Hacking Day 2012 – Future Security

Android Smartphones und Sicherheit

Tobias Ellenberger - COO & Co-Partner - OneConsult GmbH

Agenda

- → Vorstellung
- → Android OS
- → Sicherheitsanalyse
- → Security Suites für Android
- → Fazit

Über mich

- Tobias Ellenberger
- Ausbildung als Mediamatiker
- Stetige Weiterbildung in den Bereichen Security, Netzwerk, Microsoft
- Seit 2002 in den Bereichen Consulting und Engineering tätig
- COO & Co-Partner der OneConsult GmbH

OneConsult GmbH

- → IT Security Consulting & strategische Beratung
- → Kein Verkauf von Hard- und Software
- → Kunden
  - Hunderte Unternehmen und Konzerne in Europa und Übersee
  - tätig in allen Branchen
- → Kompetenz
  - mehr als 500 technische Security Audits (davon 450 OSSTMM konform)
  - Dutzende konzeptionelle Projekte
- → Standorte
  - Schweiz: Hauptsitz in Thalwil
  - Deutschland: Büro in München
  - Österreich: 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
- Practical Security Scanning
- Secure Software Development
- Coaching

→ Security as a Service

Agenda

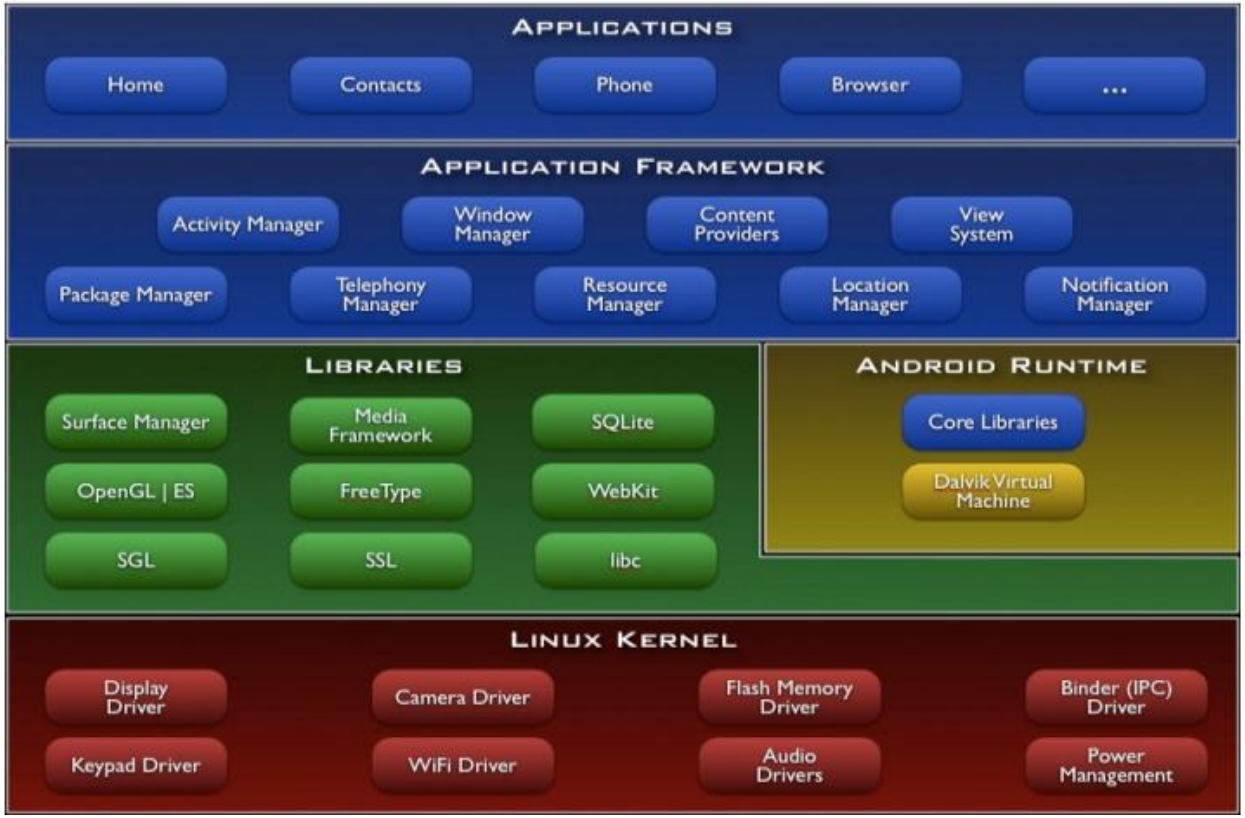
- → Vorstellung
- → Android OS
- → Sicherheitsanalyse
- → Security Suites für Android
- → Fazit

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: Technischer Stand

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

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

Fazit:
Die Security-Grundlagen und Erfahrungen sind in die Entwicklung mit eingeflossen…

… unter Berücksichtigung der eigenen Interessen

Agenda

- → Vorstellung
- → Android OS
- → Sicherheitsanalyse
- → Security Suites für Android
- → Fazit

Sicherheitsanalyse: Sicherheitsfunktionen...

- → Kernel
- → Sandboxing
- → Rechteverwaltung
- → Bildschirmsperre
- → Google Play – ex 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 keinen 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…
  - Fun-Foto App (Zugriff Bilder)
  - Game (Zugriff Internet für High-Score)

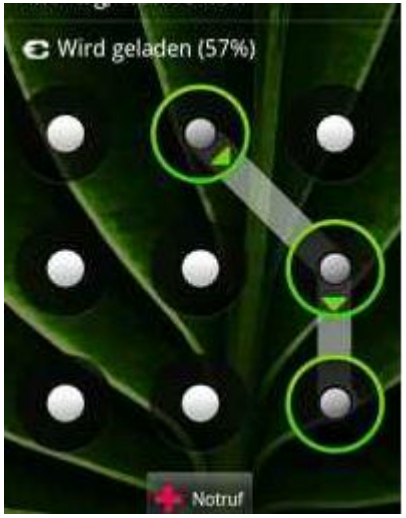
Sicherheitsanalyse: Rechteverwaltung

- → 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: Bildschirmsperre

→ Passwort sinnvoll für den Schutz des Smartphones

→ Folgende Möglichkeiten:



Sicherheitsanalyse: Google Play

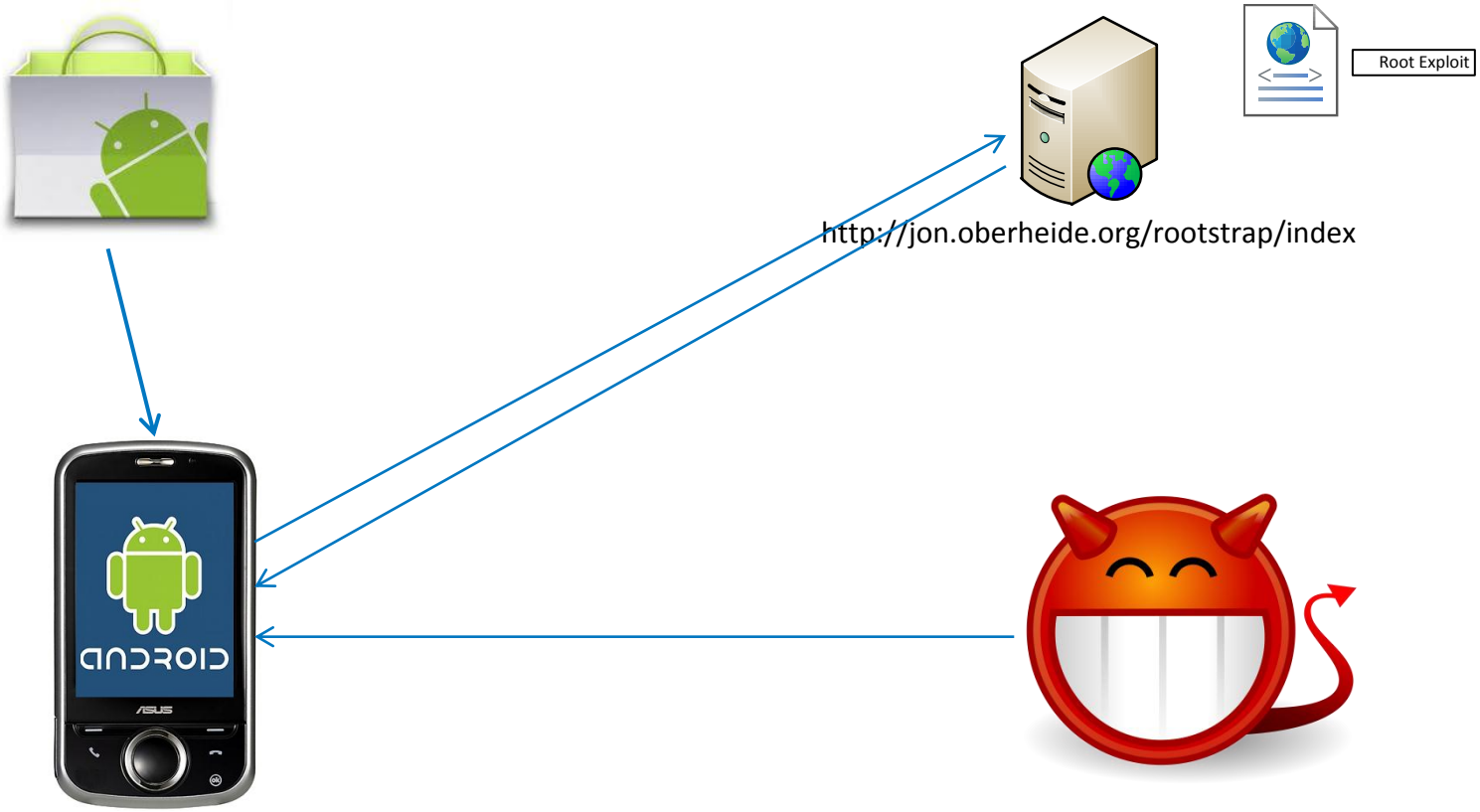
- → Applikationen erweitern die Funktionen des Smartphones
- → Benutzerbasierte Kontrolle des Inhalts
- → Bouncer (Malwarekontrolle – seit 2011)
  - Summercon Juni 2012
- → Jeder kann für $25 Applikationen veröffentlichen (auch anonym)
- → Apps müssen signiert werden; selbst signiertes Zertifikat für den Benutzer-Account
- → Seit Februar 2011: Installation von Apps via Browser möglich

…und wie sie ausgenutzt werden

→ Kernel

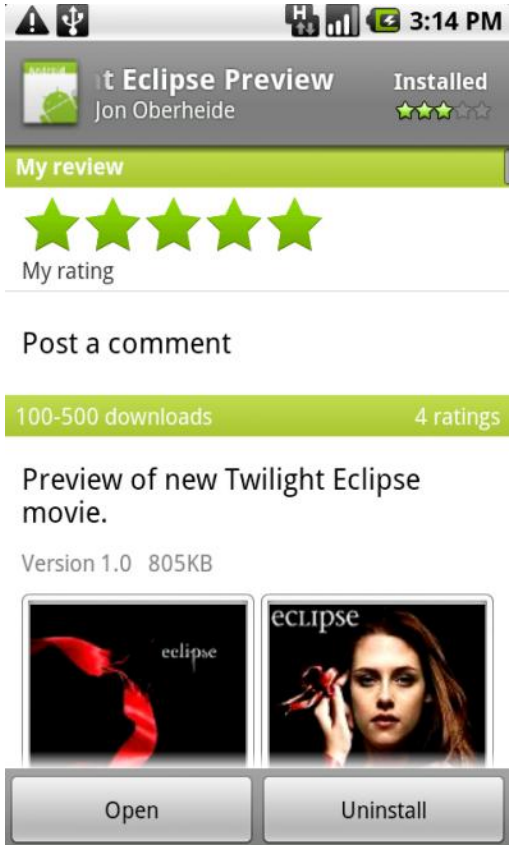
- Rooting (z.B. rage against the cage)
  - Beispiel: 23.01.2012 *(http://www.heise.de/security/meldung/Linux-Root-Rechte-durch-Speicherzugriff-1419608.html)*
- Anwendungsbeispiel:
  Android Hax von Jon Oberheide (Twilight:Eclipse App)

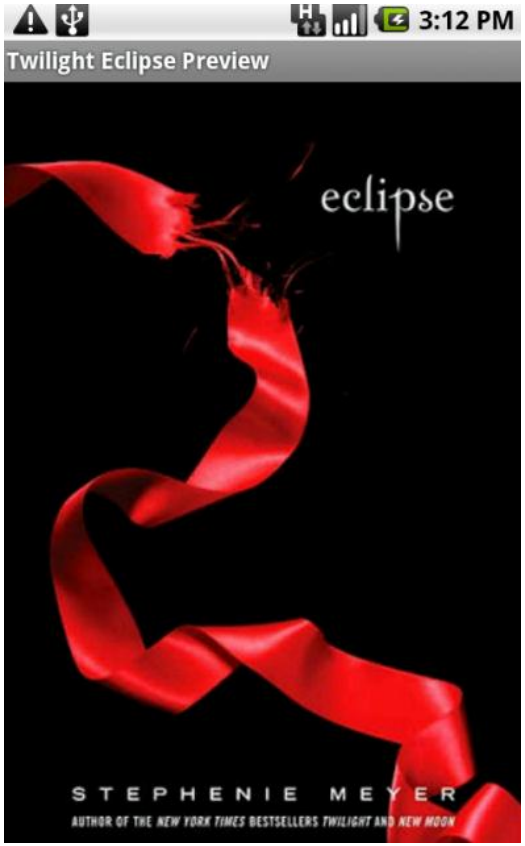
Android Hax (Funktion)



Android Hax (Verbreitung)

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





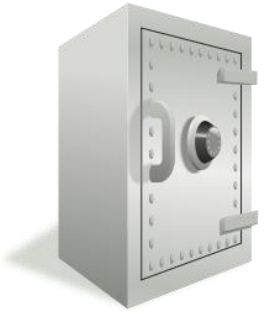
…und wie sie ausgenutzt werden

- → 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
  - Shared User-ID
- → Rechteverwaltung
  - Eigene Berechtigungen…

Rechteverwaltung (Beispiel)

(1) Password-Safe

- Kein Internet
- *pw.exchange*

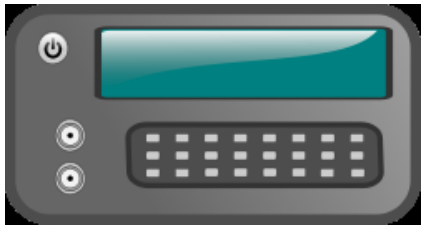


(2) Google Play

- Top Rating
- X Downloads

(3)Password-Gen

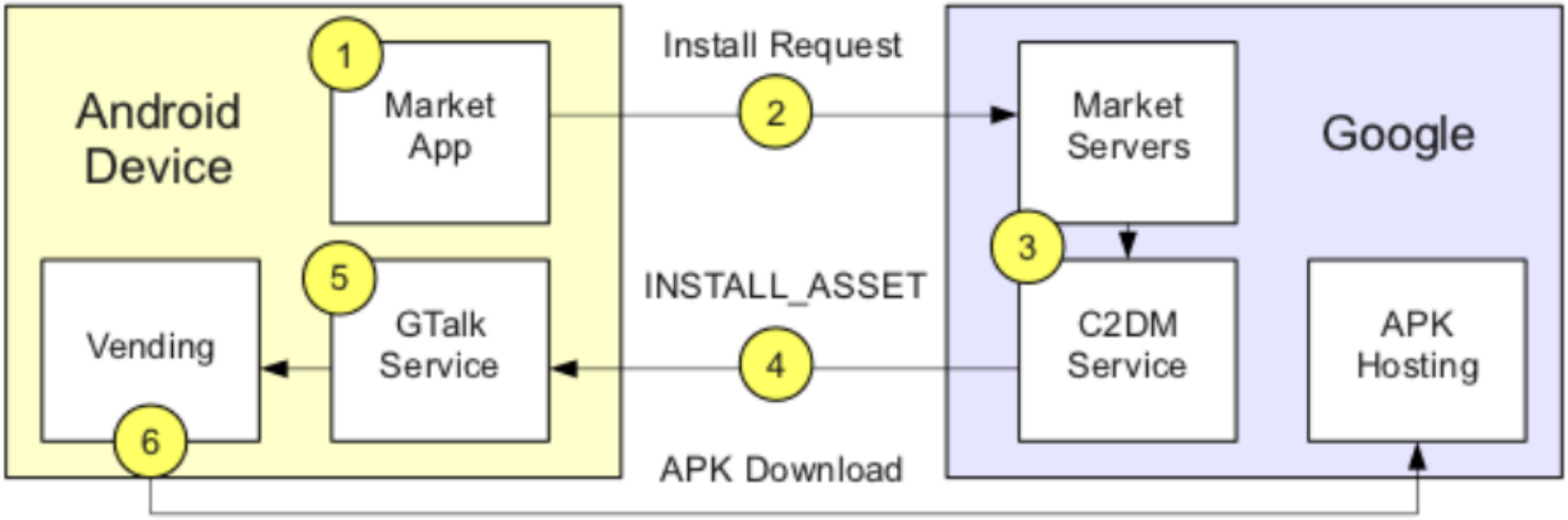
- Internet Zugriff
- *pw.exchange*



…und wie sie ausgenutzt werden

- → Kernel
  - Rooting (z.B. rage against the cage)
    - › Beispiel: 23.01.2012
  - Anwendungsbeispiel:
    Android Hax von Jon Oberheide (Twilight:Eclipse App)
- → Sandboxing
  - Cross Application Scripting
- → Rechteverwaltung
  - Eigene Berechtigungen…
  - «exported attribute»
- → Google Play (Gtalk Service)

Google Play



Google Play (Gtalk Service)

- → Apps werden nicht über die Google Play 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

Agenda

- → 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
- Die bekannten AV-Hersteller sind bei den Tests vorne dabei

Agenda

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

Fazit

- → Modernes Betriebssystem
- → Berücksichtigung von Sicherheitsaspekten
- → Es gilt zu beachten
  - Attraktiv für Angriffe (Verbreitung, Daten)
  - Langsame Updates / Automatische Updates
  - Kein Vertrauen in Google Play
- → Eignet sich Android für den geschäftlichen Einsatz?
  - Auch andere Smartphones haben Probleme ☺
  - Mobile Device Management (MDM)
  - Einschränken der Gerätetypen (Update Aufwand)
- → XMV

Danke für Ihre Aufmerksamkeit! Fragen?

Tobias Ellenberger
Mediamatiker EFZ, MCITP, OPST & OPSA
COO & Co-Partner

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 Deutschland
Niederlassung der OneConsult GmbH
Karlstraße 35
80333 München
Deutschland

Tel +49 89 452 35 25 25
Fax +49 89 452 35 21 10
info@oneconsult.de

Büro Österreich
Niederlassung der OneConsult GmbH
Wienerbergstraße 11/12A
1100 Wien
Österreich

Tel +43 1 99460 64 69
Fax +43 1 99460 50 00
info@oneconsult.at