Abgesicherter Boot-Prozess
  - Kontrollierter Prozess zur Installation von Zusatzsoftware
- Die mobile Hardware muss dabei um einen zertifizierten Hardware-Sicherheitsanker in Form einer µSD-Kryptokarte ergänzt werden
- Der SiMKo-Ansatz wird von T-Systems mit verschiedenen Smartphones angeboten
- SIMKo3 wurde auf der CeBIT 2012 prototypisch vorgestellt

Trennung der Apps durch BizzTrust

- Der BizzTrust-Ansatz von Fraunhofer SIT schützt geschäftliche Daten und Anwendungen, ohne den Nutzer einzuschränken
- Der Ansatz erkennen, ob Daten zu einer privaten oder geschäftlichen Anwendung gehören, speichern diese in getrennten Bereichen und verhindern, dass private Apps auf geschäftliche Daten zugreifen können
- Der Mitarbeiter kann dennoch privat beliebige Apps installieren
- Selbst wenn Angreifer eine unsichere App einschleusen, können diese damit nicht auf die Firmendaten zugreifen
- Weitere Eigenschaften sind:
  - VPN-Verschlüsselung
  - Remote Management und Update
  - Automatisches Policy Enforcement
  - Android-Betriebssysteme werden unterstützt

www.bizztrust.de

Integrität der Hardware

- Die Integrität der mobilen Endgeräte (Hardware) sollte allerdings ebenfalls abgefragt werden
- Dies kann mittels Trusted-Computing-Techniken wie TNC realisiert werden
- Zur grundlegenden Absicherung mobiler Systeme sind dabei folgende Anforderungen vorzusehen:
  - Root-of-Trust-Implementierung durch MTM- oder TPM-Modul ermöglichen
  - MTM-/TPM-Integration in die Smartphones
  - Integrity Measurement Architecture (IMA) als Kernel-Erweiterung einsetzen zur Messung von ausführbaren Codes, Middleware, Konfigurationsdateien und dynamischen Bibliotheken
  - Monitoring implementieren, das nicht erlaubte Interaktionen erkennt und unterbindet

Aktuell scheitert dieser Ansatz noch, da es an TPM-/MTM-Implementierungen in Smartphones mangelt und eine Kernelerweiterung notwendig ist

Vielen Dank für ihre Aufmerksamkeit

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

Consultancy & Internet Technologies