Sicherheit und Datenschutz in **mobilen Endgeräten**

Dr. Malte Engeler
Unabhängiges Landeszentrum für Datenschutz
Schleswig-Holstein

Sommerakademie

Kiel, 25. August 2014

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Bedeutung und Problematik

- **Mobile Endgeräte sind lohnende Datenquellen**
  - Bewegungsdaten
  - Gesundheitsdaten und Biometrie
  - Verhalten und Vorlieben

- **Mobile Endgeräte sind offene Datenquellen**
  - Bequemer Jedermann-Nutzer
  - Kleiner Bildschirm – kleiner Schutz
  - Verschiebung hin zu mobiler Nutzung (Post-PC-Ära)

Bedeutung und Problematik

- **Beispiele:**
  - **NSA Backdoors**
    - **Bei Rovio** (Angry Birds)
    - **Arbeitsgruppen für jedes OS**
    - **Internet ohnehin offen**
  - **Geräte-ID und Profile/Werbung**
  - **Social Media und Social Device verschmelzen**
  - **Endgeräte als Identifikations- und Zugangsgeräte**
  - **Abhängigkeit** (z.B. Ransomware bei iCloud)

Bedeutung und Problematik

- **Personenbezogene Daten in mobilen Geräten**
  - IMEI (Gerätenummer)
  - UDID (Gerätenummer eines iOS-Gerätes)
  - IMSI (SIM-Kartennummer)
  - MAC-Adresse (Hardware-Adresse eines Netzwerkadapters)
  - MSISDN (=Mobilfunknummer)
  - Name des Telefons
  - Standortdaten (Verknüpfung mit anderen Daten)
  - Audiodaten (Stimmabgleich, Gyroscope)
  - Biometrie (Fingerabdruck, Iris, Gesichtsgeometrie)
  - Informationen über die App-Nutzung (Werbe- und Interessenprofile)
  - Kontakte, Kalender, SMS-Historien, Browserverläufe

Strukturierung und Systematisierung

- **Ebenen**
  - **Betriebssystem**
    - Android
    - iOS
    - WP8
  - **Software**
    - Apps
  - **Hardware**
    - Sensoren
    - Speicher
    - Betriebszustand

Strukturierung und Systematisierung

- **Was ist übergeordnete Voraussetzung?**
  - Schutz von Servern
  - Allgemeine IT-Sicherheit
  - Sicherheit der Hardware

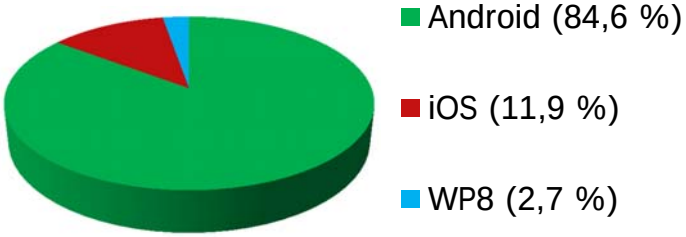
Datenschutz in mobilen Betriebssystemen

Das Betriebssystem als Weichensteller

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Die Betriebssystem-Ebene

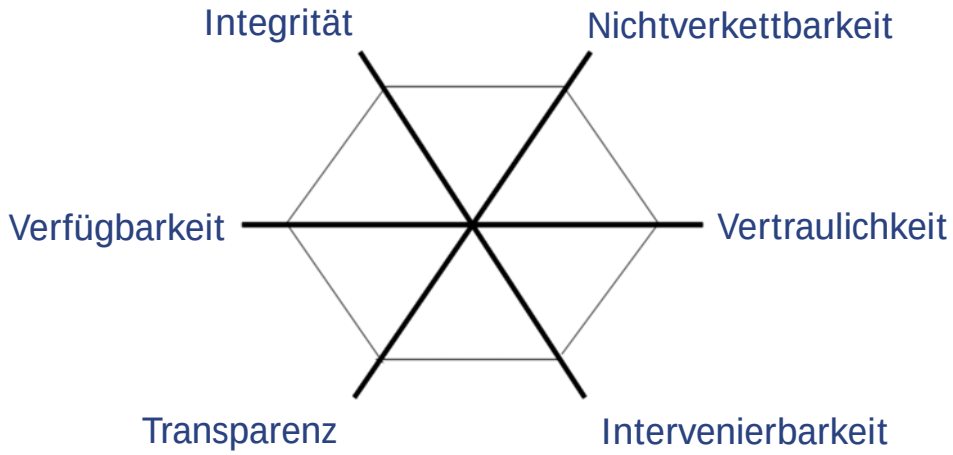
- **Definition:** Mobile Endgeräte sind Geräte mit **mobilen Betriebssystemen.**
- **Derzeit primär:**
  - Android (Google, USA)
  - iOS (Apple, USA)
  - Windows Phone 8 (Microsoft, USA)



- **Hintergrund:**
  - Apple und Microsoft waren zuerst Hard-/Softwarehersteller
  - Google verkaufte zuerst Werbung

Die Betriebssystem-Ebene

- **Strukturierung anhand der Datenschutz-Schutzziele**



Die Betriebssystem-Ebene

- **Schutzziel:** Verfügbarkeit
  (Gesicherter Zugriff auf Daten innerhalb festgelegter Zeit)

- **Android**
  - Linux/Java-Grundgerüst
  - Gingerbread instabil mit 1,7 % Crash Rate
  - Ab 4.0 nur 0,7 % CR
  - Problem: Fragmentierung
  - Gingerbread noch immer 14 % nach JB/KK mit 75 %
  - Android L?
- **iOS**
  - Objective C/Swift
  - iOS 7 mit 2,1 % CR
  - iOS 7.1 am stabilsten mit 1,6 % CR
  - iOS 7 bei fast 90 %
  - Offline-Backup über iTunes
  - iOS 8?
- **WP8**
  - C/C++
  - Wenige Untersuchungen zur Stabilität
  - WP8.1 Rollout läuft
  - Seit 8.1 jedenfalls auch Backup über WLAN

Die Betriebssystem-Ebene

- **Schutzziel:** Vertraulichkeit
  (Gesicherter Nichtzugriff auf Informationen)

- **Android**
  - Ab 3.0 (Honeycomb) Verschlüsselung
  - Fakultativ
  - Performance
  - Entsperr-PIN = Master Key
  - Akku oft entnehmbar

- **iOS**
  - Seit iOS 4: Verschlüsselung (Ziel: schnelles Löschen)
  - Seit iOS 7: „Data Protection“ sichert einzelne sensible Daten in Abstufungen (PIN)
  - Problem: Lockscreen-Benachrichtigungen

- **WP8**
  - Verschlüsselung nur über Active-Sync-Gruppen-Richtlinien
  - PIN schützt nur vor Benutzung
  - Kein CalDAV, VPN erst mit WP8.1
  - DNT ist default

Die Betriebssystem-Ebene

- **Schutzziel:** Integrität
  (Information ist gesichert echt)

- **Android**
  - 47 % - 92 % Malware
  - Fragmentierung schadet (z.B. Curesec Phonebug, fixed in 4.4.4.)
  - Dritt-Appstores
  - SMS-Trojaner möglich
  - Android L und Play Services

- **iOS**
  - Basisfunktionen nicht änderbar
  - Umstrittene Kontrolle auf Malware und Copyware
  - Cydia kaum verbreitet
  - Fast keine Malware, 0 Samples 2011

- **WP8**
  - Ähnlich enges Konzept wie iOS
  - Erst jüngst Kontrolle auf Copyware
  - Wenige Daten im Übrigen

Die Betriebssystem-Ebene

- **Schutzziel:** Integrität
  (Information ist gesichert echt)

- **Android**
  - 25 $ Gebühr
  - Nur Distribution Agreement
  - Nach Ablehnung erneut einreichbar
  - Entwickler signiert Code (ohne CA)
  - Philosophie: Malware-Abwehr durch Bewertungen im Play Store

- **iOS**
  - 99 $
  - Identitätskontrolle z.B. durch HRA
  - Code wird von Apple und Entwickler (mit CA) signiert
  - Unter iOS 4.3/5 umgehbar
  - Ablehnung wegen Datenschutz häufig (90 %), z.B. UDID

- **WP8**
  - 19 $ bis 99 $
  - Identifikation mit Kreditkarte

Die Betriebssystem-Ebene

- **Schutzziel:** Transparenz
  (Erkennbarkeit von Zweckbindung und Datenfluss)

- **Android**
  - Rechtegruppen seit Google Play Store 4.8.19 weiter
  - Kein nachträgliche Kontrolle seit 4.4.2
  - Standortabfrage separat
  - Gyroscope-Gate?!

- **iOS**
  - Ortungsdienste nicht in Control Center
  - Zentrales Datenschutzmenü
  - Backdoors auf HOPE/X bekannt geworden: nur Diagnostics?

- **WP8**
  - Kein Rechtemanagement
  - Beschreibung der Rechte unklar
  - Einstellungen rar und unübersichtlich

Die Betriebssystem-Ebene

- **Schutzziel:** Nichtverkettbarkeit
  (Zweckbindung und -trennung der Daten)

- **Android**
  - MAC, IMEI frei zugänglich
  - Google-Integration
  - Standortdaten an Google (Wahl)
  - WLAN-Scan im Standby
- **iOS**
  - Nutzung der MAC, UDID durch Apps untersagt seit iOS 7
  - iAD parallel
  - Zufalls-MAC ab iOS 8
- **WP8**
  - Standortdaten über MAC-Adresse

Positiv: Werbe-ID in jedem System deaktivierbar
Negativ: Hersteller können immer verketten

Die Betriebssystem-Ebene

- **Schutzziel :** Intervenierbarkeit
  (Jederzeit Auskunft, Sperrung, Löschung, Kontrolle über/von Daten)

- **Android**
  - Google Dashboard gibt Minimalauskunft, aber interne Protokolle unberührt
  - Niederlassung in Europa?
  - Kontrolle mit Root möglich, aber Risiko
  - System- und interner Speicher: Reset
- **iOS**
  - Datenschutz-Kontaktformular
  - Irisches Recht, also Datenschutzrichtlinie
  - Jailbreak nötig für Kontrolle über Gerät
  - iOS „löscht“ durch Vergessen des Verschlüsselungs-Keys
- **WP8**
  - Kontaktformular verfügbar
  - Ansonsten kein Dateimanager mit Systemzugriff
  - Jailbreak kaum verbreitet

Die Betriebssystem-Ebene

- **Schutzziele: Wesentliche Charakteristika**

- **Android**
  - Intervenierbarkeit dank Root jedenfalls technisch möglich
  - Verfügbarkeit leidet etwas an Fragmentierung
  - Verkettbarkeit durch starke Google-Integration
- **iOS**
  - Transparenz akut in Frage gestellt
  - Intervenierbarkeit problematisch wegen Apple-Kontrolle
  - Gute Verfügbarkeit dank lokalem Offline-Backup
- **WP8**
  - Kaum Transparenz und Intervenierbarkeit
  - Verbesserungsfähige Vertraulichkeit durch CalDAC u.ä.

Die Anwendungsebene

- **Technischer und organisatorischer Datenschutz**
  - Stabile, zuverlässige Apps
  - Backup möglich? Eigene oder fremde Server?
  - Starke Passwörter erzwingen
  - Passwörter nicht im Klartext speichern
  - Opt-Out einbauen
  - SSL nutzen
  - Keine eindeutigen Gerätenummern als Identifikatoren
  - Kein unnötiges Logging
  - Besonders sensible Daten besser schützen
    Healthboot (iOS 8), Google Fit (Android L)

Die Hardwareebene

- **Biometrie**
  - Fingerabdrücke, Iris, Gesichtserkennung
  - Speicherort? Hashwert? Zugang?
  - API? Absicherung?
- **Bildschirmqualität**
  - Schlechter Blickwinkel als Feature?
  - Polarisationsfilter auf Smartphones?
- **Mobiles Bezahlen**
  - Seit Android 4.4 KitKat „HCE“
  - Ohne Secure Element (SIM, NFC) kritisch
- **Akku wechselbar?**
  - Ultimativer Off-Switch -> Kontrolle über Hardware

Neue Herausforderung: **Wearables**

Wearables

- **Kontrahenten: Pebble, Android Wear und Samsung**
  - Pebble: Benachrichtigungen, wenig Speicher
  - Android Wear: Bilder und Sprache, viel Speicher
  - Samsung: Begrenzte Kompatibilität
- **Mobil und neugierig**
  - Armbanduhr immer dabei
  - Konzeptionell mehr Sensoren
- **Bluetooth als Schwachstelle**
  - 3-Layer-Sicherheit
  - Meist nur Authentifizierung, keine Verschlüsselung
- **Kleines Display, viele Daten**
  - 4 GB bei der LG G Watch, aber kein sicheres Löschen

Ausblick

Können mobile Systeme und Geräte
datenschutzfreundlich werden?

Ausblick

- **Ist das Blackphone die Lösung?**
  - Insel-Apps keine Lösung
  - Nutzererlebnis darf nicht auf der Strecke bleiben
- **Europa ohne eigene Hersteller** (Xiaomi, Huawei)
- **Globaler Ansatz nötig** (Standards, CE-Kennzeichnung)
- **Security** und **Privacy by Design** als App-Guidelines in App-Stores
- **Transparenz für Nutzer schaffen**
  - Prüfbarkeit für jede(n), nicht nur für Nerds
  - Widerruf der Rechte ermöglichen
  - Komplettes Löschen ermöglichen (Problem: Killswitch)
- **Umdenken:** Gratis-Apps sind nicht umsonst

Zusammenfassende Thesen

Zusammenfassung

Zusammenfassende Thesen:

- Mobile Endgeräte sind besonders lohnende Datenquellen
- Kein mobiles Betriebssystem wird aktuellen Datenschutzvorgaben gerecht
- Android, iOS und Windows Phone 8 bieten unterschiedliche Stärken und Schwächen
- Alternative Systeme mit Privatsphäre-Fokus sind im Entstehen
- Wearables bringen ganz neue und potenzieren bestehende Herausforderungen
- Europa ist derzeit kein Gestalter im Bereich Datenschutz und mobile Endgeräte

Vielen Dank für Ihre Aufmerksamkeit!

Dr. Malte Engeler
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
Holstenstraße 98, 24103 Kiel
0431 988 1200
mail@datenschutzzentrum.de