

Sicherheit und Android-Smartphones



Fachanlass W1: Mobilität und Sicherheit Fachgruppe Sicherheitstechnik FGST

Tobias Ellenberger

Inhaltsverzeichnis

- Über OneConsult GmbH & mich
- Android OS
- Sicherheitsanalyse
- Security Suites für Android
- Fazit

OneConsult GmbH

→ OneConsult GmbH

- Gründung 2003
- IT Security Consulting & strategische Beratung
- Kein Verkauf von Hard- und Software
- 11 Mitarbeitende, wovon 9 Consultants
- Für Kunden weltweit und in allen Branchen tätig

→ Standorte

- Schweiz: Hauptsitz in Thalwil
- Österreich: Virtuelles Büro in Wien

Unsere Dienstleistungen

→ Security Audits

- Security Scan
- Penetration Test
- Application Security Audit
- Ethical Hacking
- Social Engineering
- Conceptual Security Audit

→ Consulting

- Strategy & Organisation
- Policies & Guidelines
- Processes & Documentation
- Business Continuity & Disaster Recovery
- Engineering & Project Management

→ Incident Response

- Emergency Response
- Computer Forensics

→ Training & Coaching

- OSSTMM Zertifizierungskurse
- Security Awareness Training
- Coaching

Über mich

- Tobias Ellenberger
- Ausbildung als Mediamatiker mit Schwerpunkt Informatik
- Langjährige Erfahrung und stetige Weiterbildung als System Engineer und IT Consultant in den Bereichen Security, Netzwerk, Unified Messaging und Virtualisierung
- Seit Kindheit begleitendes Interesse an
 - Wie benutze ich den Computer, wenn die Eltern sagen geht nicht
 - Von BO über Sub7 zu Netbus etc...
 - ...heute...
- Team Leader Operations & Senior Security Consultant @OneConsult GmbH

Inhaltsverzeichnis

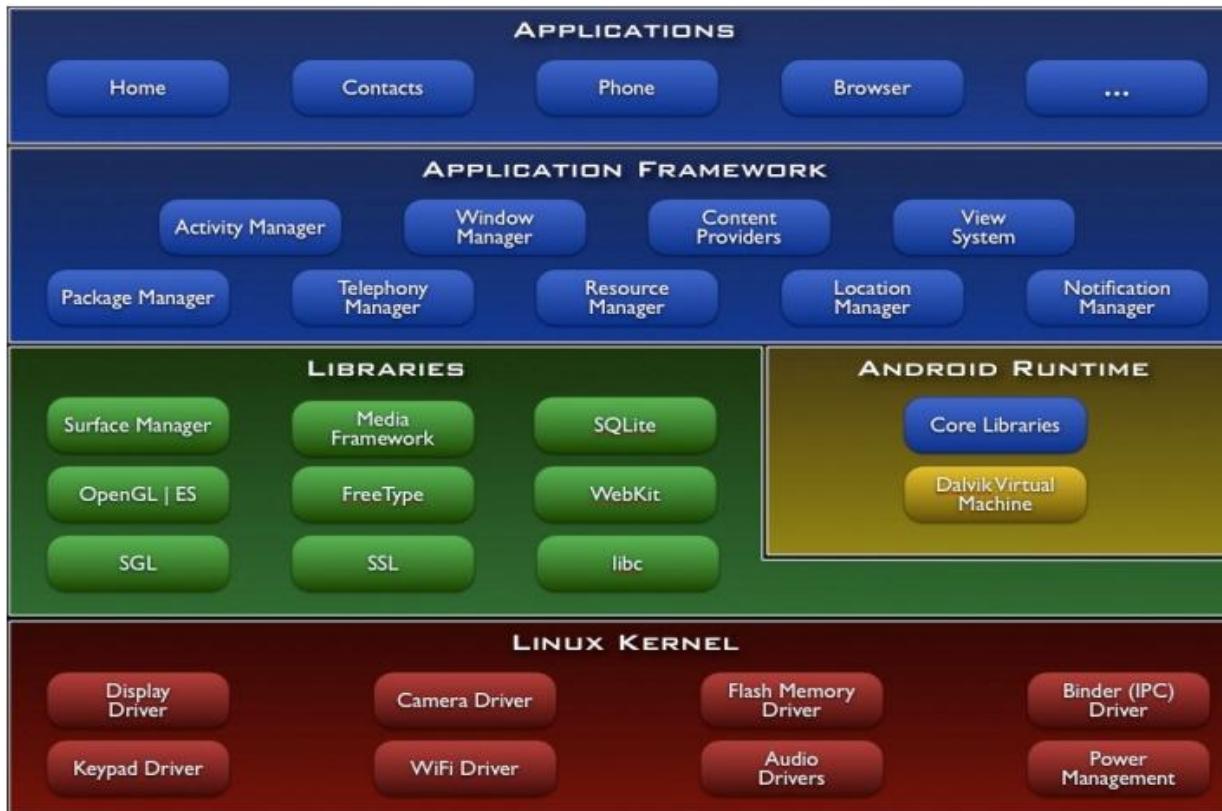
- Über OneConsult GmbH & me
- **Android OS**
- Sicherheitsanalyse
- Security Suites für Android
- Fazit

Was ist das Android OS?

- Betriebssystem für mobile Endgeräte
- Entwickelt von Google und Open Handset Alliance
- Basierend auf Linux Kernel
- Anwendungen werden mittels Java entwickelt
- Anwendungen laufen in einer virtuellen Instanz
- Bestehende Funktionen durch Applikationen erweitern
- Grundlegende Sicherheitsfunktionen
 - ...dazu später 😊

Android OS: Architektur

Architekturdarstellung von Google



Android OS: Timeline



1998



2000



2001



2006



2009

2012



Android OS: Technischer Stand

→ Was wurde aus der „PC-Vergangenheit“ gelernt?

- Sandboxing
- Least Privileges (Berechtigungskonzepte)
- Unterschiedliche Ansätze zwischen Android OS, iOS und Windows Phone
 - › Open Source vs. Closed Source
 - › Market Place, App Store etc.
 - › Updatekonzepte

Fazit:

Die Security-Grundlagen wurden und Erfahrungen sind in die Entwicklung eingeflossen, unter Berücksichtigung der Eigeninteressen

Inhaltsverzeichnis

- Über OneConsult GmbH & me
- Android OS
- **Sicherheitsanalyse**
- Security Suites für Android
- Fazit

Sicherheitsanalyse: Sicherheitsfunktionen...

- Kernel
- Sandboxing
- Rechteverwaltung
- Dalvik VM & Bibliotheken
- Bildschirmsperre
- Android Market (Gtalk Service)
- Faktor Mensch

Sicherheitsanalyse: Kernel

- Linux Kernel ja / nein?
- Gut gepflegte Software (Analyse von Coverty)
- Daraus folgt:
 - Linux ist eine gute Basis für das Entwickeln eines sicheren Produktes
- Jon Oberheide: «Schweizer Käse»
 - Linux bietet eine hervorragende Angriffsfläche
 - Praxis: z.B Rooting

Sicherheitsanalyse: Sandboxing

- Prinzip: Applikation hat kein Zugriff auf eine andere Anwendung oder auf das System
- Bekannt von Linux und Windows (UAC)
- Aber:
 - Dateisystem
 - › Ab Android 2.3 Ext4 (vorher YAFFS)
 - › Auf SD-Karten FAT
 - Shared User ID's
- Kleines Beispiel...

Sicherheitsanalyse: Rechteverwaltung

- Erlaubt Kommunikation zwischen Anwendungen
- Aufweichen des Sicherheitsmechanismus
- Vier Schutzstufen
 - «normal»
 - «dangerous»
 - «signature»
 - «signatureOrSystem»
- Schwächen der Rechteverwaltung
 - Es gibt nur JA oder NEIN
 - Sehr global gefasste Berechtigungen
 - › android.permission.INTERNET
 - › android.permission.WRITE_EXTERNAL_STORAGE

Sicherheitsanalyse: Dalvik VM & Bibliotheken

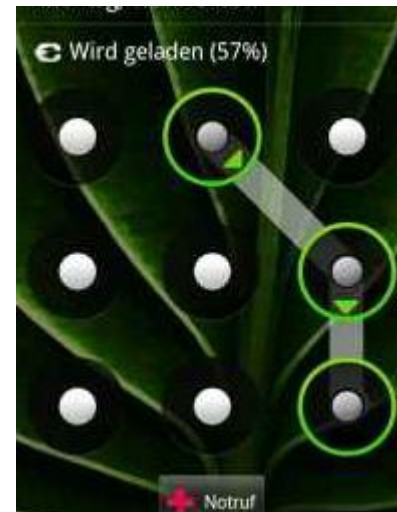
→ Dalvik Virtual Machine

→ Bibliotheken

- Libc «Bionic»
- FreeType
- SQLite
- WebKit

Sicherheitsanalyse: Bildschirmsperre

- Passwort sinnvoll für den Schutz des Smartphones
- Folgende Möglichkeiten:



Sicherheitsanalyse: Android Market

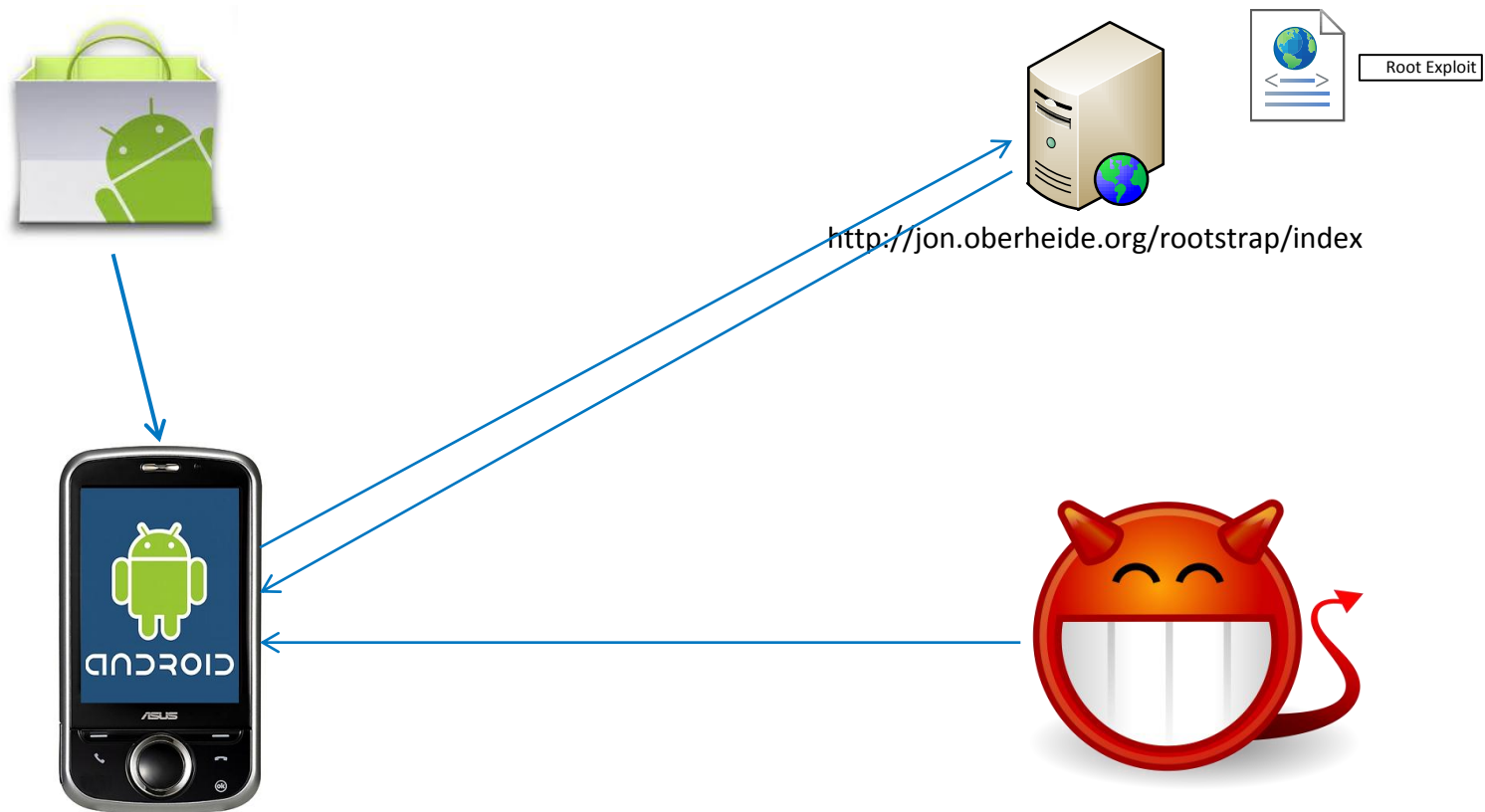
- Applikationen erweitern die Funktionen des Smartphones
- Keine Überprüfung durch Google
- «Benutzer basierte» - Kontrolle des Inhalts
- Jeder kann für 25\$ Applikationen veröffentlichen (auch anonym)
- Apps müssen signiert werden. Selbst signiertes Zertifikat für den Benutzer Account.
- Seit Februar 2011: Installation von Apps via Browser möglich

...und wie sie ausgenutzt werden

→ Kernel

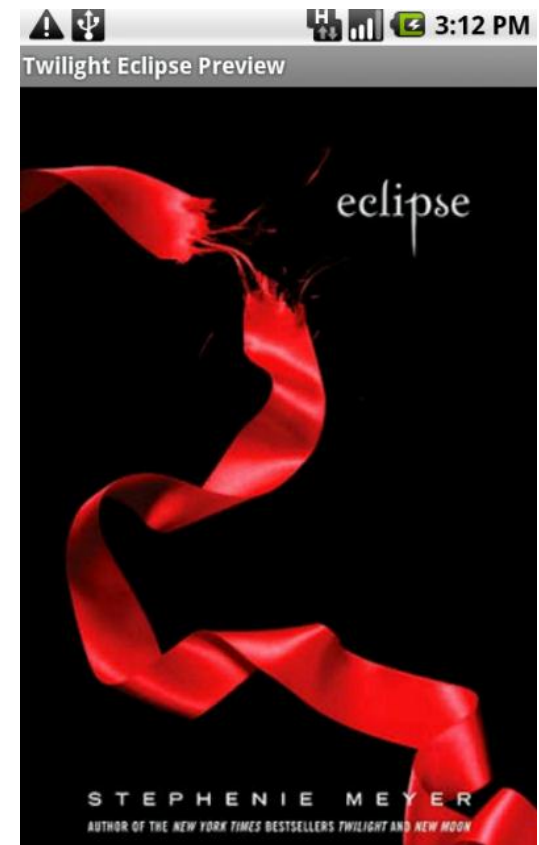
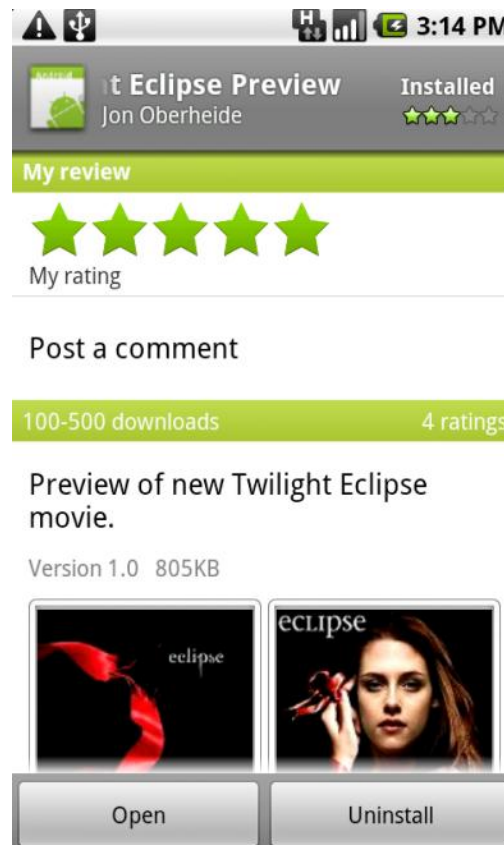
- Rooting (z.B. rage against the cage)
 - › **Aktuelles Beispiel: 23.01.2012**
(<http://www.heise.de/security/meldung/Linux-Root-Rechte-durch-Speicherzugriff-1419608.html>)
- Anwendungsbeispiel:
Android Hax von Jon Oberheide (Twilight:Eclipse App)

Android Hax (Funktion)



Android Hax (Verbreitung)

- Über 200 Downloads in weniger als 24h
- Reaktion: Remote Wipe



...und wie sie ausgenutzt werden

→ Kernel

- Rooting (z.B. rage against the cage)
 - › **Aktuelles Beispiel: 23.01.2012**
- Anwendungsbeispiel:
Android Hax von Jon Oberheide (Twilight:Eclipse App)

→ Sandboxing

- Cross Application Scripting

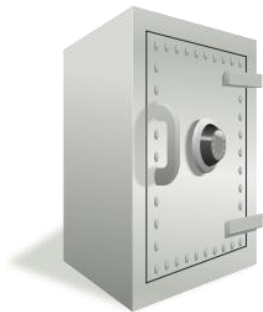
→ Rechteverwaltung

- Eigene Berechtigungen...

Rechteverwaltung (Beispiel)

(1) Password-Safe

- Kein Internet
- *pw.exchange*



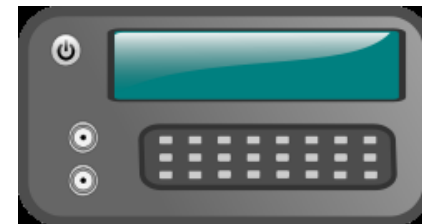
(2) Android Market

- Top Rating



(3) PasswortGen

- Internet Zugriff
- *pw.exchange*



...und wie sie ausgenutzt werden

→ Kernel

- Rooting (z.B. rage against the cage)
 - › **Aktuelles Beispiel: 23.01.2012**
- Anwendungsbeispiel:
Android Hax von Jon Oberheide (Twilight:Eclipse App)

→ Sandboxing

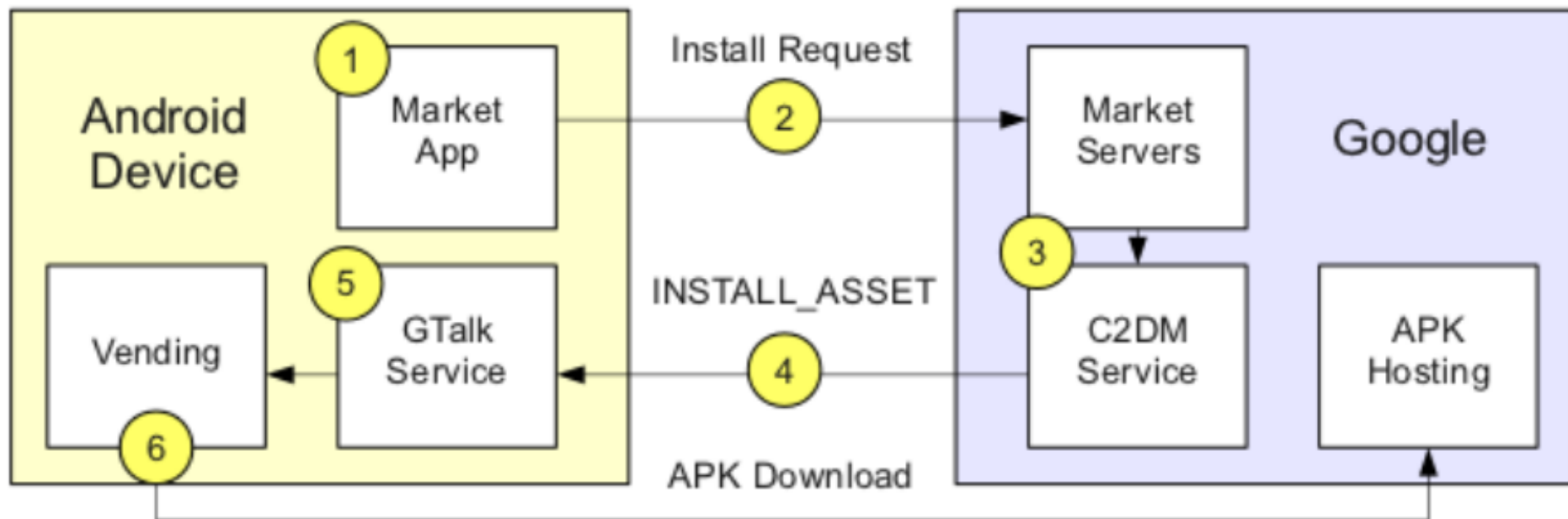
- Cross Application Scripting

→ Rechteverwaltung

- Eigene Berechtigungen...
- «exported attribute»

→ Android Market (Gtalk Service)

Android Market





Android Market (Gtalk Service)

- Apps werden nicht über die Android Market App installiert
- Die App wird mittels C2DM-Server gepusht
- Google hat mindestens folgende Funktionen zur Verfügung:
 - INSTALL_ASSET (App installieren)
 - REMOVE_ASSET (App entfernen)
 - › Twilight Eclipse App
 - › DroidDream-Trojaner
- Was wenn jemand die Google Server «übernimmt» ?!?

Sicherheitsanalyse: Faktor Mensch

- «JA Klick» - Syndrom
- «Ich will» - Syndrom
- «KLDAZL» - Syndrom
- «DGMNA» - Syndrom

Inhaltsverzeichnis

- Über OneConsult GmbH & me
- Android OS
- Sicherheitsanalyse
- Security Suites für Android
- Fazit

Security Suites

→ Hersteller

- Neue Hersteller z.B Lookout spezialisiert auf Mobile Security
- Die meisten namhaften Hersteller von AV-Software für PC's

→ Nutzen

- Schutz vor Malware, Phishing, Datenverlust und Diebstahl
- Erweiterte / zusätzliche Funktionen für das Smartphone

→ Funktionen

- Malware Scanner
- Backup & Locator Dienste
- Datenschutz
- Div. Sperr und Filterfunktionen

Security Suites

→ Gegen was helfen Security Suites wirklich?

- Ergänzung der Schutzfunktionen vom Smartphone
- Erkennen von bestehenden / bekannten Gefahren

→ Was Security Suites nicht können

- Neue Angriffe erkennen
- «intelligente» Angriffe verhindern
- Menschliches Verhalten ändern
- Entwickler sensibilisieren (Vergabe von Rechten)

→ Fazit:

- Sinnvolle Ergänzung zum Betriebssystem
- Falsches Sicherheitsgefühl

Inhaltsverzeichnis

- Über OneConsult GmbH & me
- Android OS
- Sicherheitsanalyse
- Security Suites für Android
- Fazit

Das sichere Smartphone

Wie Sie sehen, sehen Sie nichts...
Das sichere Smartphone existiert nicht.

Fazit

- Modernes Betriebssystem
- Berücksichtigung von Sicherheitsaspekten
- Es gilt zu beachten
 - Android OS = „Windows der Smartphones“
 - Attraktiv für Angriffe (Verbreitung, Daten)
 - Langsame Updates / Automatische Updates
 - Kein Vertrauen in den Android Market
- XMV
- Fragen?

Vielen Dank für Ihre Aufmerksamkeit!



Tobias Ellenberger

Mediamatiker EFZ, MCITP, OPST & OPSA
Team Leader Operations &
Senior Security Consultant

tobias.ellenberger@oneconsult.com

+41 79 314 25 25

Hauptsitz

OneConsult GmbH
Schützenstrasse 1
8800 Thalwil
Schweiz

Tel +41 43 377 22 22

Fax +41 43 377 22 77

info@oneconsult.com

Büro Österreich

Niederlassung der OneConsult GmbH
Twin Tower, Wienerbergstrasse 11/12A
1100 Wien
Österreich

Tel +43 1 99460 64 69

Fax +43 1 99460 50 00

info@oneconsult.at

