universität wien

MASTERARBEIT

Titel der Masterarbeit

„Sicherheit, Datenschutz und Privatsphäre von Smartphones am Beispiel von Microsofts Windows Phone“

Verfasser

Georg Binder, Bakk.rer.soc.oec.

angestrebter akademischer Grad

Magister der Sozial- und Wirtschaftswissenschaften (Mag.rer.soc.oec.)

Wien, 2011

Studienkennzahl lt. Studienblatt:	A 066 926
Studienrichtung lt. Studienblatt:	Wirtschaftsinformatik
Betreuerin / Betreuer:	PD DI Mag. Dr. Edgar Weippl

Kurzfassung

Der Untersuchungsgegenstand dieser Arbeit ist Windows Phone. Anhand Microsofts Smartphone soll die These geprüft werden, wonach moderne Smartphones den grundlegenden Anforderungen an Sicherheit, Datenschutz und Privatsphäre nicht gerecht werden. Die Arbeit zeigt, wie die zuvor vorgestellte Sicherheitsarchitektur umgangen werden kann, aber auch wo die Sicherheit akzeptabel erscheint. In Fallbeispielen werden die Privatsphäreneinstellungen überprüft und in Szenarien mögliche Gefahren für den Benutzer analysiert. Auch die Usability hat einen Einfluss auf die Sicherheit, so wird in drei Szenarien Windows Phone mit iOS und Android verglichen, welches Betriebssystem mit weniger Schritten auskommt. Außerdem wird eine videogestützte Untersuchung bezüglich Warnhinweisen durchgeführt, die zeigt, dass Warnhinweise auch auf mobilen Geräten nicht gelesen werden.

Die Arbeit konnte schließlich mittels einer Umfrage nachweisen, dass zu strenge Sicherheitsrichtlinien, zu eklatant unsicherem Verhalten führen. In der Umfrage wurde offenbart, dass in einem Unternehmen eine Sicherheitsrichtlinie direkt dazu führt, dass der PIN-Code für die Bildschirmsperre weitergegeben wird, wenn Kinder im selben Haushalt leben. Eine fortführende Untersuchung hat dann zudem feststellen müssen, dass die Kinder- und Jugendschutzeinstellungen unzureichend sind.

Die These konnte nicht falsifiziert werden.

Abstract

Focus of this work is Windows Phone. Based on Microsoft's smartphone the following thesis should be falsified: modern smartphones do not fulfill the basic requirements for security, data protection and privacy. This work shows how to work around the security boundaries of Windows Phone, but also where security seems to be adequate. In case studies the privacy settings are analyzed as well as possible threats for the user. The usability of the phone has also an impact on security, therefor comparison in three scenarios between Windows Phone, iOS and Android will tell the most efficient system. Next to that a video assisted study shows, that warning messages will not change or influence user behavior.

Based on a survey this work shows, that security policies can be harmful, when they are too strict. In this discovered case a company's policy led to the behavior, that parents share their PIN-code for the lock screen with their children. Following that survey a test of the parental features showed, that they are not sufficient to protect children.

The thesis could not be falsified.

Inhaltsverzeichnis

Kurzfassung I
Abstract II
Inhaltsverzeichnis III
Abbildungsverzeichnis IX
Tabellenverzeichnis X
Abkürzungsverzeichnis X
1 Einleitung 1
1.1 Problemstellung 1
1.2 Erwartete Ergebnisse der Arbeit 1
1.3 Methodischer Ansatz 1
1.3.1 Sicherheitsarchitektur und sicherheitsrelevante Bereiche 1
1.3.2 Erweiterung des Funktionsumfanges von Windows Phone 1
1.3.3 Analyse von Benutzer-Szenarien 2
1.3.4 Videobasierte empirische Userbeobachtung 2
1.3.5 Fragebogen mit statistischer Auswertung 2
1.3.6 Endbewertung 2
1.4 Nutzen der Arbeit 2
1.5 Verwandte Arbeiten 3
2 Grundlagen: Datenschutz und Privatsphäre in Österreich 5
2.1 Definition und von Privatsphäre und Datenschutz und rechtliche Verankerung 5
2.2 Grundrechte und die Fiskalgeltung der Grundrechte 5
2.3 Rechte des Betroffenen 6
3 Einführung in den Untersuchungsgegenstand 8
3.1 Hintergrund von Windows Phone 8
3.2 Die Benutzeroberfläche von Windows Phone 9
3.3 Die Bedienung von Windows Phone 10
3.4 Windows Live ID 11
3.5 Accounts einrichten 12
3.6 Software beziehen 13
3.7 Zune Software 15

3.8 Länderspezifische Unterschiede 15
3.9 Exchange, SharePoint und Office 365 16
4 Sicherheitsarchitektur und sicherheitsrelevante Bereiche 17
4.1 SIM-PIN und Bildschirmsperre 17
4.2 Multitasking 17
4.3 Netzwerksicherheit und Zertifikate 19
4.4 Exchange und Exchange Policies 20
4.5 Wiederauffinden nach Verlust des Phones 22
4.6 Remote Wipe 23
4.7 Information Rights Management 24
4.8 Device Management 25
4.9 Sicherheit im Browser 25
4.10 Bluetooth 25
4.11 Kammern und Sandkästen - Applikationssicherheit 26
4.12 Rechte für Applikationen 26
4.13 Verschlüsselter Speicher 28
4.14 Updates 29
4.15 Sicherheit mit SharePoint Server 29
5 Erweiterung des Funktionsumfanges und Umgehung von Sicherheitssperren 29
5.1 Sideloading 30
5.2 Die nächste Sperre: INTEROP Lock 31
5.3 Registry Editor 31
5.4 Windows Phone als Massenspeicher 31
5.5 Homebrew Software 32
5.6 Illegaler Bezug von Applikationen 34
5.7 Debranding von Windows Phone 34
6 Privatsphäre und Datenschutz auf Windows Phone 36
6.1 Persönliche Daten auf Windows Phone 36
6.2 Datenschutz und Passwort-Sicherheit 38
6.3 Ändern Updates etwas an der Privatsphäre? 38
6.4 Speicherort von privaten und geschäftlichen Daten 39
6.5 Erhöhen der Privatsphäre durch Deaktivierung von Funktionen 39
6.5.1 Setup 39

6.5.2 Aufgabenstellung 40
6.5.3 Erwartungshaltung 41
6.5.4 Auswertung 41
6.5.5 Erkenntnisse 42
7 Benutzer-Szenarien zur Sicherheit 42
7.1 Remote Desktop App 42
7.1.1 Ausgangsbasis/Situation 43
7.1.2 Angriff/Problematik 43
7.1.3 Bedrohungs-/Schadenspotential 43
7.1.4 Lösung/Milderung des Problems 44
7.2 Angriff mittels gefälschter Zertifikate 44
7.2.1 Ausgangsbasis/Situation 44
7.2.2 Angriff/Problematik 44
7.2.3 Bedrohungs-/Schadenspotential 44
7.2.4 Lösung/Milderung des Problems 44
7.3 Apps, die die anonyme ID weniger anonym machen 44
7.3.1 Ausgangsbasis/Situation 45
7.3.2 Angriff/Problematik 46
7.3.3 Bedrohungs-/Schadenspotential 46
7.3.4 Lösung/Milderung des Problems 46
7.4 Positionsdaten missbrauchen 46
7.4.1 Ausgangsbasis/Situation 47
7.4.2 Angriff/Problematik 47
7.4.3 Bedrohungs-/Schadenspotential 47
7.4.4 Lösung/Milderung des Problems 47
7.5 Verzögerte Updates 47
7.5.1 Ausgangsbasis/Situation 47
7.5.2 Angriff/Problematik 48
7.5.3 Bedrohungs-/Schadenspotential 48
7.5.4 Lösung/Milderung des Problems 48
7.6 VPN Tunnel 48
7.6.1 Ausgangsbasis/Situation 48
7.6.2 Angriff/Problematik 48

7.6.3 Bedrohungs-/Schadenspotential 48
7.6.4 Lösung/Milderung des Problems 49
7.7 Personenmarkierungen auf Facebook 49
7.7.1 Ausgangsbasis/Situation 49
7.7.2 Angriff/Problematik 49
7.7.3 Bedrohungs-/Schadenspotential 49
7.7.4 Lösung/Milderung des Problems 49
7.8 Die unsichere Messenger App 50
7.8.1 Ausgangsbasis/Situation 50
7.8.2 Angriff/Problematik 50
7.8.3 Bedrohungs-/Schadenspotential 50
7.8.4 Lösung/Milderung des Problems 51
7.9 Firmeneigene Software nur für die Firma verfügbar machen 51
7.9.1 Ausgangsbasis/Situation 51
7.9.2 Angriff/Problematik 51
7.9.3 Bedrohungs-/Schadenspotential 51
7.9.4 Lösung/Milderung des Problems 52
7.10 Marketplace-Fallen für Benutzer 52
7.10.1 Ausgangsbasis/Situation 52
7.10.2 Angriff/Problematik 52
7.10.3 Bedrohungs-/Schadenspotential 52
7.10.4 Lösung/Milderung des Problems 53
7.11 Sprachsteuerung trotz gesperrtem Bildschirm 53
7.11.1 Ausgangsbasis/Situation 53
7.11.2 Angriff/Problematik 53
7.11.3 Bedrohungs-/Schadenspotential 53
7.11.4 Lösung/Milderung des Problems 53
7.12 Backup- oder Umzugsszenario 54
7.12.1 Ausgangsbasis/Situation 54
7.12.2 Angriff/Problematik 54
7.12.3 Bedrohungs-/Schadenspotential 54
7.12.4 Lösung/Milderung des Problems 54
7.13 Experiment: Unbekannter erlangt auf Facebook Freundesstatus 55

7.13.1 Ausgangsbasis/Situation 55
7.13.2 Angriff/Problematik 55
7.13.3 Bedrohungs-/Schadenspotential 57
7.13.4 Lösung/Milderung des Problems 57
8 Effizienz der Benutzeroberfläche von Windows Phone im Vergleich 58
8.1 Vergleich in Schritten – Weniger ist mehr Sicherheit 58
8.2 Erwartungshaltung 58
8.3 Aufgabenstellung und Testszenarien 59
8.3.1 Szenario 1: E-Mail und Kalender 59
8.3.2 Auswertung und Beurteilung von Szenario 1 65
8.3.3 Szenario 2: Soziale Netzwerke und Kontakte 65
8.3.4 Auswertung und Beurteilung von Szenario 2 70
8.3.5 Szenario 3: Suche und Karten 71
8.3.6 Auswertung und Beurteilung von Szenario 3 76
8.4 Erkenntnisse 76
9 Videogestützte Analyse zu Usability und Privatsphäre 77
9.1 Setup 77
9.2 Aufgabenstellung 80
9.3 Erwartungshaltung 80
9.4 Auswertung 81
9.5 Erkenntnisse 82
10 Umfrage zum Verhalten 82
10.1 Setup 82
10.2 Aufgabenstellung 83
10.3 Erwartungshaltung 84
10.4 Auswertung 84
10.5 Erkenntnisse 86
11 Kinderschutz 88
11.1 Setup 88
11.2 Aufgabenstellung 88
11.3 Erwartungshaltung 88
11.4 Auswertung 89
11.5 Erkenntnisse 90

12 Zusammenfassung und Ausblick 90
13 Quellenverzeichnis 93
14 Anhang 104
14.1 Quelldaten zu Videoanalyse 104
14.2 Quelldaten der Umfrage zum Nutzungsverhalten 104
14.3 Lebenslauf 107

Abbildungsverzeichnis

Abbildung 1 - Lagebasierte Ansichtsänderung, Quelle: Eigene Darstellung 10
Abbildung 2 - Windows Phone Trade Off, Quelle: [38] 18
Abbildung 3 - Lebenszyklus von Applikationen, Quelle: [38].....19
Abbildung 4 - Video-Out Gerät Asus E600; Quelle: Eigene Darstellung.....33
Abbildung 5 - Beispiel für Homebrew-Software, Quelle: Eigene Darstellung 33
Abbildung 6 - Sicherheitsarchitektur, Quelle: Eigene Darstellung 43
Abbildung 7 - Diagramm Experiment Facebookfreund 56
Abbildung 8 - Diagramm Freundschaftsanfragen, Quelle: Eigene Darstellung.....57
Abbildung 9 - Szenario 1 Schritt 1, Quelle: Bearbeitung nach [97].....59
Abbildung 10 - Szenario 1 Schritt 2, Quelle: Bearbeitung nach nach [97] 59
Abbildung 11 - Szenario 1 Schritt 3, Quelle: Bearbeitung nach [97].....60
Abbildung 12 - Szenario 1 Schritt 4, Quelle: Bearbeitung nach [97].....60
Abbildung 13 - Szenario 1 Schritt 5, Quelle: Bearbeitung nach [97].....61
Abbildung 14 - Szenario 1 Schritt 6, Quelle: Bearbeitung nach [97].....61
Abbildung 15 - Szenario 1 Schritt 7, Quelle: Bearbeitung nach [97].....62
Abbildung 16 - Szenario 1 Schritt 8, Quelle: Bearbeitung nach [97].....62
Abbildung 17 - Szenario 1 Schritt 9, Quelle: Bearbeitung nach [97].....63
Abbildung 18 - Szenario 1 Schritt 10, Quelle: Bearbeitung nach [97].....63
Abbildung 19 - Szenario 1 Schritt 11, Quelle: Bearbeitung nach [97].....64
Abbildung 20 - Szenario 1 Schritt 12, Quelle: Bearbeitung nach [97].....64
Abbildung 21 - Szenario 2 Schritt 1, Quelle: Bearbeitung nach [97].....66
Abbildung 22 - Szenario 2 Schritt 2, Quelle: Bearbeitung nach [97].....66
Abbildung 23 - Szenario 2 Schritt 3, Quelle: Bearbeitung nach [97].....67
Abbildung 24 - Szenario 2 Schritt 4, Quelle: Bearbeitung nach [97].....67
Abbildung 25 - Szenario 2 Schritt 5, Quelle: Bearbeitung nach [97].....68
Abbildung 26 - Szenario 2 Schritt 6, Quelle: Bearbeitung nach [97].....68
Abbildung 27 - Szenario 2 Schritt 7, Quelle: Bearbeitung nach [97].....69
Abbildung 28 - Szenario 2 Schritt 8, Quelle: Bearbeitung nach [97].....69
Abbildung 29 - Szenario 2 Schritt 9, Quelle: Bearbeitung nach [97].....70
Abbildung 30 - Szenario 3 Schritt 1, Quelle: Bearbeitung nach [97].....71
Abbildung 31 - Szenario 3 Schritt 2, Quelle: Bearbeitung nach [97].....71
Abbildung 32 - Szenario 3 Schritt 3, Quelle: Bearbeitung nach [97].....72
Abbildung 33 - Szenario 3 Schritt 4, Quelle: Bearbeitung nach [97].....72
Abbildung 34 - Szenario 3 Schritt 5, Quelle: Bearbeitung nach [97].....72
Abbildung 35 - Szenario 3 Schritt 6, Quelle: Bearbeitung nach [97].....73
Abbildung 36 - Szenario 3 Schritt 7, Quelle: Bearbeitung nach [97].....73
Abbildung 37 - Szenario 3 Schritt 8, Quelle: Bearbeitung nach [97].....74
Abbildung 38 - Szenario 3 Schritt 9, Quelle: Bearbeitung nach [97].....74
Abbildung 39 - Szenario 3 Schritt 10, Quelle: Bearbeitung nach [97].....75
Abbildung 40 - Szenario 3 Schritt 11, Quelle: Bearbeitung nach [97].....75
Abbildung 41 - Vorbereitung für den ersten Testaufbau, Quelle: Eigene Darstellung 78
Abbildung 42 - Berührungen sind exakt sichtbar, Quelle: Eigene Darstellung.....79

Abbildung 43 - Diagramm Verweildauer Gruppe 1, Quelle: Eigene Darstellung.....81
Abbildung 44 - Diagramm Verweildauer Gruppe 2, Quelle: Eigene Darstellung.....81
Abbildung 45 - Diagramm Mittelwert Verweildauer, Quelle: Eigene Darstellung.....82
Abbildung 46 - Diagramm Geschlechterverteilung, Quelle: Eigene Darstellung 84
Abbildung 47 - Diagramm Nachgeprüfte Anfragen , Quelle: Eigene Darstellung.....85
Abbildung 48 - Diagramm PIN-Code Weitergabe, Quelle: Eigene Darstellung.....85
Abbildung 49 - Diagramm Haushalten mit Kindern, Quelle: Eigene Darstellung.....86
Abbildung 50 - Diagramm Haushalten ohne Kinder, Quelle: Eigene Darstellung.....86

Tabellenverzeichnis

Tabelle 1 - Exchangefunktionen, Quelle: Eigene Darstellung nach [46] 20
Tabelle 2 - EAS Richtlinien-Unterstützung, Quelle: Eigene Darstellung nach [46] 21
Tabelle 3 - EAS Rückgabewerte, Quelle: Eigene Darstellung nach [46] 21
Tabelle 4 - Liste von Eigenschaften bzw. Capabilities, Quelle: Eigene Darstellung 26
Tabelle 5 - Besondere Eigenschaften, Quelle: Eigene Darstellung 27
Tabelle 6 - Vertriebsmöglichkeiten des, Quelle: Eigene Darstellung nach [94] 51
Tabelle 7 - Beispiele für Sprachbefehle, Quelle: Eigene Darstellung 53

Abkürzungsverzeichnis

Diese Abkürzungen und Synonyme wurden in der Arbeit verwendet.

ADC = Auto Data Config
APN = Access Point Name
Capability = Eigenschaft des Windows Phone Rechtesystems
iOS = Apples OS für iPhone, iPad
IRM = Information Rights Management
Mango = Windows Phone 7.5 (Codename)
MMS = Multimedia Message Service
NTLM = NT LAN Manager (Authentifizierungsverfahren)
OS = Betriebssystem
Phone = Windows Phone
RDP = Remote Desktop Protokoll
SDK = Software Development Kit
SMS = Short Message Service
UAG = Unified Access Gateway
Vgl. = vergleiche
VNC = Virtual Network Computing
VPN = Virtual Private Network
XAP = Installerformat von Apps

1 Einleitung

1.1 Problemstellung

Die Verbreitung von Smartphones ist stark steigend [1]. Ziel der Arbeit ist eine Analyse, welche Auswirkungen die Nutzung eines Smartphones auf die Bereiche (Daten-)Sicherheit, Datenschutz und Privatsphäre hat. Untersucht wird die neueste Plattform von Microsoft -„Windows Phone 7“.

Fragestellungen beinhalten unter anderem:

- Welche Anforderungen an den Datenschutz bestehen? Was kann die Privatsphäre stören?
- Welche Abhängigkeiten gibt es, welche Funktionen können zur Stärkung der Privatsphäre deaktivieren, ohne die Funktionalität einzuschränken? Beispiel: Kann Ortsinformation (GPS) genutzt werden, ohne Daten an den Anbieter zu senden?
- Welche Auswirkung hat die Usability von Privatsphären-Einstellungen?
- Welche Auswirkungen können Updates auf diese Fragestellungen haben?

1.2 Erwartete Ergebnisse der Arbeit

Die These lautet, dass moderne Smartphones den grundlegenden Anforderungen an Sicherheit, Datenschutz und Privatsphäre nicht gerecht werden. Die Arbeit versucht diese These mittels verschiedener methodischer Ansätze zu falsifizieren, erwartet wird jedoch, dass der Beweis nicht zu erbringen ist.

1.3 Methodischer Ansatz

Nach der allgemeinen Einführung in das Thema Smartphone, Datenschutz, Privatsphäre und Windows Phone unterscheidet sich die Methodik der Arbeit nach dem Themengebiet sowie der Fragestellung und beinhaltet:

1.3.1 Sicherheitsarchitektur und sicherheitsrelevante Bereiche

Dieses Kapitel besteht durch Recherche der sicherheitsrelevanten Funktionen und Eigenheiten des Untersuchungsgegenstandes, z.B. wie arbeitet Windows Phone mit Zertifikaten? Welche Möglichkeiten sieht Microsoft für die Fernlöschung vor, welche Bedingungen müssen erfüllt sein, damit das funktioniert?

1.3.2 Erweiterung des Funktionsumfanges von Windows Phone

Nachdem in Kapitel 4 die Sicherheitsarchitektur beschrieben wurde, wird in Kapitel 5 analysiert, mit welchen Mitteln diese Sicherheitsarchitektur umgangen werden kann. Das wird dann auch in Fallbeispielen durchgeführt um empirisch nachzuweisen, wie einzelne Angriffsszenarien auf den Untersuchungsgegenstandes aussehen können, z.B. wie der Marketplace umgangen werden kann, um eine Applikation zu verwenden, die den Richtlinien von Microsoft widerspricht. Ziel dieser Angriffe ist dabei nicht primär der Benutzer oder die Daten auf dem Phone, sondern die Umgehung von Schutzmaßnahmen von Microsoft.

1.3.3 Analyse von Benutzer-Szenarien

In diesem Kapitel werden Szenarien definiert, wo es zu Problemen mit der Sicherheit im Zusammenhang mit Smartphone-Benutzern kommen kann. Hier ist es speziell von Interesse, was mit dem Smartphone gemacht werden kann, z.B. Teilnahme an sozialen Netzwerken oder das Teilen von Informationen mit Cloud Diensten.

Der Aufbau der Szenarien folgt diesem Muster:

- Ausgangsbasis/Situation: beschreibt die Umgebung des Experiments oder des Szenarios und stellt die Grundlage für die weitere Untersuchung dar, z.B. wie bestimmte Konfigurationsmöglichkeiten aussehen.
- Angriff/Problematik: beschreibt die Attacke auf den Benutzer oder die Problemstellung die aus einem Bestimmen (Nicht-)Verhalten oder Umstandes erwächst.
- Bedrohungs-/Schadenspotential: Wenn der unter „Angriff/Problematik“ beschriebene Fall eintritt, dann ist die hier beschriebene negative Auswirkung zu erwarten.
- Lösung/Milderung des Problems: Wenn möglich, dann beschreibt dieses Kapitel, wie das dargestellte Problem zumindest in der Auswirkung abgeschwächt, oder aber gänzlich umgangen werden kann.

1.3.4 Videobasierte empirische Userbeobachtung

In einer videogestützten Teststellung wird nachvollzogen, wie lange die Testkandidaten brauchen, um gegebene Aufgaben zu lösen. Wie werden diese gelöst und werden Sicherheitsprobleme durch die Testkandidaten erkannt? In diesem Kapitel soll einer kleinen Anzahl von Testkandidaten sprichwörtlich „auf die Finger geschaut“ werden um Rückschlüsse bezüglich Usability und Sicherheit ziehen zu können.

1.3.5 Fragebogen mit statistischer Auswertung

Auswertung eines Fragebogens, der Antwortkatalog enthält sowohl offene Fragen als auch geschlossene Fragen um eine bestimmte, während der Erstellung der Arbeit entstandene, Fragestellung zu prüfen.

1.3.6 Endbewertung

Die Ergebnisse fließen in die Endbewertung ein, wo zusammenfassend dargestellt wird, ob die Erwartungshaltung erfüllt werden konnte.

1.4 Nutzen der Arbeit

Die wissenschaftliche Aufarbeitung der Fragestellung rund um den Technologieeinsatz von Smartphones gibt Herstellern die Möglichkeit zum Nachbessern und Benutzern eine Analyse, was bei der Nutzung von Smartphone passiert. Die aufgrund der Erkenntnisse aus Kapitel 7 durchgeführte Umfrage in Kapitel 10 zeigt schließlich auf, welche Konsequenz eine gut gemeinte Sicherheitsrichtlinie auf die reale Sicherheit haben kann.

1.5 Verwandte Arbeiten

Von besonderem Interesse waren bestehende Werke zu mobiler Usability, Nutzung von Smartphones und mobiler Sicherheit.

Windows Phone ist ein Smartphone, in [2] sind Smartphones beschrieben als „mobile Geräte, die meistens einen Breitbandzugang, Office Programme und die Möglichkeit zur Installation von Drittherstellerprogrammen“ aufweisen. Heute dienen sie zur Navigation, zum Spiele, zur Kommunikation über verschiedenartigste Netzwerke und die Nutzung von Smartphone kann weit über das hinausgehen, was nur den einzelnen Benutzer betrifft, so beschreibt [3] einen Mechanismus, wie mit Hilfe von Smartphones die Straßenverhältnisse und Verkehrsbedingungen beobachtet werden können oder sie können Menschen mit besonderen Bedürfnissen, z.B. Gehörlosen die Kommunikation mit Notdiensten ermöglichen, [4] beschreibt eine Windows Phone Applikation mit einer ikonografischen Benutzeroberfläche für solche Fälle. In einer älteren Untersuchung [5], dass es offenbar ein „häufiges Szenario ist, zur Beendigung einer Aufgabe zum PC zu wechseln“, ein Hinweis darauf, dass eben noch nicht alles möglich ist.

Über die Messung zur Nutzung von Smartphone gibt es bereits verschiedene Ansätze, beispielsweise die Analyse über den vom Smartphone verursachten Traffic [6], weiterverfolgt in [7], demnach reicht die Nutzung von 1 MB bis 1000 MB täglich. Dieser Traffic wird wohl auch durch das Hinaufladen von Fotos in soziale Netzwerke zu Stande kommen.

Da Smartphones auch mit sozialen Netzwerken verbunden sind, ist auch deren Sicherheit relevant und bei deren Nutzung avancieren die Benutzer regelrecht zu „zu Richtlinien-Administratoren“ [8], um ihre Privatsphäre zu bewahren. Zum Verlust der Privatsphäre führen aber auch die in [9] genannten und diskutierten Attacken. Weitere Angriffe beschreibt [10] mit einer „Friend-in-the-middle“-Attacke, während sich [11] auf die nicht ausreichend gesicherte Verbindung zwischen Benutzer und Service konzentriert. Ebenso dem Bereich der Privatsphäre einzuordnen sind die Standortdaten. Fluch und Segen zugleich ist die Möglichkeit der Location-based Services, also die Konsumierung von Diensten basierend auf dem Standort, was „einer hohen Bedrohung für die Privatsphäre“ [12] einhergeht. [13] beschreibt ein System, wie man solche Services nutzt „ohne dass die Daten das Gerät verlassen“, alternative Wege sieht auch [14].

Wie in [15] argumentiert, werden “Smartphones oft für, für die Privatsphäre sensible, Aufgaben benutzt”. In ihrer Arbeit geht es um ein alternatives Sicherheitskonzept zu Android, auch [16] entwickelt ein neues System namens *SecureMyDroid*. Die beschriebenen Attacken sind Grundlage für eigene Untersuchungen für Windows Phone. Bezüglich der Sicherheit auf Windows Phone stellt [17] zwar fest, dass Windows Phone nicht der Untersuchungsgegenstand war, denn das war Malware für iOS und Android, meint jedoch, dass es derzeit keine der dort beschriebenen Angriffe auf Windows Phone gibt. Jedoch seien „Die Antriebe für mobile Malware nicht plattformabhängig“.

Das Rechte- und Genehmigungssystem von Smartphones ist von besonderem Interesse, da dieses ja, wie in [18] aufgeführt, dafür verantwortlich ist „Drittherstellerapplikationen in Google Chrome Browser oder in der Facebook Applikationsplattform“ einzuschränken, sodass diese nicht „ausbrechen“ können. Die Arbeit vergleicht auch die Systeme und sieht gewisse Parallelen im Rechtesystem zwischen Windows Phone und Android, wenngleich Windows Phone hier restriktiver erscheint. Die Schnittstellen für den Zugriff wie für Android auch in [19] beschrieben, sind aus Sicherheitssicht auch für diese Arbeit relevant.

Für Android und Windows Phone hat sich als eine zusätzliche inspirierende Quelle für jene Dinge, die nicht offiziell dokumentiert sind, das Forum von *XDA-Developers.com* erwiesen, da dort schon zu den Zeiten des früheren Windows Mobile gute Einblicke in die Umgehung der Sicherheit zu bekommen waren.

Eine völlig andere Nutzung von Smartphones ist das Spielen. Auch das ist für diese Arbeit von Interesse, soll doch eine Wechselwirkung zwischen Kindern und IT gezeigt werden, z.B. wenn ein Mitarbeiter sein Phone seinem Kind zum Spielen zur Verfügung stellt. Die Arbeit von [20] geht auf eine ähnliche Problematik ein, die dann in dieser Arbeit zu einer weiteren Untersuchung geführt hat. Spiele können auch neben reiner Unterhaltung auch einen Lerneffekt haben, so beschreiben [21] die Entwicklung eines Lernspiels auf Basis von Windows Phone. Schließlich ging es bei [22] noch um die Absicherung der Technologie.

Neben der technischen Sicherheitsarchitektur und deren Umgehung ist auch der Zusammenhang zwischen mobiler Sicherheit und mobiler Usability von Interesse. [23] untersucht die Usability von grafischen Klick-Passwörtern auf mobilen Geräten. Diese erscheinen zumindest besser als herkömmliche Passwörter, [24] sieht es so: „Mobile Sicherheit ist von kleinen Geräten gekennzeichnet, die es z.B. schwer machen, lange Passwörter einzugeben“. Auch die Effizienz ist in diesen Zusammenhang zu nennen, wobei [25] offenbart, dass bei besonders attraktiven Produkten „Teilnehmer die Usability sehr hoch bewertet haben, obwohl es offensichtliche Ineffizienzen“ gegen habe. Für die Durchführung eigener Studien das natürlich interessant und ebenso die Fragestellung nach der Datenerfassung bei der Durchführung von Studien. Eine Möglichkeit besteht darin, dass man die Teilnehmer Tagebücher führen lässt, so wie das in [26] und [27] getan wird. Einen wichtigen Hinweis gab [28] dann zur Messbarkeit der Usability über die Effizienz, also „den Grad in wie weit das Produkt ermöglicht Aufgaben schnell, effektiv und ökonomisch zu erledigen oder genau das verhindert“.

Während also gerade im Sicherheitsbereich für andere mobile Geräte bereits Arbeiten vorhanden sind, fehlen diese für Windows Phone noch. Dafür können die Grundlagen und Methoden der Forschung aus dem Bereich der Usability für den Untersuchungsgegenstand übernommen werden.

2 Grundlagen: Datenschutz und Privatsphäre in Österreich

Die Begriffe Datenschutz und Privatsphäre sind in erster Linie auch rechtliche Begriffe. Diese sind in Österreich in einem eigenen Datenschutzgesetz festhalten.

2.1 Definition und von Privatsphäre und Datenschutz und rechtliche Verankerung

Um ein einheitliches Schutzniveau innerhalb der Union herzustellen, besonders im Hinblick nicht nur auf den freien Warenverkehr, sondern auch den auf den freien Datenverkehr, hat das EU Parlament die Datenschutzrichtlinie[1] beschlossen. Eine EU Richtlinie muss von den Mitgliedsstaaten durch entsprechende Gesetze in nationales Recht übernommen werden, die österreichische Umsetzung der EU Datenschutzrichtlinie ist das Datenschutzgesetz 2000[2] (DSG 2000). Datenschutz ist ein Grundrecht[3], das sagt auch die Europäische Menschenrechtskonvention (Art. 8 EMRK). Das Datenschutzgesetz setzt die Rahmenbedingungen für den Umgang mit Personendaten, es gilt gleichermaßen für öffentlich-rechtliche wie für privatrechtliche Datensammlungen (wie bei Unternehmen, Vereinen, sonstigen Organisationen, ...). Das DSG 2000 regelt alle Fragestellungen zum Thema Privatsphäre, sofern nicht durch einzelgesetzliche Regelungen, gültige vertragliche Vereinbarungen, gültige Willensübereinstimmung oder gültige freiwillige Zustimmung durch den Betroffenen andere Regelungen wirksam sind.

Als sensible und schützenswerte Daten werden im §4 DSG 2000 Daten gesehen, wenn von einem Betroffenen die Identität bestimmt oder bestimmbar ist. Sensible Daten sind weiters, wenn „rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder ihr Sexualleben“ betroffen sind.

2.2 Grundrechte und die Fiskalgeltung der Grundrechte

Grundrechte sind verfassungsgesetzlich gewährleistete subjektive Rechte[4]. Unter den klassischen, bürgerlichen Grundrechten versteht man den Schutz der Freiheit des Einzelnen gegenüber der Staatsgewalt, z.B. dem Recht auf die persönliche Freiheit. Daneben kennt man politische Grundrechte oder Teilhaberechte wie der Beteiligung des Volkes an der Ausübung der Staatsgewalt, z.B. das Wahlrecht. Soziale Grundrechte wiederum definieren Leistungsansprüche des Einzelnen gegenüber dem Staat, z.B. das Grundrecht auf Arbeit. Der Staat ist verpflichtet, die ungestörte Grundrechtsausübung vor Eingriffen von dritter Seite zu mit angemessenen Mitteln schützen, sofern er dazu in der Lage ist. Grundrechte stehen jeder natürlichen und juristischen Person zu (letztere wenn das dem Wesen des betreffenden Grundrechts nach möglich ist, z.B. Eigentums- und Erwerbsfreiheit). Neben Jedermannsrechten, die allen Menschen zustehen, wie z.B. Menschenrechte, gibt es Grundrechte die nur für die Staatsbürger gewährleistet sind, z.B. das Wahlrecht. Durch eine verfassungsrechtliche Ermächtigung kann der einfache

[1] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995
[2] Datenschutzgesetz 2000 (DSG 2000), BGBl. I Nr. 165/1999
[3] § 1 Abs. 1 DSG 2000
[4] Art 144 B-VG

Gesetzgeber die Ausübung des Grundrechts auch in beschränkendem Sinne näher regeln. Eingriffe dürfen dabei niemals gegen das „Wesen“ des Grundrechts verstoßen, d.h. so weit gehen, dass das Grundrecht gleichermaßen aufgehoben wird. Eingriffe müssen durch ein öffentliches Interesse sachlich gerechtfertigt, zu dessen Durchsetzung geeignet und in ihrer Wirkung Maß haltend sein. Beschränkungen kann es durch ein besonderes Rechtsverhältnis geben, z.B. im Strafvollzug oder bei Militär- bzw. Zivildienst. Der Staat ist auch dann an die Grundrechte gebunden, wenn er in privatrechtsförmiger Weise typisch staatliche („öffentliche“) Aufgaben besorgt. Grundsätzlich, soweit nicht gesetzlich etwas anderes vorgeschrieben ist, steht es dem Staat frei, ob er sich zur Erfüllung seiner materiell und funktionell öffentlichen Aufgaben öffentlicher oder privater Rechtsformen z.B. Verkehrsbetriebe, Energieversorgung, Theater. Doch kann sich der Staat der Bindung an die Grundrechte in Bereichen, in denen er zur Wahrnehmung öffentlicher Aufgaben verpflichtet ist, nicht entziehen, auch dann nicht, wenn er hoheitlich handelt. Die Pflicht des Staates zur Beachtung der Grundrechte bleibt somit unabhängig von der wirtschaftlichen Form, in der er handelt, immer bestehen. Man bezeichnet das die „Fiskalgeltung der Grundrechte“. Dies gilt natürlich auch für den Datenschutz. Privatpersonen werden durch Grundrechte nicht gebunden, sehr wohl aber durch auf diesen Grundrechten aufbauende Gesetze, es besteht nur eine mittelbare (keine unmittelbare) Drittwirkung, d.h. Grundrechte wirken über einfache Gesetze (und nicht direkt als Verfassungsgesetz) auch auf die Rechtsverhältnisse zwischen Privaten.

2.3 Rechte des Betroffenen

Das DSG 2000 regelt auch Grundrechte, die es Betroffenen ermöglichen sollen ihre Privatsphäre zu sichern, sowie den Betroffenen auch Rechtsmittel in die Hand zu geben, ihre Rechte gegenüber Dritten durchzusetzen. Diese Betroffenenrechte werden als "subjektive Rechte" bezeichnet.

- Recht auf Geheimhaltung (§§ 1ff DSG 2000, Verfassungsbestimmung): Gleich ob Daten maschinell oder manuell verarbeitet werden, unterliegen personenbezogene Daten der Geheimhaltung, „verwendungsfreie“ Daten existieren nicht. Eingeschränkt wir der Geheimhaltungsanspruch bezüglich Daten, die zulässigerweise veröffentlicht wurden, z.B. wenn jemand zugestimmt hat, dass seine Adresse im Telefonbuch veröffentlicht wird. Unter bestimmten Voraussetzungen bzw. durch bestimmte Gesetze wird das Recht auf Geheimhaltung weiter eingeschränkt, z.B. das Einkommenssteuergesetz, das Meldegesetz, die Sozialversicherungsgesetze, das Sicherheitspolizeigesetz.
- Recht auf Auskunft (§ 26 DSG 2000): Betroffene haben das Recht Auskunft über Daten zu anzufordern. Dabei muss die Auskunft innerhalb von acht Wochen erfolgen sowie in allgemein verständlicher Form zu erfolgen, d.h. ohne unverständliche Codes und Abkürzungen. Dieses Auskunftsrecht steht einem Betroffenen pro Auftraggeber einmal im Jahr zu. Als Voraussetzung um erfolgreich eine Auskunft zu erhalten, muss der Betroffenen dem Auftraggeber seine Identität nachweisen, sowie bei der Auskunftserteilung mitwirken, indem er

z.B. seine Beziehung zum Auftraggeber angibt oder die DVR Nummer, wo der Betroffenen seine Daten vermutet.

- Recht auf Berichtigung und Löschung (§ 27 DSG 2000):Prinzipiell sind nicht mehr aktuelle oder unrichtige Daten zu berichtigen und nicht mehr benötigte Daten oder unberechtigt ermittelte bzw. verwendete Daten zu löschen. Eine aktive Kontrolle und Aktualisierung der Daten durch den Auftraggeber hat auch der nach wirtschaftlicher Vertretbarkeit zu erfolgen. Wesentlich verschärft sind die Aktualisierungspflichten, wenn Daten auch für Dritte bereitgestellt werden oder sogar veröffentlicht werden, gerade dann wenn die Art der Daten eine für den betroffenen negative Auswirkung haben kann (z.B. unrichtige Bonitätsauskünfte). Erlangt ein Datenverarbeiter Kenntnis (nicht nur, aber vornehmlich durch den Betroffenen) von einer, für seine Zwecke wesentlichen, Änderung der Daten, so hat binnen acht Wochen die Berichtigungen oder Löschungen zu erfolgen, andernfalls ist innerhalb dieser Frist zu begründen, warum dem nicht nachgekommen werden kann.
- Informationsrecht (§ 24 DSG 2000): Dem Betroffenen muss anlässlich der Ermittlung seiner persönlichen Daten durch den Auftraggeber mitgeteilt werden, zu welchem Zweck Daten ermittelt werden und auch wer der Verantwortliche für die Datenanwendung ist. Dieses Informationsrecht hat der Auftraggeber ohne besonderes Zutun des Betroffenen einzuhalten. Sinn hinter dieser Regelung wäre, dem Betroffenen eine gewisse Orientierungshilfe über die Verwendung seiner Daten zu geben.
- Recht auf Widerspruch (§ 28 DSG 2000): Gegen die Aufnahme der eigenen Daten in bestimmten Datenanwendungen kann Widerspruch erhoben werden. Im Gegensatz zum Widerruf, der sofort gültig ist, ist ein Widerspruch binnen acht Wochen zu berücksichtigen. Die ARGE Daten definiert [29]: "Das wesentlichste Unterscheidungskriterium besteht darin, dass ein Widerruf vorher die Zustimmung zu einer Datenverwendung voraussetzt (in der Regel wird irgendein Vertragsverhältnis zwischen Auftraggeber und Betroffenen existieren), während der Widerspruch auch bei Auftraggebern anzuwenden ist, mit denen man zwar keine Geschäftsbeziehungen hat, denen es aber gelungen ist, die persönlichen Daten irgendwie legal zu erhalten."
- Recht auf Widerruf (§§ 8, 9 DSG 2000): Betroffene können eine zuvor freiwillig eingeräumte Verwendung der Daten jederzeit widerrufen. Dabei darf der Widerruf keinen Einfluss auf einen bestehenden Vertrag haben, solange der Auftraggeber seine vertraglichen Pflichten trotz Widerruf erfüllen kann. Ein Widerruf ist immer sofort wirksam.
- Recht auf Information über logischen Ablauf bei automatisierten Einzelentscheidungen (§ 49 Abs. 3 DSG 2000): Der Betroffene kann von sich aus beantragen, darüber informiert zu werden, mit welchen Mitteln, Methoden und Programmen eine automatisierte Entscheidung zustande kam (z.B. Computer-Führerscheinprüfung).

3 Einführung in den Untersuchungsgegenstand

Der Untersuchungsgegenstand ist Windows Phone, das Smartphonebetriebssystem von Microsoft.

3.1 Hintergrund von Windows Phone

Um die Fähigkeiten und die Welt von Windows Phone zu verstehen, ein kurzer Blick in die Geschichte: Microsoft hat schon öfters die Fähigkeit bewiesen, aktuelle Trends zu verschlafen, darunter das Internet: die ersten Versionen von Windows 95 hatten noch nicht mal einen Browser mit dabei, Bill Gates schrieb in seinem Buch [30] noch von Compuserve, AOL und dem Microsoft Network, erst in späteren Auflagen kam das Internet dazu und bei Windows 95 ein Browser. Zuerst war dieser sogar ein kostenpflichtigerer Zusatz im Rahmen des Produkts „Microsoft Plus! for Windows 95“ [31]. Dann gibt es noch die Sache mit dem falschen Zeitpunkt, immerhin hatte Microsoft bereits 2002 eine extra Ausgabe von Windows XP TabletPC Edition mit Stifteingabe und Handschrifterkennung. Natürlich gehört auch dazu, das Potential von Ideen richtig einzuschätzen, so hatte Microsoft mit TerraServer [32] etwas, das später Google durch Kauf der Firma Keyhole erfolgreich zu Google Earth gemacht hat. Das Beispiel Google dürfte Microsoft aber auch ermutigt haben: mit Android wurde bewiesen, dass man mit einem neuen Produkt im Smartphone-Markt nicht verloren dasteht.

Microsoft hatte beginnend im Jahr 2001 mit *Pocket PC 2002 for Smartphones* bis hin zu Windows Mobile 6.5 schon einige Smartphone-Betriebssysteme, jedoch galt „Windows Mobile“ veraltet und die Unterstützung seitens Mobilfunkbetreiber oder Hardware-Hersteller reichte offenbar nicht mehr aus um dieses System weiterzuführen. Microsoft entschloss sich, einen Neustart zu versuchen. Ausgehend vom Windows CE Kernel des Musikplayers Zune wurde das neue Windows Phone 7 Betriebssystem entwickelt. Auf der Hardwareseite gab es stärkere Vorgaben an die Hardware-Hersteller, so musste beispielsweise jedes Endgerät eine Auflösung von 800x480 Pixel aufweisen. Teilweise gab es auch Mindestanforderungen, die übertroffen werden können, wie z.B. mindesten 8 GB Speicher. Die Anforderungen an die Performance, die Sicherheit und das Benutzererlebnis sollen so überall erfüllt werden. Hersteller sind unter anderem Nokia, HTC, Samsung, LG oder Acer. Außerdem wurde die Zielgruppe des neuen Smartphones neu definiert, diese lautete nunmehr: „Konsumenten“. Allerdings bedeutete der Ausrichtung in der ersten Version von Windows Phone auf Konsumenten auch den Verzicht auf die bisherige Zielgruppe des alten Windows Mobile: Firmenkunden. Zwar sind einige Dinge in Windows Phone enthalten, die ausschließlich (größeren) Firmenkunden vorbehalten sind (wie etwa der Dokumentenschutz IRM, siehe Kapitel 4.7), andererseits fehlen Dinge wie Device Management oder VPN-Tunnel nahezu komplett..

Als Untersuchungsgegenstand ist Windows Phone vor allem dadurch interessant, dass Microsoft nach wie vor einen sehr guten Stand bei Firmenkunden hat. Microsoft „profitiert vor allem von einem weiterhin guten Geschäft mit Firmenkunden“ [33] meint Heise. Mit dem Partner Nokia damit eine gute Ausgangsbasis für die Etablierung eine

dritten großen Smartphoneökosystems neben Googles Android und Apples iOS, das prophezeien auch Analysten wie Gartner, die Windows Phone im Jahr 2015 beim einem Marktanteil von knapp 20% sehen wollen [1]. Deswegen wird Windows Phone relevant und die Frage nach der Sicherheit bei diesem System ist umso relevanter.

3.2 Die Benutzeroberfläche von Windows Phone

Microsoft hat eine mit Windows Phone 7 eine sehr eigenständige Benutzeroberfläche geschaffen. Zentrales Element ist der Startbildschirm mit seinen sogenannten Hubs und den Live-Kacheln (das sind die Quadrate, die in zwei Spalten nach Belieben angeordnet werden können). Dieses Oberflächendesign von Windows Phone 7 hört auf den Namen „Metro". Die abgeschnitten Überschriften zeigen immer an, in welche Richtung man scrollen kann. Dadurch wird die Fehlbedienung erschwert, weil man weiß: da geht es weiter. Am Startbildschirm werden in individuell angeordneten Kacheln („Tiles") die wichtigsten Informationen („Gibt es neue E-Mails?") und Neuigkeiten (aus den Hubs wie etwa den Kontakten) angezeigt werden. Zum Startbildschirm kommt man jederzeit durch Druck auf die Windows-Taste. Ebenso auf dem Startbildschirm sichtbar sind die sogenannten Hubs. Anders als Kacheln, die Informationen nur aus einer Quelle beziehen, agieren diese Hubs in gewisser Weise als „Über-Apps". Sie stellen die Informationen und Daten aus verschiedenen Quellen zusammen dar bieten und auf einfachste und schnelle Weise Zugang zum jeweiligen Thema. So ist beispielsweise der Kontakte-Hub nicht einfach nur ein Adressbuch mit den Einträgen der entsprechenden Konten (Outlook, Google, etc.) sondern zeigt die gesammelten Informationen aus den sozialen Netzwerken an (Facebook und Windows Live).

Bei Windows Phone gibt es insgesamt sechs Hubs:

- Kontakte
- Bilder
- Marketplace
- Xbox Live
- Musik & Video
- Office

Die Bedienelemente auf Windows Phone umfassen:

- Schieberegler: Die Schieberegler finden sich oft in Einstellungsseiten Ihres Phones oder Applikationen. Sie funktionieren wie Ein-/Ausschalter. Durch Schieben in die jeweils andere Position wird eine Option (de-)aktiviert, was auch farblich angezeigt wird.
- Drehräder: Bei Datums- oder Zeiteingaben helfen Drehräder bei der schnellen Eingabe. Wischen (mit dem Finger auf den Screen drücken und gedrückt in eine Richtung ziehen) Sie schnell vertikal um flott in den richtigen Bereich zu kommen, stoppen Sie die Drehbewegung durch nochmaliges Antippen.
- Buchstabenselektor zum Springen in langen alphabetischen Listen, wie zum Beispiel den Kontakten

- Bildschirmrandoptionen: Bei vielen Anwendungen tauchen am Bildschirmrand Symbole für Funktionen auf.
- Checkboxen, Texteingabefelder und weitere Eingabefelder

Am oberen Bildschirmrand befindet sich die Statusleiste, die neben der Uhrzeit auch noch andere Zustände anzeigt, z.B. über Verbindungsqualität, die Verbindungsart, und den Ladezustand der Batterie. Die Leiste wird meistens nur reduziert dargestellt, nur WLAN (wenn eingeschaltet) und die Uhrzeit sind sichtbar – und die Akkuanzeige, wenn sie zur Neige geht. Streicht man mit dem Finger von oben (außerhalb des Bildschirms beginnen) nach unten, dann erscheint sie vollständig.

Inhalte des Phones werden je nachdem wie man das Gerät hält im Hochformat (auch: Porträt) oder Querformat (Landscape) angezeigt. Nicht alle Anwendungen oder Screens lassen sich drehen. So wird beispielsweise der Startbildschirm immer im Hochformat angezeigt. Spiele hingegen sind dagegen oft auf das Querformat festgelegt.

Abbildung 1 - Lagebasierte Ansichtsänderung, Quelle: Eigene Darstellung

Dafür bietet das Querformat manchmal zusätzliche Funktionen, wie in Abbildung 1 am Beispiel des Rechners ersichtlich, der sich vom einfachen Taschenrechner im Hochformat zum wissenschaftlichen Werkzeug im Querformat verwandelt – und das sogar mit unterschiedlichen Funktionen, je nach dem in welche Richtung man das Phone dreht.

3.3 Die Bedienung von Windows Phone

Auch wenn es einzelne Phones mit Tastatur gibt, wie das DELL Venue Pro oder das HTC HD 7 Pro, so ist Windows Phone konsequent auf Touch-Bedienung ausgelegt. Elemente werden durch Tippen, dem Äquivalent von einem „Klick“ aktiviert. Hält man eine kurze Zeit auf derselben Stelle den Finger gepresst, dann spricht man von „Tappen“. Zweimal kurz hintereinander auf dieselbe Stelle tippen – das ist das Äquivalent zum Doppelklick auf dem PC. Der Doppelklick kommt relativ selten vor, er findet beispielsweise Verwendung bei Bildern um in das Bild zu zoomen, ebenso bei den Karten oder um auf der Tastatur durch Doppeltippen auf die Umschalttaste die Feststelltaste zu aktivieren.

Für den Bildlauf z.B. im Browser oder in der Kontakteliste wischen man schnell über den Bildschirm, von oben nach unten um zu Scrollen – oder auch in der horizontalen, um sich seitlich durch die Menüs zu bewegen. Für eine genauere, kontrollierte Bewegung, um etwa nur einige Zeilen zu scrollen, wischt man nicht gleich über den Bildschirm, sondern tippt auf ein Element, hält den Finger am Screen und zieht dann in die gewünschte Richtung. Um Bilder oder Kartenausschnitte gezielt zu vergrößern oder zu verkleinern tippt man gleichzeitig mit zwei Fingern auf den Bildschirm und zieht diese auseinander (vergrößern) oder zueinander (verkleinern).

Texteingabe erfolgt über die Bildschirmtastatur, die im Hoch- oder Querformat funktioniert. Links unten befindet sich mit &123 gekennzeichnet die Wechsel-Taste zu den Zahlen und Sonderzeichen und darüber die Umschalt-Taste für Großbuchstaben. Mit einem Doppelklick auf die Umschalttaste (also zweimal schnell hintereinander antippen) aktiviert man die Feststell-Taste. Auf der rechten Seite befindet Sie die Backspace/Rückschritt-Taste und darunter die Eingabe-Taste. Umlaute oder Akzentzeichen lassen sich durch tappen des entsprechenden Buchstabens eingeben, so wird aus einem A ein Ä oder Á. Oftmals ist es jedoch schneller keine Umlaute zu verwenden, sondern sich auf die Autokorrektur zu verlassen. Das Feld &123 führt zu den Ziffern und Sonderzeichen, dort ist statt der Umschalttaste noch ein Pfeil für weitere allgemeine Sonderzeichen. Hier befindet sich auch die Option um an weitere Zeichen zu kommen. Tappt man die entsprechende Taste bekommt man statt einer runden Klammer eine eckige angezeigt, statt € den $, usw. Je nachdem, in welcher Anwendung man sich gerade befindet, ändern sich das Texteingabefeld und die Tastatur. Ist es ein Feld, in dem man E-Mail-Adressen oder URLs eingeben kann, sind das „@“-Zeichen und ein Feld für die Top-Level-Domain .com neben dem Leerzeichen zu finden. Wenn man einen Text tippt, dann blenden sich automatisch Vorschläge aus dem Wörterbuch ein. Tippt man auf einen Vorschlag, dann wird dieser sofort übernommen und man kann weiter schreiben. Weitere Vorschläge lassen Sie sich mit einem Wischen in der Vorschlagsleiste anzeigen. Eigene Vorschläge fügt man dem Wörterbuch hinzu, in dem man das bis dato unbekannte Wort antippt und in der Vorschlagsleiste auf das „+“-Symbol klickt. Erscheint in den Vorschlägen ein Eintrag fett, dann ist das der Hinweis, dass das Wort automatisch ersetzt wird. Die Autokorrektureinstellung und weitere Eingabehilfen sind im Auslieferungszustand eingeschaltet. Konfiguriert werden diese unter Einstellungen unter *Einstellungen, System, Tastatur* wo man auch das Benutzerwörterbuch zurücksetzen kann. Ein einzelnes Löschen von Worten aus dem Wörterbuch ist nicht vorgesehen. Ebendort lassen sich auch weitere Tastaturlayouts für weitere Sprachen hinzufügen. Diese wechseln auch das Wörterbuch in die gewählte Sprache.

3.4 Windows Live ID

Die Windows Live ID ist das Authentifizierungssystem von Microsoft und wird bei vielen Diensten genutzt, etwas Online-Spieleservice Xbox, dem Video- und Musikstreamingdienst Zune oder dem Instant Messenger Windows Live Messenger. Es besteht aus einer E-Mail-Adresse und dem dazugehörigen Kennwort, vergleichbar mit einer Google ID oder einem iTunes-Konto. Hierzu kann jede beliebige E-Mail-Adresse

herangezogen werden. Das Anlegen eines Hotmail-Kontos – Microsofts E-Mail-Dienst – ist nicht zwingend notwendig. Sämtliche Einkäufe, die über den Marketplace getätigt werden, wie z.B. Apps oder Musik, werden an diese Live-ID gebunden, genauso wie der Xbox Live Account, der für Spiele verwendet wird. Auch die Verwaltung über die Weboberfläche, z.B. die Lokalisierung des Endgeräts hängt an dieser Live ID. Es kann nur eine einzige „volle“ Live ID gewählt werden, mit der die Funktionen des Betriebssystems genutzt werden können. Weitere, zusätzliche, Live IDs zur Nutzung von Hotmail-Mailboxen, Kontakte- und Kalendersynchronisation können nachträglich beliebig viele weitere hinzugefügt und wieder gelöscht werden, jedoch ist nur die primäre ID mit den Diensten wie Xbox, Zune, Messenger oder SkyDrive verbunden. Diese primäre ID kann nicht mehr geändert werden, das Phone ist auf diese ID festgelegt. Muss man diese ID ändern, so geht das nur über einen „Hardreset“, der das Phone in den Auslieferungszustand zurückversetzt wird.

Die Live ID lässt sich auch direkt am Phone erstellen, dann braucht man allerdings eine bestehende E-Mail-Adresse. Es lässt sich keine neue Live ID am Phone erstellen, wenn man keine andere E-Mail-Adresse hat, das geht nur über Web, wo man bei der Erstellung über *www.live.com* statt einer alternativen E-Mail-Adresse auch eine Sicherheitsfrage zum Zurücksetzen des Passworts angegeben werden kann. Um eine bestehende E-Mail-Adresse, also z.B. vorname.nachname@example.org zu verwenden, muss diese erst als Live-ID registriert werden. Das kann man unter *www.live.com* bei *Registrieren* und *Eigene E-Mail-Adresse verwenden* gemacht werden.

3.5 Accounts einrichten

Es gibt verschiedene Typen von Konten, die man mit Windows Phone abrufen kann. Hier kann zwischen „Premium“ und “Basic” unterscheiden. Als „Premium“ gelten jene Dienste, die über Exchange ActiveSync die Verbindung aufnehmen (siehe dazu Kapitel 4.4):

- Microsoft Exchange
- Microsoft Hotmail
- Google Mail
- Alle weiteren Anbieter die das Exchange ActiveSync Protokoll verwenden.

Diese Dienste synchronisieren neben E-Mails, auch die Kontakte, Aufgaben und Kalender. Durch die „Direct Push“ genannte Technologie kommen diese Elemente unmittelbar auf das Endgerät und nicht erst nach einer Wartezeit. Beim primären Windows Live-Account werden Kontakte und Kalender immer synchronisiert, lediglich der E-Mail-Abgleich lässt sich ausschalten. Bei allen anderen Konten kann gewählt werden, ob Mail, Kalender, Aufgaben und Termine synchronisiert werden sollen. Konfigurierbar ist die Zeitspanne in welchen Abständen das jeweilige Konto auf Neuerungen abgefragt werden soll. Man kann hier zwischen *Manuell* bis hin zu *Bei Eintreffen* (Push Mail, nicht bei POP3) wählen.

Bei „Basic“-Konten wie POP3- und IMAP4-Konten, die ebenfalls am Phone unterstützt werden, werden nur E-Mails abgefragt. Was alle Konten jedoch gemeinsam haben: Man fügt sie unter *Einstellungen, System, E-Mail-Konten & andere* hinzu. Die Einrichtung wird durch Autodiscover erleichtert, einem Automatismus zur Erleichterung der Einrichtung durch den Versuch, die entsprechenden Servernamen durch Abfrage des DNS bzw. MX-Eintrags des Kontos ohne weiteres Zutun des Benutzers zu ermitteln. So wird bei den allermeisten Konten die Eingabe von E-Mail-Adresse und dazugehörigem Passwort ausreichend zur Konfiguration sein. Schlägt das fehl, lassen sich die Server-Adressen auch manuell eingeben. Die Anzahl an Konten ist nicht beschränkt.

Außerdem lassen sich die Verknüpfungen zu bestimmen sozialen Netzwerken einrichten, das sind neben Windows Live: Facebook, Twitter und LinkedIn. Diese Netze sind tief in das System integriert und Neuigkeiten tauchen im Kontakte-Hub, sowie bei den einzelnen Kontakten auf. Es gibt keine öffentliche Schnittstelle („API“) zur Integration weiterer Anbieter. Diese können nur mittels einer extra App auf das Phone kommen, vgl. [34].

Wenn man seine Daten und Einstellungen mit einem Dienst gar nicht mehr synchronisieren will, lässt sich das Konto unter *Einstellungen, System, E-Mail-Konten & andere* entfernen.

Jedes Konto erscheint als eigene Live-Kachel auf dem Startseite und bleibt so sauber getrennt. Allerdings lassen sich Konten auch zusammenfassen, dies nennt Microsoft *Linked Inboxes*. Beispiel: Die private Hotmail-Adresse und die ebenfalls private GMX-Adresse sollen auf dem Gerät als ein einziger Posteingang erscheinen und zusammengefasst werden. Dazu wählt der Benutzer den ersten Posteingang und dort in den Optionen *Posteingänge verknüpfen*. Am nächsten Bildschirm wählt er das zweite Konto (oder mehrere) aus. Diese werden fortan als ein Posteingang gezeigt, lediglich beim Senden von diesem Konto wird man gefragt, welche Absenderadresse (bzw. Server) verwendet werden soll.

3.6 Software beziehen

Die Software bzw. im Smartphonebereich „Apps“ genannt lassen sich auf drei verschiedene Arten beziehen:

- Über den Marketplace auf dem Phone, hier gibt es einen eigenen Hub (siehe Kapitel 3.2), wo die Software in Kategorien wie etwas „Spiele“ oder „Tools und Produktivität“ eingeordnet ist.
- Über den Web Marketplace auf über *www.windowsphone.com*, wo man auch eine Historie der installierten Anwendungen sieht, was sich gut eignet um Software auf einem weiteren Endgerät zu installieren, da man nur dort sieht, was man alles gekauft oder zumindest probiert hat (Testversionen).
- Über die Zune-Software. Eine Reinstallation einer bereits bezogenen App ist über die Zune-Software nicht möglich („Bereits gekauft“). Diese App muss über den Web Marketplace oder das Gerät selbst wieder installiert werden.

Der Applikations-Entwickler kann einen Preis für die App festsetzen, dieser reicht von mindestens 0,99 € bis hin zu 426,49 €. Eine Rückgabe bei gekaufter Software sieht Microsoft nicht vor, es gilt „gekauft ist gekauft". Deshalb kann der Entwickler eine Testversion vorsehen. Diese Testversion kann beschränkt sein, z.B. nicht alle Funktionen verfügbar, oder nur eine bestimmte Zeit nutzbar. Der Anwender kann sich so ein Bild machen, und erst anschließen den Kauf tätigen. Auch Gratis-Applikationen bzw. werbefinanzierte Apps sind vorgesehen. Ein Feedbacksystem soll dem Benutzer ebenso einen Hinweis auf die Qualität der App geben, so können Apps mit einem bis fünf Sternen bewertet werden, je mehr Sterne, desto besser. Zusätzlich können Kommentare abgegeben werden.

Im Marketplace wird angegeben, welche Fähigkeiten, von nun an „Capabilities" genannt, die Software nutzt. Diese sollen „die Angriffsoberfläche reduzieren" [35] dies wird nicht nur angezeigt, sondern im Fall, dass Ortungsfunktionen genutzt werden auch beim Benutzer abgefragt, ob er damit einverstanden ist. Mehr zu den Capabilities siehe Kapitel 4.11.

Software die größer ist als 20 MB muss über WLAN- oder die Zune-Software installiert werden, das sieht Microsoft als Schutz vor irrtümlich überzogenem Volumen bei Mobilfunkverträgen mit Datenlimit vor. Beispiel: Die Navigationssoftware *Navigon* hat 2,3 GB an Kartenmaterial mit dabei. Werden mehrere Apps installiert, so wird die Gesamtsumme nicht für das 20 MB Limit zusammengezählt, es zählt also die Einzelapplikation zum 20 MB Limit.

Im Marketplace kann derzeit ausschließlich mit Kreditkarte bezahlt werden. Ohne Kreditkarte können keine kostenpflichtigen Applikationen bezogen werden. So man das über *www.windowsphone.com* unter *Konto* nicht bereits eingestellt hat – oder andere Live Services, wie etwa Xbox Live nutzt und dort bereits seine Daten hinterlegt hat, wird man beim ersten Kauf zur Eingabe der Kreditkartendetails aufgefordert.

Allerdings kennt Microsoft sehr wohl ein Prepaid-Verfahren mit Rubbelkarten. Denn für Filme über den Zune-Marketplace oder kostenpflichtige Xbox Live Avatar-Gegenstände müssen vorher Microsoft-Points gekauft werden. Auch ein Spiel mit In-Game Bezahl-Inhalten namens *Beards & Beaks* nutzt diese Microsoft Points. Diese kann man entweder im Handel beziehen oder online mit Kreditkarte gekauft werden. Einzulösen sind die Punkte dann auf *www.xbox.com* und können dann eingesetzt werden. Über *https://billing.microsoft.com* sieht man die Einkaufshistorie und die aktuelle Abrechnung. Dort kann auch die Kreditkarte aktualisiert oder andere Abrechnungsdetails verändert werden. Anwendungen, die einmal gekauft wurden, können jederzeit wieder installiert werden, solange man dieselbe Live-ID verwendet – auch auf mehreren Geräten installiert werden.

Eine Abrechnung auf Firmenrechnung, bzw. eine Applikation den Mitarbeitern zu bezahlen und die Kosten auf ein Sammel- oder Firmen-Konto zu übernehmen, ist nicht vorgesehen. In Falle, dass eine Firma aus geschäftlichen Gründen eine bestimmte

Anwendung bei den Mitarbeiter installieren und bezahlen möchte, müssen die Mitarbeiter dies selbst bezahlen und über eine Spesenabrechnung rückverrechnen. Ebenso nicht vorgesehen sind Familienfunktionen, so kann ein Elternteil nicht einem Kind-Konto eine Applikation „schenken“ (also für das Kind mit der Elternkreditkarte kaufen). Mehr dazu unter Kapitel 11.

3.7 Zune Software

Unter dem Brand „Zune“ lassen sich bei Microsoft verschiedene Dinge finden, einerseits die mittlerweile eingestellte Zune-Hardware, ein Musikplayer. Andererseits steht Zune auch für die Zune-Services, das sind Musik- und Video-Streaming Services, die von PCs, der Xbox oder Windows Phone konsumiert werden können. Und schließlich ist Zune eine Desktop-Software für Windows-PCs, die für bestimmte Szenarien mit Windows Phone erforderlich ist. Zwar ist zur Inbetriebnahme von Windows Phone keine Zune-Software notwendig, zwingend benötigt wird Zune jedoch aus diesen Gründen:

- Synchronisation von Bildern, Musik und Videos vom Desktop-PC auf das Telefon.
- Installation von Updates.
- Download von Bildern und Videos in Originalauflösung vom Telefon auf den PC.

Diese Dinge können ausschließlich über die Zune-Software durchgeführt werden. Außerdem lassen sich über die Zune Anwendung Anwendungen installieren. Die Synchronisation mit dem PC lässt sich auch über WLAN bewerkstelligen, dazu wird in der Zune-Software festgelegt, dass man sich im „Heimnetzwerk“ befindet. Zur Erkennung des Heimnetzes vergleicht das Windows Phone die MAC-Adresse des Routers bzw. des DHCP-Servers. Die Synchronisation über WLAN startet nur, wenn das Handy mindestens zehn Minuten am Netzladegerät hängt, womit es sich hierbei nur bedingt um eine kabellose Synchronisation handelt.

Die Installation der Zune-Software benötigt Administrator-Rechte, kann also vom Benutzer in Firmenumgebungen, wo der Benutzer keine lokalen Administrationsrechte hat, nicht durchgeführt werden.

3.8 Länderspezifische Unterschiede

Die Windows Live ID ist unabhängig von der Domain der verwendeten E-Mail-Adresse an ein bestimmtes Land gebunden. Dieses wird durch eines der dahinterliegenden Systeme festgelegt. Davon gibt es mehrere wie etwa Zune oder Xbox, was historische Gründe hat. Die Festlegung auf ein Land hat massive Auswirkungen auf die Verfügbarkeit der Services. So stehen für österreichische Live IDs keinerlei musikbezogene Dienste zur Verfügung, weil die entsprechenden Rechteinhaber und Microsoft keine Vereinbarung getroffen haben. Eine deutsche ID würde sofort den Zune Musik Marketplace zugänglich machen und bei einer französischen ID hätte man gar die Möglichkeit eine Flatrate („Zune Pass“) zu erstehen.

Eine durch Zune oder Xbox getroffene Ländereinstellung lässt sich nachträglich nicht mehr ändern, auch durch den Support nicht. Das betrifft vor allem Personen, die von einem Land in ein anderes ziehen, z.B. von Österreich nach Deutschland, oder von Kanada in die Vereinigten Staaten. Diese können die Services nicht mehr nutzen, z.B. keine Applikationen mehr kaufen, wenn die Rechnungsadresse der Kreditkarte auf ein anderes Land zeigt. Hier ist die einzige Lösung jene, dass man einen neuen Account anlegt. Der Verlust sämtlicher „Freunde", Erfolge auf Xbox Live und sämtlicher lizensierter Software muss in Kauf genommen werden.

Eine vollständige Matrix, welche Services und Funktionen in welchem Land verfügbar sind, ist von Microsoft nicht zu bekommen, am nächsten kommt dieser Anforderung diese Darstellung [36]. Vor allem nicht berücksichtigt werden hier Funktionen, die problemlos funktionieren würden, wenn man sie denn nur seitens Microsoft aktivieren würde bzw. die funktionieren, wenn der Benutzer in den *Einstellungen* die *Browser- und Suchsprache* umstellt. Populärstes Beispiel für diesen Anwendungsfall ist die Routenplanung in BING Maps („Karten"). Diese Funktion ist in Österreich nicht verfügbar, stellt man in den Optionen jedoch die *Browser- und Suchsprache* auf „Deutsch (Deutschland)" dann steht diese Funktion auch in Österreich zur Verfügung. Eine vollständigere, wenngleich nicht offizielle Matrix, liefert [37].

3.9 Exchange, SharePoint und Office 365

Exchange ist der Mail- und Groupwareserver von Microsoft[5]. Man kann auch ohne einen Exchange Server mit Windows Phone die Desktopanwendung Outlook synchronisieren, beispielsweise in dem man einen Windows Live Account nimmt und Outlook mittels des „Outlook Connector" mit Windows Live abgleicht (und von dort dann mit Windows Phone). Hierbei gibt es jedoch einige Einschränkungen so werden beispielsweise bei Kontakten keine Fotos synchronisiert oder bezüglich der Aufgaben aus Outlook: diese verbleiben ebendort. Mit Exchange Server hat man diese Probleme nicht und erhält als Firma außerdem einige sicherheitsrelevante Verwaltungsfunktionen zusätzlich, wie etwa Remote Wipe.

Microsoft SharePoint Server[6] ist eine Plattform zur Zusammenarbeit, vorrangig jene von Mitarbeitern im Intranet. Über Portale und Teamseiten werden Informationen verwaltet, Dokumente mit Versionierung abgelegt oder Workflows angestoßen. Exchange und SharePoint kann man entweder „On Premise", also Vor-Ort, installieren und betreiben oder in einer von Microsoft betriebenen Variante als Office 365[7] buchen, einem so genannten Cloud-Service. Für Überlegungen bezüglich Sicherheit On Premise im Vergleich mit einem Cloud-Service siehe Kapitel 6.4, für weitere sicherheitsrelevante Funktionen und Bereiche dieser Server im Zusammenhang mit Windows Phone siehe Kapitel 4.15.

[5] Mehr Information http://www.microsoft.com/exchange
[6] Mehr Information siehe http://sharepoint.microsoft.com/
[7] Mehr Information siehe http://www.microsoft.com/office365

4 Sicherheitsarchitektur und sicherheitsrelevante Bereiche

Welche Bereiche sind für die Bewertung des Themas Sicherheit bei Windows Phone von Interesse? Dieses Kapitel untersucht die Sicherheitsarchitektur von Windows Phone.

4.1 SIM-PIN und Bildschirmsperre

Bevor das Telefon in Betrieb gehen kann, muss der Benutzer bis zu zwei Personal Identification Number- (PIN-)Codes eingeben. Der erste ist für das Subscriber Identity Module (SIM-Karte), mit dem das Telefon am Netzbetreiber angemeldet wird. Um ihn auszuschalten, kann man in *Einstellungen, Anwendungen, Telefon* diesen der Option bei *SIM-PIN Abfrage* deaktivieren.

Der zweite PIN-Code betrifft die Bildschirmsperre. Wird das Telefon über einen konfigurierbaren Zeitpunkt (30 Sekunden, eine Minute, drei Minuten, 5 Minuten, „Nie“) nicht benutzt, schaltet sich der Bildschirm aus. Zur Reaktivierung muss die „Einschalten“-Taste gedrückt werden. Die darauf sichtbare Bildschirmsperre zeigt Datum und Uhrzeit, Anzahl erhaltener E-Mail-, Chat-, SMS-Nachrichten und versäumte Anrufe sowie den nächsten Termin aus den aktiven Kalendern. Zur Aufhebung der Sperre muss das Bild nach oben gewischt werden. So unter *Einstellungen, System, Sperre & Hintergrund* eine Kennwort-Sperre aktiviert wurde, muss jetzt das Kennwort bzw. der PIN eingegeben werden.

Sowohl bei gesetzter SIM-PIN, als auch bei aktiver Bildschirmsperre ist auch ohne Kenntnis des korrekten Codes das Absetzen eines Notrufs möglich, die entsprechenden Nummern wie 112 oder 911 können gewählt werden.

Der SIM-PIN ließe sich immer ausschalten, jener von der Bildschirmsperre nur dann, wenn eine Richtlinie (über EAS, siehe 4.4) nichts Anderweitiges festlegt. Je nach Einstellung kann das Gerät bei mehrmaliger Eingabe des inkorrekten PINs auch gelöscht werden, siehe Remote Wipe (siehe Kapitel 4.6).

4.2 Multitasking

Der Kernel von Windows Phone basiert auf Windows CE und ist voll Multitasking-fähig. So kann problemlos eine E-Mail geöffnet werden und gleichzeitig Musik gehört werden, oder es kann während eines Telefonats auf den Kalender zugegriffen werden. Diese Art des Multitaskings können allerdings ausschließlich Anwendungen von Microsoft verwenden (siehe auch 4.11). Anwendungen von Drittherstellern müssen sich hier einigen Restriktionen unterwerfen. Microsoft liefert als Begründung für diese Restriktionen den Trade-Off zwischen dem Benutzererlebnis und der Systemgesundheit [38], siehe Abbildung 2.

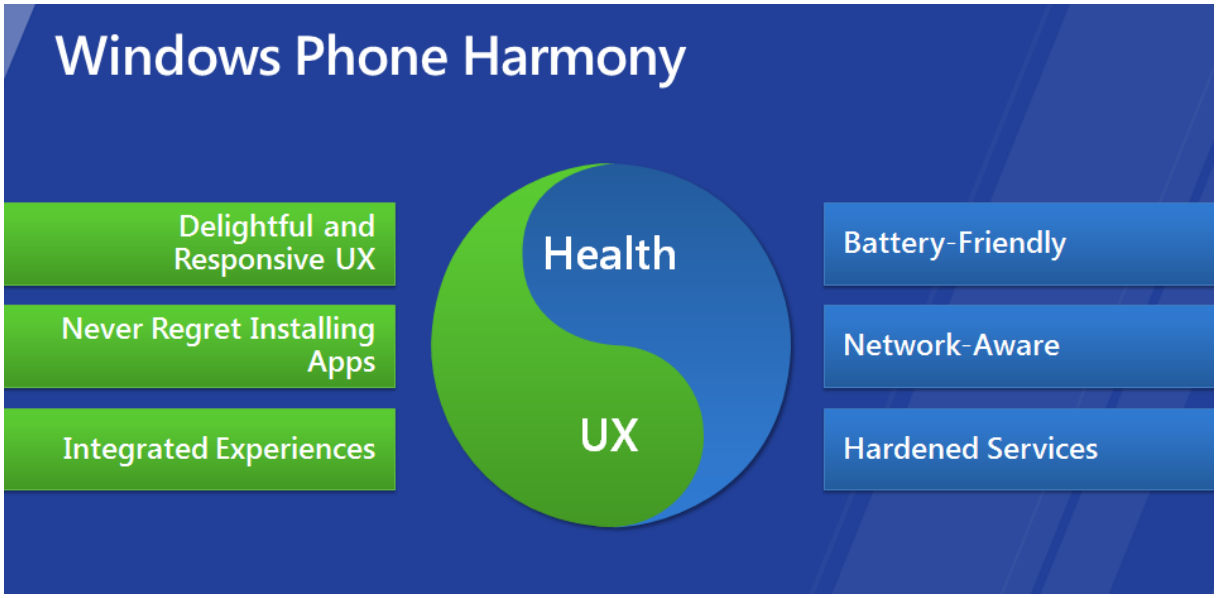


Abbildung 2 - Windows Phone Trade Off, Quelle: [38]

Deshalb steht Entwicklern kein volles Multitasking zur Verfügung, sondern ein Modell mit Hintergrund-Agents, die periodisch laufen können, aber nur eine bestimmte Anzahl von Ressourcen in Anspruch nehmen dürfen, z.B. maximale Laufzeit von 25 Sekunden haben.

Im Marketing wird auch der schnelle Anwendungswechsel als Multitasking dargestellt, die österreichische Pressemeldung [39] meint: „Multitasking: Einfach zwischen aktiven Apps wechseln. Dadurch wird sowohl Batterielebensdauer als auch Performance optimiert“. Das wäre aus technischer Sicht zu diskutieren, wenngleich es sich für den Benutzer so anfühlen mag.

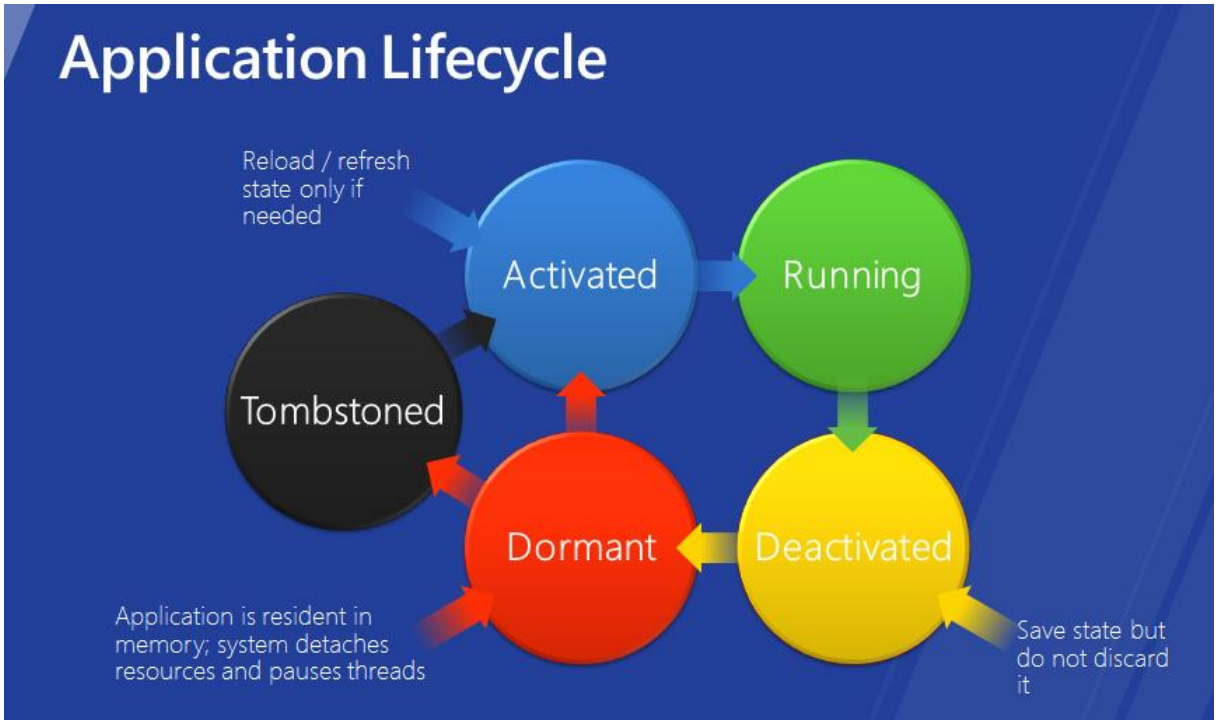


Abbildung 3 - Lebenszyklus von Applikationen, Quelle: [38]

Beim „Fast Application Switching“ wird die Anwendung schnell wieder aus dem „Ruhezustand“ („Dormant state“) geholt und steht so „beinahe augenblicklich“ [40] wieder zur Verfügung, statt neu initialisiert zu werden. Zu keinem Zeitpunkt ist die Anwendung jedoch parallel gelaufen.

4.3 Netzwerksicherheit und Zertifikate

Alle Netzwerkimplementierungen kommen von Microsoft. Die Hardwarehersteller, die prinzipiell die Treiber liefern, „mussten hierfür den Code von Microsoft übernehmen“ [41], der so programmiert wurde, wie es Microsofts Prinzipien, sicheren Code zu schreiben, entspricht [42]. WLAN auf Windows Phone unterstützt die Wi-Fi Protected Access (WPA) und Wi-Fi Protected Access II (WPA2) Protokolle jeweils in den Modi Personal und Enterprise.

Sämtliche Synchronisationen zwischen Windows Phone und Serverdiensten wie Exchange, SharePoint oder SkyDrive laufen über eine Secure Socket Layer-(SSL-)Verbindung. Je nach Server beträgt die Schlüssellänge 128 oder 256 Bit. Windows Phone erlaubt keine Synchronisation mit dem lokalen PC für etwas anderes außer Bilder, Videos und Musik. Windows Phone hat dabei eine Reihe von SSL Root Zertifikaten [43] mit an Bord, die Synchronisation klappt nur, wenn dem jeweiligen Zertifikat der Gegenstelle vertraut wird. Eigene Zertifikate, die nicht ein öffentliches Zertifikat von einem vertrauenswürdigen Herausgeber („Trusted CA“) sind, können zwar verwendet werden, müssen aber manuell dem Zertifikatsspeicher hinzugefügt werden. Für das Phone gibt es zwei Wege: entweder man stellt das cer-File (das Zertifikat) auf einen Webspace bzw. SkyDrive, und klickt es an – „oder man schickt es sich selber per E-Mail (auf einen Account, der kein Zertifikat braucht)“ [44].

Über die WLAN-Verbindung wird eine Authentifizierung über NTLM unterstützt, dies kann in weitere Folge auch dazu genutzt werden damit sich Benutzer „über WS-Trust und SOPA gegenüber Active Directory über eine SSL-Verbindung in einer App anmelden“ [41].

4.4 Exchange und Exchange Policies

Wird Windows Phone mit einem Exchange Server verbunden, kommt zur Synchronisation von E-Mails, Kalender, Aufgaben und Kontakten das Exchange ActiveSync Protokoll (EAS) zum Einsatz. EAS ist ein Protokoll, das „optimiert ist für den Einsatz in Netzwerken mit geringer Bandbreite und hoher Latenz“ [45]. Clientseitig unterstützt Windows Phone 7 die EAS Version 14.0 und mit „Windows Phone 7.5 wird EAS 14.1 unterstützt“ [41].

Je höher die verwendete Exchange-Version ist, desto mehr Funktionen stehen zur Verfügung, die Mindestanforderung besteht in Exchange Server 2003 Service Pack 2 [46], unterstützt werden je nach Version unterschiedliche Funktionen, siehe Tabelle 1.

Tabelle 1 - Exchangefunktionen, Quelle: Eigene Darstellung nach [46]

Exchange ActiveSync	Exchange Server 2003	Exchange Server 2007	Exchange Server 2010
Direct Push	X	X	X
E-Mail Synchronisation	X	X	X
Kalender Synchronisation	X	X	X
Kontakte Synchronisation	X	X	X
Remote Wipe	X	X	X
Synchronisation mehrere Ordner	X	X	X
128-bit SSL verschlüsselte Verbindung	X	X	X
Benutzerinitiierter Remote Wipe		X	X
HTML E-Mail		X	X
Nachschlagen in der GAL		X	X
Follow-up Fahnen		X	X
Teilnehmerinformation (Besprechungen)		X	X
Autodiscover		X	X
Bandbreitenreduktion		X	X
Beantwortungsstatus			X
Zwischenspeicher für Namen			X
Block/Allow/Quarantine List			X
Information Rights Management			X
256-bit SSL verschlüsselte Verbindung			X

Außerdem können über EAS Richtlinien bezüglich Sicherheit gesetzt werden. Ist das Phone mit mehr als einem Exchange verbunden, so gelten die jeweils strengsten Richtlinien. Insgesamt werden zurzeit neun Richtlinien unterstützt:

- [PasswordRequired] macht es erforderlich, dass der Benutzer die Bildschirmsperre aktiv hat und einen PIN-Code zum Entsperren setzen muss,

bevor das Phone E-Mail, Kalender, Aufgaben oder Kontakte synchronisieren kann. Diese Einstellung graut auch das Optionsfeld in den Phone Einstellungen bezüglich der Deaktivierung der Bildschirmsperre aus.

- [ComplexPasswordRequired] erfordert, dass der Benutzer ein komplexes (alphanumerisches) Passwort für die Bildschirmsperre setzt.
- [PasswordComplexity] kann verwendet werden, um den Grad der Passwortkomplexität festzulegen.
- [PasswordExpiration] setzt die Zeitspanne, nach deren Ablauf ein Passwort erneuert warden muss.
- [PasswordHistory] verhindert, dass der Benutzer wiederholt dasselbe Passwort setzt.
- [AllowSimplePassword] kann verwendet werden, um einfache Passwörter wie 1111 zu erlauben oder zu untersagen.
- [MinPasswordLength] legt die minimale Passwortlänge fest.
- [IdleTimeoutFrequencyType] definiert die Zeitspanne, ab wann sich die Bildschirmsperre automatisch aktiviert und das Telefon sperrt.
- [DeviceWipeThreshold] legt die Anzahl an erlaubten Fehlversuchen bei der PIN-Eingabe fest. Wird die festgelegte Anzahl überschritten, löscht das Phone sämtliche Daten und Anwendungen und setzt sich in den Fabrikszustand zurück.

Auch die EAS Richtlinien sind abhängig von der Serverversion, siehe Tabelle 2.

Tabelle 2 - EAS Richtlinien-Unterstützung, Quelle: Eigene Darstellung nach [46]

EAS Funktion	Exchange Server 2003	Exchange Server 2007	Exchange Server 2010
PasswordRequired	X	X	X
ComplexPasswordRequired		X	X
PasswordComplexity		X	X
PasswordExpiration		X	X
PasswordHistory		X	X
AllowSimplePassword		X	X
MinPasswordLength		X	X
IdleTimeoutFrequencyType		X	X
DeviceWipeThreshold		X	X

Eine Reihe weiterer EAS Richtlinien geben einen festen Rückgabewert zurück und sind nicht weiter konfigurierbar, siehe Tabelle 3.

Tabelle 3 - EAS Rückgabewerte, Quelle: Eigene Darstellung nach [46]

EAS Richtlinie	Fester Rückgabewert	Anmerkung/Begründung für den Wert
DisableRemovableStorage	TRUE	Durch den Benutzer austauschbarer Speicher wird von Windows Phone nicht unterstützt.

DisableIrDA	TRUE	Windows Phone unterstützt kein Infrarot.
DisableDesktopSync	TRUE	Die Exchange-Synchronisation läuft bei Windows Phone ausschließlich „over the air“, eine lokale Synchronisation ist nicht vorgesehen.
BlockRemoteDesktop	TRUE	Windows Phone unterstützt keinen Remote Desktop.
MobileEncryptionRemovable	FALSE	Verschlüsselung bei Windows Phone nicht verfügbar.
MobileEncryptionEnabled	FALSE	Verschlüsselung bei Windows Phone nicht verfügbar.
EnableDeviceEncryption	FALSE	Verschlüsselung bei Windows Phone nicht verfügbar.
AllowUnsignedApplications	FALSE	Alle Apps müssen über den Marketplace installiert werden.
UnsignedCABAccessRole	FALSE	Installer-Format ist XAP.
UnapprovedApplicationList	FALSE	Wird von Windows Phone nicht unterstützt, Apps müssen über den Marketplace installiert werden.
ApprovedApplicationList	FALSE	Wird von Windows Phone nicht unterstützt, Apps müssen über den Marketplace installiert werden.
AllowHTMLEmail	FALSE	Ungeachtet des fixen Rückgabewerts zeigt Windows Phone immer HTML-Nachrichten an.
SyncWhenRoaming	FALSE	Einstellung wird nicht unterstützt, Verhalten kann durch den Benutzer geändert werden.
Alle anderen Richtlinien	FALSE	

4.5 Wiederauffinden nach Verlust des Phones

Sollte das Handy nicht auffindbar sein, so stehen über *www.windowsphone.com* verschiedene Optionen zur Verfügung um das Gerät wieder zu erhalten. Diese Optionen bedingen allerdings, dass der Benutzer eine Windows Live ID eingerichtet hat, die GPS-Funktion eingeschaltet hat und unter Einstellungen muss die Funktion *Mein Handy finden* aktiviert sein. Für genauere und aktuellere Ergebnisse sollte ebendort die Option *Schnellere Ergebnisse erhalten* eingeschalten sein, dann meldet das Phone die Position in kürzeren Abstanden. Diese Optionen stehen zur Verfügung:

- Ortung und Anzeige der Position: Hier wird das Phone auf einer BING Maps-Karte angezeigt. Bei Klick auf *Aktualisierung* nimmt der Service direkt Kontakt mit dem Phone auf und versucht eine aktuellere Bestimmung des Standortes. Kann das Telefon nicht ausgemacht werden, kann man sich eine E-Mail zusenden lassen, wenn es durch den Service „wieder entdeckt“ wird.

- Per Web läuten lassen: Unabhängig von der eingestellten Lautstärke, auch wenn das Phone nur auf Vibrieren eingestellt ist, ertönt ein Klingelton. Das kann nützlich sein, wenn das Phone zwar in der unmittelbaren Nähe vermutet wird, jedoch nicht auffindbar erscheint, etwa, weil es in einer Jackentasche steckt und auf „stumm“ geschaltet ist.
- Dem Finder eine Nachricht hinterlassen: die Nachricht, die man über das Webinterface eingibt, wird auf dem Display angezeigt, dies kann dienlich sein, wenn ein ehrlicher Finder das Phone retournieren möchte.
- Remote Wipe, dazu mehr in Kapitel 4.6.

Weitere Anmerkungen:

- Alle Optionen bedingen, dass das Handy eingeschaltet und beim Netzbetreiber angemeldet ist, sowie Empfang hat.
- Der Benutzer muss bei aktiver Funktion „Mein Handy finden“ mit erhöhtem Stromverbrauch rechnen.
- Lediglich der Remote Wipe kann durch den Exchange-Administrator ebenso durchgeführt werden, die anderen Aktionen sind rein dem Benutzer mit der Windows Live ID vorbehalten.

4.6 Remote Wipe

Insgesamt stehen vier Wege zur Fernlöschung („Remote Wipe“) zur Verfügung. Alle haben gemeinsam, dass die Einstellungen, Benutzerdaten und Applikationen auf den Werkszustand zurückgesetzt werden.

- Remote Wipe durch den Benutzer über Windows Live: über die Administrationsoberfläche auf *www.windowsphone.com* kann der Benutzer sein Gerät zurücksetzen.
- Remote Wipe durch den Benutzer über Exchange: über die Weboberfläche von Exchange, der so genannten Outlook Web App (früher Outlook Web Access) kann der Benutzer ebenso die Fernlöschung anstoßen.
- Remote Wipe durch den Administrator: das Absetzen des Löschbefehls ist auch durch den Administrator des Exchange-Servers über Exchange Server Management Console möglich.
- PIN Fehleingabe: Durch setzen einer Exchange ActiveSync-Richtlinie kann konfiguriert werden, wie oft ein PIN-Code bei der Bildschirmsperre falsch eingegeben werden kann, bevor das Gerät zurückgesetzt wird. Ist eine solche Richtlinie in Kraft, so kann das Gerät also auch einfach durch mehrfache Fehleingabe des PINs zurückgesetzt werden. Diese Art der Fernlöschung, wo die Richtlinie remote konfiguriert wird, ist die einzige Remote Wipe-Methode, die auch ohne Empfang und Internetkonnektivität funktioniert.

4.7 Information Rights Management

Um sensible Informationen in E-Mails oder Dokumenten zu schützen können diese über ein digitales Rechtemanagement geschützt werden. Der Exchange Server nutzt dabei die Active Directory Rights Management Services (AD RMS) des Windows Server 2008 (oder neuer). Diese Technologie, bei Exchange oder Office auch Information Rights Management (IRM) genannt, nutzt „extensible rights markup language“ (XrML)-Zertifikate [47] und ist an die Benutzerverwaltung von Active Directory gebunden. Damit lassen sich Rechte E-Mails oder Dokumenten einschränken, z.B. wer darf bearbeiten, weiterleiten, lesen oder drucken. Auch ein Zeitablauf, ab wann ein Dokument nicht mehr geöffnet werden kann lässt sich definieren. Diese Rechte können manuell durch den Benutzer via Outlook, Outlook Web Access oder die entsprechende Office-Anwendung vergeben werden. Auch eine die regelbasierte Vergabe von Rechten am Hub Transport Server (Exchange) kann genutzt werden. „Man kann die Transportschutzregeln dazu nutzen, Richtlinien zu implementieren, die die Nachricht inspizieren und sensible E-Mails verschlüsseln und mit dem Rechtemanagement den Zugriff regeln” [48].

Exchange 2010 inkludiert „keine eingebaute Lösung um geschützte Dokumente an externe Empfänger zu schicken“ [47], also an Benutzer, die weder Mitglied in der Active Directory Domain noch in einer föderierten Domain Mitglied sind. Um an einen solchen externen Empfänger eine verschlüsselte Nachricht zu schicken, müsste die Organisationen bzw. deren Active Directory Forests über die Active Directory Federation Services eine Vertrauensstellung („Trust“) bilden, vgl. dazu [47]. Eine weitere Möglichkeit bestünde darin, einen Trust zu Windows Live aufzusetzen. Damit könnte der Anwender mit seinem Firmenkonto verschlüsselte Mails an Windows Live IDs schicken. Da im geschäftlichen Gebrauch die Windows Live ID generell nicht die Firmen-E-Mail-Adresse ist, ist dieser Weg wenig praktikabel, die Nutzung ist daher hauptsächlich auf die interne Kommunikation beschränkt.

Windows Phone Benutzer können ab Windows Phone 7.5 an IRM-geschützten Konversationen teilnehmen und geschützte Office-Dokumente öffnen, unabhängig davon, ob diese per Mail, über SharePoint, Skydrive oder über einen anderen Weg auf das Telefon kommen. Geschützte Mails werden über EAS übertragen. Bei der Nutzung von IRM über EAS „entschlüsselt der Client Access Server die IRM-geschützte Nachricht und liefert diese dann an das Endgerät“ [49], zwar ebenso über eine gesicherte Verbindung, darüber allerdings ohne die IRM-Verschlüsselung. Den weiteren Schutz der Nachricht und die Einhaltung der Richtlinien übernimmt dann die lokale Client Anwendung, in diesem Fall die Mailapplikation auf Windows Phone. Anders sieht das bei verschlüsselten Dateianhängen an die Mail aus. Diese Anhänge werden vom Mailprogramm an die Anwendung z.B. wie etwa Word übergeben und müssen von dieser entschlüsselt werden. Aus diesem Grund muss der entsprechende AD RMS von außerhalb des Netzwerkes erreichbar sein, damit sich der Benutzer mit seinem Active Directory Konto gegenüber dem Server authentifizieren und die Client Anwendung den Dateianhang öffnen kann.

4.8 Device Management

Unter der Verwaltung von mobilen Systemen versteht Microsoft vorrangig das eigene Produkt in Form des noch nicht veröffentlichten System Center Configuration Manger 2012 (SCCM). Mit diesem Server lassen sich sämtliche Endgeräte, vom PC, über Server bis hin zu mobilen Clients verwalten. Firmen mit System Center Configuration Manager 2007 können Athena von Odyssey Software verwenden. Eine weitere Möglichkeit liefert die Firma Maas360. Zu beachten ist allerdings, dass all diese Management Software derzeit einen eng umfassten Funktionsumfang hat, der nicht mit jenem vergleichbar ist, den die Software mit Windows Mobile erreicht hat. Mitunter wird Windows Mobile 6.5 mit Windows Phone 7 gleichgestellt, was aber aus technischer Sicht nicht zutreffend ist. Das mobile Management ist neben der einfachen Sichtbarkeit der Geräte („Discoverability“) auf jene Richtlinien beschränkt, die durch die EAS-Implementierung auf Windows Phone vorgegeben sind, siehe Kapitel 4.4. In keiner Lösung ist die Verwaltung von Zertifikaten, Applikationen oder Eigenschaften für Windows Phone 7 möglich. Jedoch meint [50] „Eine solide Strategie für mobiles Device Management zu haben ist essentiell“, es dürfte daher ungeachtet der beschränkten Fähigkeiten wichtig sein, sich mit diesem Thema zu beschäftigen.

4.9 Sicherheit im Browser

Der Internet Explorer auf Windows Phone 7.5 basiert auf der Desktopversion von Internet Explorer 9 und übernimmt von dort u.a. dessen Rendering-Engine. Im Gegensatz zur Desktopversion „unterstützt der Browser auf Windows Phone keine Add-Ins“ [51]. Deswegen, und auch aufgrund des in Kapitel 4.11 beschrieben Sicherheitsmodells gibt es auch kein Adobe Flash für Windows Phone, selbst Microsoft Silverlight läuft nicht innerhalb des Browsers.

In den Standardeinstellungen nimmt der Browser Cookies an und sendet die Eingabe in der Adresszeile an die Standardsuchmaschine BING (bei manchen Mobile Operators: Google) um Vorschläge für die Autovervollständigung der Benutzereingabe zu empfangen. Der Benutzer kann den Verlauf, die Cookies und gespeicherte Passwörter löschen, allerdings nur alles auf einmal und nicht selektiv.

4.10 Bluetooth

Es gibt viele verschiedene so genannten Bluetooth-Profile. Das sind Spezifikationen, die festlegen, wie Geräte miteinander kommunizieren. Windows Phone 7 unterstützt gemäß [52] diese:

- Advanced Audio Distribution Profile (A2DP 1.3)
- Audio/Video Remote Control Profile (AVRCP 1.0)
- Hands Free Profile (HFP 1.5)
- Headset Profile (HSP 1.1)
- Phone Book Access Profile (PBAP 1.0)

Damit kann man Windows Phone nicht nur mit einer Bluetooth-Freisprecheinrichtung koppeln, sondern das Phone auch zur Fernsteuerung von Audio-/Video-Geräten einsetzen

oder Audio-Streaming vom Gerät über Bluetooth auf eine HiFi-Anlage durchführen. Sicherheitsrelevante Profile z.B. zum Aufbau einer Internetverbindung oder zum Datentransfer fehlen völlig.

4.11 Kammern und Sandkästen - Applikationssicherheit

Windows Phone setzt auf Isolation der Anwendungen, die nur als „managed code" Anwendungen vorliegen (C# oder VB.net). Der managed code soll laut [41] „gegen die Fehler wie Buffer Overflows oder Speicherfehlern schützen, wie sie bei C oder C++ Entwicklern passieren". Die Apps haben generell die geringsten möglichen Rechte. Es gibt laut [53] vier so genannte Kammern:

- Trusted Computing Base (TCB): hat die höchsten Rechte und erlaubt unbeschränkten Zugang zu allen Ressourcen. Beispiel: Kernel und Kernel Treiber.
- Elevated Rights Chamber (ERC): weniger Rechte als TCB, verwendet für Services und User-Mode Treiber, die von anderen Apps genutzt werden sollen.
- Standard Rights Chamber (SRC): Standardanwendungen, die vorinstalliert sind, aber keinen geräteweiten Zugriff brauchen, z.B. Microsoft Office.
- Least Privileged Chamber (LPC): der Normalfall für Applikationen die über den Marketplace vertrieben werden, haben die wenigsten Rechte und brauchen spezielle Genehmigungen, wenn sie bestimmte Fähigkeiten des Phones nutzen wollen (siehe Kapitel 4.12)

Jede LPC-Anwendung läuft in einer eigenen isolierten Kammer bzw. Sandbox, ausschließlich mit dem Zugriff auf den eigenen Speicherbereich („Isolated Storage") und auf jene APIs, die Microsoft den Entwicklern zur Verfügung stellt. Einen direkten Zugriff auf die Hardware haben die Applikationen nicht und auch die Kommunikation zwischen den Anwendungen kann nur über die Netzwerkverbindung und einem Cloudservice passieren, nicht jedoch zwischen zwei Apps. Einzig der Zugriff auf die gemeinsame Medienbibliothek ist über die Capabilities möglich, d.h. es können zwischen den Applikationen z.B. Bilder getauscht werden, in dem der Benutzer bzw. die App ein Bild speichert und in der nächsten App dieses Bild lädt.

4.12 Rechte für Applikationen

Bevor eine Anwendung von sich aus auf bestimmte Funktionen von Windows Phone zugreifen darf, muss der Software-Entwickler dieser Anwendung erst die notwendigen Rechte einräumen. Dies soll vor allem der Transparenz und der Sicherheit dienen. Im Marketplace, sowohl auf dem Phone selbst, als auch in der Zune-Software wird dann angeführt, welche dieser in Tabelle 4 aufgeführten Eigenschaften benötigt werden.

Tabelle 4 - Liste von Eigenschaften bzw. Capabilities, Quelle: Eigene Darstellung

Englische Bezeichnung	Deutsche Bezeichnung/Beschreibung
data connection	Datenverbindungen: Anwendung nutzt Datenverbindungen
media library	Medienbibliothek: Zugriff auf die Medienbibliothek, wie etwa die Bilder und Musik des Benutzers
web browser	Webbrowser Internet Explorer wird innerhalb der Anwendung benutzt

phone calls	Anwendung kann die Telefonieanwendung aufrufen
phone identity	Identität des Handys: Eindeutige Geräte-ID, Hersteller und Modellnummer, aber auch Eigenschaften wie „Wie viel Speicher ist verfügbar“.
owner identity	Identität des Eigentümers: Die anonymisierte, aber eindeutige Live ID. Wer diese ID hat, kann zwar nicht auf den tatsächlichen Benutzer rückschließen, unterschiedliche Benutzer aber eindeutig auseinanderhalten.
sensors	Sensoren: Gravitations-, Annäherungssensor und Kompass können genutzt werden.
microphone	Mikrofon: Anwendung kann das Mikrofon nutzen, es muss dazu verpflichtend eine Anzeige am Bildschirm erscheinen.
XBOX Live	Anwendung nutzt die XBOX Live Daten

Für manche Fähigkeiten muss eine Applikation vorab beim Benutzer anfragen. Ohne Bestätigung kann die Anwendung diese in Tabelle 5 beschriebenen Services nicht nutzen.

Tabelle 5 - Besondere Eigenschaften, Quelle: Eigene Darstellung

Englische Bezeichnung	Deutsche Bezeichnung/Beschreibung
location services	Speicherortdienste: Anwendung erhält Zugriff auf den aktuellen Standort des Benutzers
push notifications	Push-Benachrichtigungen: Es können Popups oder aktualisierte Live-Kacheln empfangen werden.
RunsUnderLock	Anwendung kann trotz Bildschirmsperre weiterhin ausgeführt werden

Microsoft prüft alle Einsendungen in den Marketplace auf die Einhaltung dieser auch Capabilities genannten Applikations-Eigenschaften. Für den Benutzer soll dies zusätzliche Sicherheit bedeuten, wenn er vorab sehen kann, dass eine Anwendung etwas auf die Standortdaten zugreift. Die Capabilities müssen deshalb im Applikationsmanifest festgehalten werden, der diesbezügliche Inhalt dieser XML-Datei namens *WMAppManifest.xml* könnte daher so aussehen:

```
<Capabilities>
	<Capability Name="ID_CAP_NETWORKING" />
	<Capability Name="ID_CAP_LOCATION" />
	<Capability Name="ID_CAP_MICROPHONE" />
	<Capability Name="ID_CAP_MEDIALIB" />
	<Capability Name="ID_CAP_PHONEDIALER" />
	<Capability Name="ID_CAP_WEBBROWSERCOMPONENT" />
</Capabilities>
```

In diesem Beispiel soll eine App per Mikrofon eine Aufnahme machen und in die Medienbibliothek abspeichern. Dazu braucht die Applikation die Zugriff auf verschiedene Dienste, etwa auf das Mikrofon selbst(„MICROPHONE“), die Bibliothek („MEDIALIB“) zum Speichern. Um schließlich den Support für die App zu erreichen hat der Entwickler vorgesehen, direkt aus der App heraus einen Telefonanruf zu initiieren

(„PHONEDIALER“). Außerdem inkludiert er ein Online-Handbuch direkt in die App, in dem er das Browsercontrol („WEBBROWSERCOMPONENT“) verwendet.

Alle verwendeten Capabilities werden zum Zeitpunkt der Applikationsinstallation festgelegt, damit sollen „Angriffe zur Erlangung höherer Rechte unterbunden werden“ [41]. Zusätzliche Sicherheitsmaßnahmen inkludieren, dass beispielsweise auch bei erlaubter PHONEDIALER-Eigenschaft, eine Anwendung niemals selbst wählen kann, sondern lediglich die Nummer an die Telefonkomponente weiterreichen kann, wählen muss der Benutzer immer selbst.

Neben den offiziellen und dokumentieren Capabilities, vgl. [54], gibt es auch noch eine Reihe weiterer, allerdings nicht dokumentierter, Eigenschaften, vgl. [55], bei deren Verwendung allerdings die Notwendige Zertifizierung der App fehlschlägt. Diese können somit nur per Sideloading auf das Gerät gebracht werden, siehe Kapitel 5.1.

4.13 Verschlüsselter Speicher

Microsoft zu Folge ist das Fehlen von durch den Benutzer austauschbaren Speichermedien, etwa über Secure Digital-(SD-)Karten eine Sicherheitsfunktion. „Um Sicherheitsrisiken abzuschwächen, verhindert Windows Phone den Datentransfer vom Gerät, in dem es Wechselspeicher nicht unterstützt“ [56]. Alle Geräte haben zwar intern eine SD-Karte, diese ist jedoch nicht direkt zugänglich. Teilweise könnte der Speicher durch das Öffnen des Gerätes unter Verlust der Gewährleistung ausgetauscht werden, das ist beispielweise beim HTC HD7 der Fall. Bei anderen Geräten wie dem Samsung Omnia 7 ist der Aufwand schon um einiges höher, hier ist der Speicher direkt aufgelötet. Die einzige Hardware, die einen weiteren zugänglichen SD-Kartenslot hatte, war das in den USA vertriebene Samsung Focus.

Windows Phone fasst sämtlichen Speicher, der verfügbar ist zusammen, ähnlich einem Software-RAID (Redundant Array of Independent Disks). Dieser zusammengefasste Speicher steht dem System zur Verfügung. Jede Änderung am Speicher z.B. Austauschen der SD-Karte oder hinzufügen einer weiteren Karte zum Gerät, hat eine Reinitialisierung des Systems zur Folge, also einer kompletten Neuinstallation, wo das Betriebssystem aus dem ROM heraus neu aufgespielt wird. Windows Phone nutzt dabei die Verschlüsselung der SD-Karte und verschlüsselt den Speicher beim Initialisieren der Karte.

Die verwendete Verschlüsselung ist dabei Teil der SD-Karten-Spezifikation. „Der Passwortschutz ermöglicht dem Hostgerät die Karte zu verschlüsseln und gleichzeitig ein Passwort zu erhalten, das die Karte entsperrt.“ [57] . Demnach wird mit einem zufälligen 128-Bit Schlüssel die Karte an das Telefon gebunden. Damit ist die Karte an das Gerät gebunden und kann ohne den Schlüssel zu kennen nicht ausgelesen werden.

Microsoft selbst sagt „Das Speichern von vertraulichen Daten im Isolated Storage ist nicht sicher“ [58]. Applikationen können deshalb ihren eigenen Speicher („Isolated

Storage“ siehe auch 4.11) verschlüsseln, eine entsprechende Klasse namens *ProtectData* steht dazu zur Verfügung.

4.14 Updates

Anders als die früher bei Windows Mobile der Fall war, stellt Microsoft die Updates für das Betriebssystem selbst über eine eigene Infrastruktur zur Verfügung vergleichbar mit jener für Windows Desktop Betriebssysteme. Damit einem Endgerät ein Update angeboten wird, müssen die Updates vom Hardwarehersteller für das jeweilige Modell und vom jeweiligen Mobile Operator freigegeben werden. Erst wenn diese Freigabe erfolgt ist, steht das Update bei Windows Phone bereit. Microsoft verteilt allerdings die Updates nicht gleichzeitig an alle Geräte, sondern in Wellen. „Sollte ein Problem auftauchen, so ist es kritisch, dass wir dieses schnell isolieren und lösen können“ [59]. Im Bedarfsfall wird die Verteilung also ausgesetzt.

Je nach Einstellung prüft das Phone regelmäßig das Vorhandensein neuer Updates über die Datenverbindung und zeigt dies über eine Benachrichtigung an, ebenso wir ein Check unternommen, wenn über die Zune Software synchronisiert wird. Der Download des Updates erfolgt dann entweder per WLAN oder – wenn größer als 20 MB – über die Zune Software am PC. Over-the-Air Updates sind derzeit noch nicht möglich, die Zune Software ist daher erforderlich. Vor der Installation zieht die Zune Software noch ein Backup, das Telefon selbst kann während des Updates nicht verwendet werden.

Auch die Updates von Applikationen erfolgen zentralisiert über den Marketplace-Hub, es könne auch mehrere Applikationen auf einmal aktualisiert werden.

4.15 Sicherheit mit SharePoint Server

Um mit dem im Office Hub enthaltenen SharePoint Workspace Client auf Windows Phone auf einen SharePoint zugreifen zu können, muss dieser aus dem Internet erreichbar sein. Sollte das nicht der Fall sein, dann braucht man ein weiteres Microsoft Produkt: „Microsoft Forefront Unified Access Gateway (UAG) ist der einzige VPN Server, der von Microsoft Office Mobile auf Windows Phone 7 unterstützt wird” [60]. In diesem Fall kann in den Optionen bei Windows Phone der UAG Server als VPN-Endpunkt angegeben werden und die Kommunikation zur internen Ressource läuft dann verschlüsselt über diesen UAG Server. Außerdem muss bei SharePoint die NTLM-Authentifizierung aktiviert sein. Bei der Cloud-Lösung Office 365 (siehe auch Kapitel 3.9) ist dies der Fall, Windows Phone kann hier ohne weitere Schritte nur mit Benutzernamen und Passwort für Office 365 bzw. dessen SharePoint konfiguriert werden.

5 Erweiterung des Funktionsumfanges und Umgehung von Sicherheitssperren

In diesem Kapitel geht es darum, den Funktionsumfang von Windows Phone um Dinge zu erweitern, die Microsoft aus unterschiedlichen Gründen so nicht vorgesehen hat. Alle diese Erweiterungen erfordern den physischen Zugriff auf das Telefon.

5.1 Sideloading

Diese Anleitung beschreibt, wie man „Sideloading" betreibt, also eine Windows Phone Software ohne den Marketplace auf das Telefon aufspielt. Das braucht man, wenn man selbst Software entwickelt zum Debuggen, oder aber wenn andere, so genannte Homebrew-Software (siehe 5.5), auf dem Gerät landen soll.

Die dafür notwendigen Schritte:

1. Als Entwickler registrieren
2. Die notwendige Software installieren
3. Das Handy freischalten
4. XAP-Deployment - Die Anwendung auf das Phone überspielen

Um sich als Entwickler offiziell zu registrieren, wird eine Jahresgebühr von 99 EUR fällig, man kann dann Anwendungen in den Marketplace stellen, bekommt Infos, Zugang zu Foren und vieles mehr. Für das reine Entwickeln und Testen von Apps ist keine kostenpflichtige Mitgliedschaft notwendig – diese wird erst gebraucht, wenn man sein Gerät "Developer-unlocken" möchte und auch Geld verdienen will. Mehr Info dazu bei[8].

Für Studenten hat Microsoft über Dreamspark[9] eine kostenlose Bezugsmöglichkeit der Mitgliedschaft vorgesehen. Dreamspark ist ein Programm, das für Studenten teilnehmender Unis bzw. Inhabern eines internationalen Studentenausweises, der International Student Identity Card (ISIC), offensteht und größtenteils aus gratis Softwareangeboten (Visual Studio, Server,…) besteht.

Um im nächsten Schritt das Telefon freizuschalten, braucht man ein Werkzeug aus dem jeweils aktuellen Windows Phone SDK[10]. Eventuell vorhandene Beta- oder RC-Versionen des SDK müssen vorab entfernt werden. Jetzt muss das Phone freigeschaltet werden, das geht mit dem „Windows Phone Developer Registration" Tool, das ebenfalls im SDK enthalten ist. Mit der Eingabe der entsprechenden Entwickler-Live ID wird das Gerät zu dem Account hinzugefügt und ab dann kann man auch „eigene" Software sowie Homebrew-Software auf das Gerät aufspielen.

Eine dritte Möglichkeit, wenn es nur das Ziel ist, dass man Anwendungen „sideloaden" will, besteht darin, das Telefon ohne Mitgliedschaft freizuschalten („Jailbreak"). Ein Werkzeug namens ChevronWP7 [61] konnte das – mittlerweile arbeitet das Team von ChevronWP7 mit Microsoft zusammen und bietet eine Variante an, wo man für 9 US$, per Paypal gezahlt, einen „Unlock-Token" für jeweils ein Gerät erstehen kann.

Die Anwendung im XAP-Format wird dann mit dem Werkzeug Tool „Application Deployment" auf das Gerät überspielt. Damit ist eine Anwendung, die nicht über den Marketplace bezogen wurde, auf dem Gerät gelandet und kann gestartet werden.

[8] Mehr Information dazu unter: http://create.msdn.com
[9] Mehr Information dazu unter: http://www.dreamspark.com
[10] Download unter http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=27570

5.2 Die nächste Sperre: INTEROP Lock

Auch wenn eine Anwendung über Sideloading auf dem Gerät gelandet ist, so unterliegt sie dennoch der Sicherheitsarchitektur von Windows Phone, siehe 4.11. Bei den Windows Phone Versionen vor Version 7.5 Codename „Mango“ war es noch möglich, dass der Entwickler Anwendungen mit nativem Code ausführt. [62] schreibt: „Diese Apps brauchten eine COM-Interop-Brücke um zwischen managed und nativem Code wechseln zu können. Die Apps wurde mit der Capability für Interop ausgestattet: „ID_CAP_INTEROPSERVICES“. Das bedeutet, dass im *WMAppManifest.xml* die Fähigkeit diese COM-Interop-Brücke zu nutzen angefragt wurde.

```
<Capabilities>
      <Capability Name="ID_CAP_INTEROPSERVICES" />
      …
</Capabilities>
```

Mit Windows Phone 7.5 hat Microsoft diese Möglichkeit gesperrt. Anwendung, die diese Capability benötigen, können nicht ausgeführt werden. Allerdings wurde schnell eine Umgehung für diese Sperre gefunden, laut [62] ist ein Registry Wert namens *MaxUnsignedApp* dafür verantwortlich.

In *MaxUnsignedApp* steht als Wert die maximal mögliche Anzahl an unsignierten, nicht über den Marketplace installierten, Anwendungen. Dieser ist je nach Konto unterschiedlich, normale Entwickler, die 99 EUR im Jahr zahlen, haben dort als Wert 10, Studenten über Dreamspark jedoch nur 3. Wie in [62] angeführt ist, schaltet ein Wert von über 300 die Interop-Sperre aus. Alles was zu tun ist, ist also unter „\Software\Microsoft\DeviceReg\Install“ den DWORD Wert für *MaxUnsignedApp* auf „2147483647“ setzen – wenn ein Registry Editor auf dem System ist.

5.3 Registry Editor

Die Registry ist in Windows die zentrale Einstellungsdatenbank in der die Werte in einer Baumstruktur jeweils als Schlüssel und Wert gespeichert sind. Dies ist auch bei Windows Phone der Fall, jedoch liefert für Windows Phone 7 keinen Registry Editor mit. Mittels Homebrew-Software (siehe 5.5) gibt es verschiedene Alternativen, z.B. wird bei [63] eine solche Software vorgestellt. Besitzer von Geräte der Firma LG haben es überhaupt einfach, hier ist ein Editor in der so genannten MFG App, einer Wartungsanwendung, die normalerweise versteckt ist, eingebaut. Diese aktiviert man laut [64] über einen Anruf an die Nummer ##634#. Das anschließend abgefragte Passwort lautet 277634#*# und schon ist man in einer Anwendung, die neben vielen Analysemöglichkeiten auch den Zugriff auf die Registry erlaubt.

5.4 Windows Phone als Massenspeicher

Windows Phone meldet sich am Windows PC beim Anschluss über USB nicht als Massenspeichergerät und kann somit nicht als „USB-Stick” eingesetzt werden. Gemäß Anleitungen wie [65] kann dieser Modus jedoch aktiviert werden, in dem man auf dem Windows PC einige Registry Werte verändert.

Microsoft rät von der Nutzung explizit ab, laut Paul Thurrott [66] hat Microsoft Corporate Vice President Joe Belfiore ausdrücklich davon abgeraten: „Windows Phone ist kein Massenspeicher, es ist ein Zune Gerät. Die Daten auf dem Phone müssen konsistent sein und das System muss in der Lage sein, die Elemente auf dem Speicher zu identifizieren.“ Was nicht der Fall wäre, wenn man über USB Dateien wahllos hinzufügt. Auf der anderen Seite scheint es sowieso nicht praktikabel, da auf jedem PC, an dem das Phone angeschlossen werden soll, vorab die Registry geändert werden muss, dazu sind lokale Administratorrechte notwendig. Außerdem muss die Zune-Software installiert sein. Aus diesen beiden Gründen ist hier das Potential, dass Windows Phone hier als USB-Gerät ein mögliches Datenleck darstellt gering oder zumindest die kleinere Gefahr, verglichen mit jener, die vorhanden ist, wenn der Benutzer Administratorrechte hat.

5.5 Homebrew Software

Unter Homebrew-Software versteht man Applikationen, die nicht über offizielle Kanäle vertrieben werden, oftmals, weil sie den Bestimmungen des jeweiligen Herstellers widersprechen. Das ist beispielsweise bei einem Nintendo Emulator der Fall [67] , der eine Konsole des Herstellers auf Windows Phone emuliert, ohne die dafür notwendigen Lizenzen zu besitzen.

Als Beispiel für die Brauchbarkeit von Homebrew-Software sei hier das Fallbeispiel „Screenshot erstellen“ angeführt. Auf Windows Phone kann durch den Endbenutzer kein Bildschirmfoto erstellt werden. Das kann auch aufgrund der Sicherheitsarchitektur von Windows Phone (siehe 4.11) nicht von einer „normalen“ Applikation durchgeführt werden. Unter [68] wird die Problematik beschrieben. Microsoft hat spezielle Geräte, mit denen das sehr wohl möglich ist. Diese haben eine spezielle Firmware, wo ein „USB Video Out” aktiviert werden kann. Damit werden z.B. die YouTube-Videos von Microsoft[11] erstellt oder die Geräte kommen bei Pressekonferenzen zum Einsatz.

[11] http://www.youtube.com/windowsphone

Abbildung 4 - Video-Out Gerät Asus E600; Quelle: Eigene Darstellung

Geräte, die das können sind zum Beispiel das LG GW910 oder das Asus E600 (siehe Abbildung 4) – beides Geräte, die nie in den Handel gekommen sind. Die Homebrew-App, die hier Abhilfe schafft, nennt sich laut [69] „*Screen Capturer* und nutzt die Hintergrund Aufgaben bzw. Background Tasks (Multitasking), siehe Abbildung 5, um die Bildschirmfotos zu erstellen“.

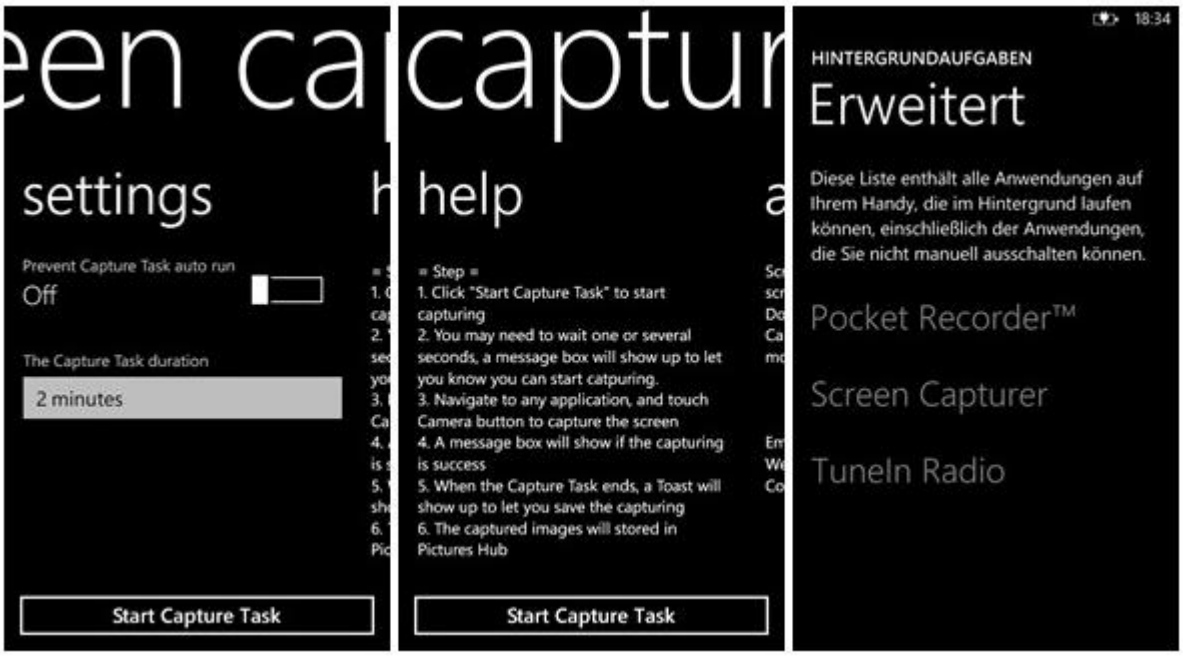


Abbildung 5 - Beispiel für Homebrew-Software, Quelle: Eigene Darstellung

Einstellen kann man in der App nicht viel, lediglicheine Abfrage kann konfiguriert werden, nämlich wie lange die Screenshot-App im Hintergrund laufen soll. Zur Erstellung wird der Kameraknopf umfunktioniert, wenn man diesen leicht drückt (Auto-

Fokus), wird der Screenshot in die „Gespeicherten Bilder" gespeichert. Eine Abfrage will wissen, ob man weitere Screenshots erstellen will oder aufhören möchte. Die App ist nicht perfekt, so ist es nicht möglich sämtliche Bildschirminhalte zu übertragen. Offenbar gelingt das nur mit Silverlight Apps und nicht mit XNA/DirectX oder dem Kamerabild.

5.6 Illegaler Bezug von Applikationen

Applikationen für Windows Phone werden über den Marketplace vertrieben und von dort über das Phone oder die Zune Software heruntergeladen. Unter [70] wird ein Angriff beschrieben, wo mittels einer Desktop-Software die XAP-Datei, also das Installationsformat, in dem Applikationen vorliegen, heruntergeladen und der Digital Rights Management-Schutz entfernt wird. Die XAP-Datei kann dann über Sideloading auf ein Gerät gespielt werden oder im Emulator des SDK verwendet werden. Ein Proof-of-Concept Videos zeigt diese Lücke[12].

Eine Variante dieser Software wurde später veröffentlicht, zum Zeitpunkt der Abfrage im Oktober 2011 war die Software auf XDA-Developers wieder zu finden[13], weil sie sich auf den Download von freier Software beschränkt.

5.7 Debranding von Windows Phone

Microsoft gestattet dem Mobile Operator eine gewisse Anzahl von Einstellung und Anpassungen an der Windows Phone Software vorzunehmen, darunter u.a. folgende:

- Ob der Benutzer andere Systemsprachen auswählen kann und welche.
- Die Standardsuchmaschine für den Browser.
- Ob Auto Data Config (ADC) eingeschalten ist.

Nimmt ein Mobile Operator solche – und weitere meist Marketing-bezogenen – Anpassungen vor, dann spricht man von einem „Branding" oder „gebrandeten" Gerät. Microsoft macht den Mobile Operators hierbei strenge Vorgaben, damit jeder Benutzer prinzipiell dieselbe Erfahrung macht, egal bei welchem Unternehmen die Telefoniedienste bezogen werden. Allerdings kann der Mobile Operator diese exemplarisch genannten Einstellungen treffen und diese können durch den Benutzer nicht geändert werden. Der Grund für diese Einschränkungen liegt in einem vereinfachten Support seitens des Mobile Operator. So müsste der Helpdesk Geräte nur in einer Sprache betreuen, da der Benutzer diese nicht ändern kann. Allerdings haben diese Einstellungen für den Benutzer, der mit den Standardeinstellungen nicht zufriedenen ist, etwa weil er eine andere Sprache spricht negative Auswirkungen die sogar so weit reichen, dass Standardfunktionalität nicht genutzt werden kann.

Beispiel 1: Ein Benutzer hat Gerät das durch einen Provider gebrandet ist. Dazu ist es nicht notwendig, dass der Benutzer tatsächlich bei einem Mobile Operator gekauft hat, solche Geräte sind auch im Handel zu finden (SIM-Lock frei, aber dennoch einem Provider zugeordnet). Während man den Access Point Name (APN) für den

[12] Video: http://www.youtube.com/watch?v=flqB9WCkGiQ
[13] Download unter http://forum.xda-developers.com/showthread.php?t=908293

Internetzugang problemlos setzen kann, so gilt dies nicht für die Multimedia Message Service (MMS) Einstellungen, wofür oftmals ein separater Proxy-Server zu benennen ist. Auch dadurch entsteht noch nicht direkt ein Problem, denn durch ADC wird dieser Proxy automatisch gesetzt – wenn der Mobile Operator nicht genau diesen Automatismus unterbunden hat, wie das beispielsweise Vodafone Deutschland tut. Unter Umständen helfen hier bestimmte Applikationen vom Hardwarehersteller, die die richtigen Einstellungen dennoch setzen können, wie etwa *Network Setup* (LG) oder *Verbindungssetup* (HTC) – wenn bei diesen Werkzeugen die korrekten Einstellungen für das gewünschte Netz enthalten sind. Ist das nicht der Fall, dann hat Benutzer folgende Situation: ein Mobile Operator hat, bei dem der Benutzer nicht einmal Kunde ist, hat negative und durch den Benutzer nicht behebbare Einschränkungen getroffen.

Beispiel 2: Ein Update steht zur Verfügung, jedoch zögert der Mobile Operator das Rollout hinaus. Dieses Update ist für den Benutzer jedoch wichtig, da dringend benötigte Funktionalität kommt, oder gar sicherheitsrelevante Patches eine schnelle Reaktion erfordern.

Im Fall der Einschränkungen kann bzw. muss mit einem Registry Editor (siehe 5.3Registry Editor) der entsprechende Wert verändert werden, z.B. kann für das genannte ADC dieser Wert [14] gesetzt werden:

```
[HKEY_LOCAL_MACHINE\System\AutoDataConfig] "RunADC"=dword:1
```

Benutzer eines LG E900 Endgerätes können die versteckte App *MFG* nutzen, um ADC direkt einzuschalten, mehr zu *MFG* siehe unter 5.3.

Im Falle des Updates, das der Mobile Operator noch nicht zur Verfügung stellt, hilft ein so genanntes „Debranding", also dem Entfernen sämtlicher Informationen, die das Gerät als „Provider-Gerät" identifiziert. Das Branding besteht aus Registry-Schlüsseln, werden diese ausgetauscht, kann das sich das Gerät als ungebrandet bzw. so genanntes Open Market Gerät ausgeben oder sogar als Gerät eines anderen Mobile Operators.

Beispiel 1: Ein LG E900 Endgerät, wie es von Vodafone Deutschland kommt, bzw. so auch im Handel (z.B. bei Media-Saturn) ohne Vertrag verkauft wurde.

```
HKEY_LOCAL_MACHINE\System\Platform\DeviceTargetingInfo
MobileOperator : VOD-DE
MOName: Vodafone
OEMDeviceName: ATLANTIC_VDF_DE
```

Beispiel 2: Ein ungebrandetes LG E900 mit Open Market ROM hat unter dem Schlüssel `HKEY_LOCAL_MACHINE\System\Platform\DeviceTargetingInfo` folgende STRING-Werte:

[14] Anmerkung: in einigen Fällen müssen hier noch weitere Schritte unternommen werden um MMS voll nutzen zu können und die Einstellungen in einer XML-Datei auf das Gerät übertragen werden. Während dieser Prozess auf entsprechenden Seiten gut beschrieben ist, erscheint das jenseits dessen, was ein Nicht-Techniker tun kann.

```
MobileOperator : 000-88
MOName: OPN
OEMDeviceName: Atlantic_OPN_NEU
```

Allerdings gibt es weitere mögliche Unterschiede, so kann die Firmware des Geräts bei gebrandeten Geräten eine andere sein, als jene die ungebrandet in den Verkauf kommen, auch dafür kann das Beispiel mit dem LG E900 dienen, vgl. [71]. Will der Benutzer also sein Endgerät komplett umstellen, so muss er das Gerät „flashen" – also eine komplett neue Software inklusive Firmware auf das Gerät aufbringen[15]. Eine entsprechende Anleitung, wie z.B. hier [72] enthält den Download der entsprechenden Werkzeuge, des Betriebssystems und der Windows-Treiber um das Gerät in einen – anderen – fabriksneuen Zustand zu bringen. Sämtliche Daten und Anwendungen, die sich vorher auf dem Telefon befunden haben, werden durch diesen Vorgang gelöscht.

6 Privatsphäre und Datenschutz auf Windows Phone

In diesem Kapitel wird untersucht, welche Dienste und Funktionen eine Auswirkung auf die Privatsphäre haben können.

6.1 Persönliche Daten auf Windows Phone

Dadurch, dass auf einem Smartphone die verschiedenen Dienste konsumiert werden, ist auch die Anzahl an beteiligten Parteien stark abhängig von der tatsächlichen Nutzung von Windows Phone durch den Benutzer.

Generell lässt sich feststellen, dass auf Windows Phone immer erst eine Handlung („Opt-In") gesetzt werden muss, bevor ein Dienst zugelassen wird, allerdings wird man sich einigen Diensten nicht verwehren können, wenn ein Betrieb als Smartphone angestrebt wird. Das betrifft beispielsweise die Anmeldung am Telefonnetz, womit man telefonieren und Datenverbindungen nutzen kann. Der Mobile Operator hätte aber nun die Möglichkeit Bewegungsprofile zu erstellen, daraus ableitend auch, mit wem sich der Benutzer häufig trifft (aus den Profilen anderer Kunden) oder, da er ja auch die Datenverbindung zur Verfügung stellt, auch welche (unverschlüsselten) Suchanfragen im Web abgesetzt werden. Der Frage nach dem bewussten Abschalten von Diensten wird in Kapitel 6.5 nachgegangen.

Viele Daten fallen bei der Nutzung von sozialen Netzwerken an, Windows Phone unterstützt dabei folgende Netzwerke mit einer tiefen Integration in das System, d.h. hierfür sind keine extra Apps notwendig:

- Windows Live: Microsofts eigener Dienst, dieser ist bei Windows Phone sichtbar mit Windows Live Messenger (Chat) der auch den Präsenz- bzw. Onlinestatus

[15] Das hat allerdings mehrere Implikationen, wie z.B. eine mehrfache Verletzung des Urheberrechts, da weder das ROM noch die benötigten Werkzeuge vom jeweiligen Rechteinhaber zur Verfügung gestellt werden. Zusätzlich wird der Mobile Operator im Falle eines Schadens etwaige Gewährleistungsansprüche ablehnen, die durch die Verwendung solcherart besorgter Software auftreten oder dem Versuch selbige auf das Gerät zu spielen.

überträgt , der Synchronisation von Microsoft OneNote-Notizbüchern auf Windows Live SkyDrive (Online-Festplatte), Bilder (ebenfalls über SkyDrive) und –so die Windows Live ID eine Hotmail-Adresse ist, auch die Synchronisation von E-Mails, Kontakten und Kalender.

- Facebook: Synchronisiert Kontakte, Kalender. Vom Phone lässt sich außerdem der Facebook-Chat nutzen. Es lassen auch direkt Bilder posten und herunterladen.
- Twitter: Statusnachrichten können gepostet werden, allerdings kein vollwertiger Client (keine Suche, keine Möglichkeit neuen Personen zu folgen).
- LinkedIn: Synchronisiert Kontakte und Statusnachrichten.
- Xbox Live: Login über Windows Live ID, eigenes Freundes-Netzwerk, Statusnachrichten und der so genannte Gamerscore. Je länger und erfolgreicher man spielt, desto höher ist dieser Score, es lassen sich also Rückschlüsse auf das Freizeitverhalten der Person ziehen, zumal auch die gespielten Spiele sichtbar sind.

Die Integration besteht vor allem darin, dass hier die Kontakte nicht in einer App gespeichert werden, sondern im Kontakte-Hub, analog dazu Kalendereinträge im Kalender. Windows Phone macht es einfach, Daten an diese Dienste zu senden, so kann eine neue Statusnachricht gleichzeitig an Facebook, Twitter, LinkedIn und Windows Live geschickt werden. Während also hier zwar viele Daten anfallen, gibt es auf dem Phone selbst für diese Dienste keine Privatsphäreneinstellungen. Diese müssen einzeln auf den Webseiten der jeweiligen Betreiber getroffen werden. Jeder dieser Betreiber hat eigene Nutzungsbestimmungen und Datenschutzeinrichtungen, die sich auch ändern können. Weitere Netzwerke, wie etwas XING, StudiVZ oä. lassen über Apps nutzen, bieten allerdings keine so tiefe Integration.

Eine andere Funktion birgt bezüglich Sicherheit und Privatsphäre Schadenspotential: Fotos. Das erste Szenario mit Schadenspotential ist die Möglichkeit, geschossene Fotos sofort hochzuladen und zwar entweder in SkyDrive oder in Facebook. Wenn der Fotoordner für andere freigegeben ist (was bei Facebook der Fall ist, die „mobilen Uploads“ sind für Freunde sichtbar), dann kann es leicht passieren, dass ein unpassendes Foto ungewollt Verbreitung findet.

Eng damit verbunden ist das zweite Szenario, Windows Phone lässt sich so konfigurieren, dass Fotos und Filme auch mit Bildschirmsperre aufgenommen werden können indem man den Auslöser vier Sekunden lang gedrückt hält. Diese Funktion im Zusammenhang mit dem automatischen Upload stellt ein nachvollziehbar gefährliches Beispiel für eine durch den Benutzer verursachte Einstellung mit Schadenspotential für die Privatsphäre dar.

Es lässt sich die Aussage nachvollziehen: je mehr der Benutzer nutzt und aktiviert, desto transparenter wird er. Es soll aber anhand eines Beispiels auch geklärt werden, ob eine Erhöhung der Privatsphäre bei akzeptablem Verlust von Funktionalität möglich ist, siehe Kapitel 6.5. Bezüglich der Wechselwirkungen von Usability und Sicherheit siehe Kapitel 9 und 10.

6.2 Datenschutz und Passwort-Sicherheit

Bei den meisten Services hängt die gesamte Sicherheit und der Schutz dieser Daten am Benutzernamen und dem Passwort, erst in jüngster Zeit rüsten hier Anbieter wie Facebook mit zusätzlichen Abfragen auf, z.B. wenn ein Login-Versuch plötzlich von einer geographisch weit entfernten Position kommt. Deshalb muss das Passwort der Windows Live ID geheim gehalten werden, so steht es in den Nutzungsbestimmungen der Windows Live ID [73]: „Sie müssen Ihr Passwort geheim halten und dürfen Dritte nicht berechtigen, in Ihrem Namen auf den Service zuzugreifen und/oder ihn zu verwenden, es sei denn Microsoft stellt diese Möglichkeit für den Zugriff auf den Service durch Dritte ausdrücklich zur Verfügung.“. Darf also das Passwort zur Anmeldung an Windows Live in eine Applikation eingegeben werden, die nicht von Microsoft stammt?

Beispiel: Es hat mit Windows Phone 7 keinen offiziellen Windows Live Messenger gegeben, erst mit Windows Phone 7.5 ist die Fähigkeit direkt mit dem Phone über das Windows Live Netzwerk zu chatten und Bilder zu senden eingeführt worden. Bis dahin hat es nur eine Applikation namens „Messenger by Miyowa“[16] gegeben. Diese hat die Windows Live ID Anmeldeinformationen (Benutzernamen und Passwort) entgegengenommen und lokal gespeichert – dabei sogar gewarnt, dass das Speichern ein mögliches Sicherheitsrisiko darstellt. Diese Anwendung ist keine offizielle Microsoft-Anwendung, aber mit Unterstützung in Form einer eigenen Presseaussendung [74] von Microsoft Frankreich beworben worden und dort als „neue Version von Windows Live Messenger“ bezeichnet. Die Frage: reicht eine Pressemeldung und u.U. eine finanziell Unterstützung für den App-Entwickler aus, damit der Benutzer davon ausgehen kann, dass die Anwendung sicher ist? Wie bemerkt der Anwender, dass Microsoft diese Art der Nutzung „ausdrücklich zur Verfügung“ stellt? Letztlich gibt der Anwender sein Passwort in eine möglicherweise unsichere Applikation ein und weiß nicht, ob diese Daten nicht übertragen werden. Siehe dazu auch die Problemstellungen von Kapitel 7.8.

6.3 Ändern Updates etwas an der Privatsphäre?

Bei den bisherigen Updates des Betriebssystems, wo auch neue Funktionalitäten hinzugekommen sind („NoDo“ und „Mango“), war keine Verschlechterung der Privatsphäre festzustellen. Das hat damit zu tun, dass Microsoft im Auslieferungszustand neuer Funktionen die Einstellungen möglichst sicher gestaltet.

Beispiel: Bei Windows Phone 7.5 („Mango“) ist die Funktionalität des Chats über Windows Live Messenger hinzugekommen. Dieser Chat und der Präsenzstatus muss jedoch erst aktiviert werden.

Bei Updates von Applikationen ist es so, dass die Capabilities (siehe Kapitel 4.12) in jedem Fall erneut abgefragt werden, nutzt also eine Anwendung nun das Mikrofon oder die Ortungsdaten, so wird beim Update der Benutzer um sein Einverständnis gefragt.

[16] Download unter http://www.windowsphone.com/de-at/apps/58470cb0-25dc-df11-a844-00237de2db9e

Nicht am Telefon sichtbar, aber umso gefährlicher sind Änderungen bei den mit dem Phone mitgenutzten sozialen Netzwerken, so schreibt [75]: „Zum einen sammelt das Netzwerk unaufhörlich ohne Einzelgenehmigung Daten der Nutzer, zum anderen ändert es so oft die Datenschutzoptionen, dass selbst der beste Facebook-Kenner oft nicht weiß, wer nun welche Texte oder Bilder von ihm momentan tatsächlich sehen kann“.

6.4 Speicherort von privaten und geschäftlichen Daten

Microsoft unterscheidet bei der Nutzung der Rechenzentren zwischen Privatbenutzern bzw. „Consumer-Services“ wie Windows Live und Firmennutzern bzw. Angebote wie Office 365. Bei den sich an die Konsumenten richtenden Diensten sichert Microsoft nicht zu, in welchem Rechenzentrum die Daten verarbeitet werden und teilt auch nicht die Standorte der Rechenzentren mit. Speichert also ein Benutzer Daten auf SkyDrive, so kann nicht gesagt werden, wo diese Daten physisch liegen.

Anders ist es bei den Microsoft Online Services wie Office 365, hier wird zugesichert, dass die Daten prinzipiell innerhalb der Region bleiben, wobei jede Region für die Services von Office 365 ein Haupt- und ein Ausfallsrechenzentrum hat. Die Daten für europäische Kunden liegen dabei in Dublin, Irland sowie im Ausfallsrechenzentrum in Amsterdam, Niederlande. Laut Microsoft „kann es jedoch einige wenige Fälle geben, in denen Microsoft-Personal oder -Vertragspartner außerhalb der angegebenen Region auf Kundendaten zugreifen müssen (z. B. für technischen Support, Problembehandlung oder in Erwiderung einer gerichtlichen Vorladung).“ [76].

Nicht erwähnt aber damit wohl gemeint wird hier die Implikationen, die der „Providing Appropriate Tools Required to Intercept and Obstruct Terrorism“ (PATRIOT) ACT”[17] mit sich bringt, wonach US Behörden Zugriff auf die in Europa gespeicherten Daten haben. Dazu wird Thilo Weichert, Chef des Unabhängigen Landeszentrums für Datenschutz Schleswig Holstein (ULD) in [77] zitiert, demnach stünden „solche Datenweitergabe aus dem EU-Gebiet heraus im Widerspruch zu europäischem Datenschutzrecht“.

6.5 Erhöhen der Privatsphäre durch Deaktivierung von Funktionen

Am Beispiel der Standort- bzw. Ortungsdienste soll gezeigt werden, wie sich der Versuch der Erhöhung der Privatsphäre durch Deaktivierung von Funktionen auf das Benutzererlebnis auswirkt.

6.5.1 Setup

Die Nutzung von Positionsdaten gehört zu einem Smartphone dazu. In diesem Kapitel soll darauf eingegangen werden, was passiert und in wie weit man die Funktionalitäten von Windows Phone beschneidet, wenn man die Ortung nicht zulässt.

[17] H.R.3162 -- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001 (Enrolled Bill [Final as Passed Both House and Senate] - ENR), Online abrufbar unter: http://thomas.loc.gov/cgi-bin/query/z?c107:H.R.3162.ENR:

Unter Location Based Services versteht man die Nutzung von Diensten abhängig vom Standort. Zum Beispiel werden auf der Karte die nächsten Restaurants angezeigt (siehe dazu Kapitel 8.3.5). Automatisch ergeben sich durch eine solche Abfrage gewisse Implikationen für die Privatsphäre, da ein Anbieter („Ich weiß wo Restaurants sind“) die Informationen über den Standort und je nach Suchbegriff auf die Vorlieben und Verhaltensweisen eines Benutzers bekommt („Suche koscheres Essen“).

Als Quellen für die Standortdaten dienen laut auf Windows Phone „der Global Positioning System- (GPS-)Empfänger, WLAN und die Zelleninformation des Mobilfunknetzes“ [78]. Bei WLAN werden die in der Nähe befindlichen WLANs hergenommen und in einer Datenbank nachgeschlagen. Wird in der Datenbank das WLAN gefunden, so kann mit dieser Information der ungefähre Standort schneller bestimmt werden, als das unter Umständen mit GPS der Fall gewesen wäre. Diese Datenbank wird von Windows Phones befüllt, denn diese schicken die in der Nähe gefunden WLANs zurück an Microsoft. Dies geschieht jedes Mal, wenn auf die Ortungdaten von Windows Phone durch eine Funktion oder App zugegriffen wird. Laut Microsoft sind dabei „keine Daten enthalten, die den Benutzer identifizieren können“ [79] , sondern lediglich eine temporäre ID um zu unterscheiden, ob der selbe Benutzer zehn Mal an einem bestimmten Ort war, oder ob es sich um zehn verschiedene Benutzer gehandelt hat. Zusätzlich wird der Service Set Identifier (SSID) des WLANs übertragen.

Für den Anwendungsentwickler steht eine Schnittstelle zur Verfügung, die „die Location Services initialisieren kann, Änderungen im Status abwickelt und die Ortungsdaten empfangen kann“ [80], unabhängig davon, von welcher Quelle diese Information kommt. Diese Schnittstelle muss über die Capabilities (siehe Kapitel 4.12) genehmigt werden. Eine Übersicht für den Benutzer, welcher App auf dem Phone der Zugriff auf die Standortdaten gestattet wurde, ist nicht vorhanden.

6.5.2 Aufgabenstellung

Im Auslieferungszustand sind sämtliche Ortungsfunktionen deaktiviert, jedoch fragt Windows Phone bei der Erstnutzung nach, ob die Ortung in der jeweiligen App genutzt werden soll. In diesen mitgelieferten Anwendungen werden die Ortungsdienste verwendet.

- Bilder: Hier kann eingestellt werden, ob die Positionsdaten mit dem Bild gespeichert werden sollen und ob diese Information beim Hochladen in sozialen Netzwerke oder auf SkyDrive gelöscht oder beibehalten werden soll.
- Internet Explorer: ist die Ortnung hier aktiv, können Webseiten (z.B. Google) ebenfalls die aktuelle Position nutzen – hier erfolgt vor Übermittlung eine Abfrage.
- Karten: Mit den Positionsdaten kann man auf seine eigene Position zoomen und eine Routenplanung von diesem Standort aus durchführen.
- Suche: Zur Darstellung von lokalen Informationen kann auch hier die Ortung zu passenderen Suchergebnissen genutzt werden. Deaktiviert im

Auslieferungszustand sind weitergehende Optionen wie das Senden von Positionsdaten bei Microsoft Tags.

- Einchecken: um den eigenen Standort in soziale Netzwerke zu schreiben kann über die „Ich“-Kachel die „Einchecken“-Funktion genutzt werden.
- Mein Handy finden: die Ortung für verlorene Phones überträgt ebenso den Standort.

Selbstverständlich benötigen weitere Apps aus dem Marketplace ebenso die Standortdaten. Für die globale Konfiguration der Ortungsdienste findet man unter Einstellungen die Option, diese zu aktivieren oder zu deaktivieren, eine feinere Einstellung oder eine Übersicht gibt es hier nicht, die Aufgabe ist nun, die Ortungsdaten global abzuschalten.

6.5.3 Erwartungshaltung

Der Umgang mit Standortdaten ist ein sensibles Thema (vgl. [81]), es wird erwartet, dass Microsoft sich des Themas umfassend angenommen hat und eine entsprechende Verwendung des Smartphone trotz Deaktivierung der Ortungsfunktionen dennoch möglich ist.

6.5.4 Auswertung

Bei den Applikationen und Anwendungsfällen, die in der Aufgabenstellung genannt wurden, ergibt das Ausschalten der Ortungsdienste folgendes Bild:

- Bilder: keine Einschränkung, es fehlen den Bildern lediglich die Standortdaten – was gewollt war.
- Internet Explorer: Keine Einschränkungen beim Surfen.
- Karten: Die Kartenanwendung bleibt grundsätzlich benutzbar, allerdings weist ein Popup darauf hin, dass man doch die Ortungsdienste aktivieren soll.
- Suche: Funktioniert, lediglich beim Reiter „Lokal“ der Ergebnisse aus der Umgebung zeigen soll, wird darauf hingewiesen dass die Ortungsdienste deaktiviert sind. Das ist aber bei BING in Österreich sowieso unerheblich, da BING hierzulande keine lokalen Daten liefert (siehe Kapitel 8.3.5).
- Einchecken: Funktion liefert Popup, wie bei Karten; es steht keine „Einchecken“-Funktion zur Verfügung.
- Mein Handy finden: Einstellungsdialog liefert Popup.

Bei Applikationen aus dem Marketplace ist es möglicherweise nicht ganz eindeutig: will man eine App beziehen, die Ortungsdienste in den Capabilities verwendet, so wird man ebenso gefragt, ob man der Anwendung nun die Ortungsdienste erlauben will. Klickt man hier auf *Abrechen*, bricht die ganze App-Installation ab. Man muss in jedem Fall *Erlauben* – da die globale Einstellung sowieso abgeschaltet ist, wird der Standort trotz des Klicks vor der Installation nicht übertragen. Zu Bedenken wäre allenfalls: erlaubt man die Ortung wieder (global), dann hat auch die neu installierte App das Recht auf die Schnittstelle zuzugreifen. Hier müsste der Benutzer in diese App gehen und die Einstellung wieder deaktivieren.

Dieses Verhalten kann als Usability-Schwäche ausgelegt werden, weil der Dialog nicht ganz klar ist, jedoch wird im Fehlerfall die Installation abgebrochen und somit bleibt – wenn gleich nicht der gewollte – ein sicherer Zustand erhalten.

Ungewollte Übertragungen, wo trotz deaktivierter Einzel-Einstellung in der Kamerasoftware dennoch Daten an Microsoft übertragen werden gelten als Fehler. Microsoft berichtet von „ungewolltem Verhalten“ und das „zukünftige Updates dieses Verhalten korrigieren“ [82]. Eine selektive Einstellung, beispielsweise „Nutze GPS, aber übertrage keine Informationen zurück ins Netz“ ist nur über einen Umweg möglich, der nicht praktikabel erscheint: Man schaltet die Ortung ein, aber sämtliche Datenverbindungen aus. Die API nutzt dann als Quelle nur noch den GPS-Empfänger und kann weder andere Daten abfragen, noch die Standortdaten senden.

Zusammenfassend kann hier die Erwartungshaltung dennoch als erfüllt angesehen werden, das Phone bleibt auch mit der erhöhten Privatsphären-Einstellung nutzbar.

6.5.5 Erkenntnisse

Nachdem die Frage bezüglich der Ortungsfunktion zufriedenstellend geklärt war ist eine weitere Fragestellung ist in diesem Zusammenhang aufgetaucht: kann ein Windows Phone auch ohne Live ID betrieben werden? Die Antwort darauf lautet: Ja, allerdings beschneidet man das Smartphone dann um genau jene Eigenschaft, die Smartphones so auszeichnet: die Erweiterung des Funktionsumfanges mittels weiterer Anwendungen. Die Live ID ist notwendig für den Marketplace, es können also keine – auch keine gratis – Anwendungen heruntergeladen werden. Auch in Bezug auf die Sicherheit: es kann weder die Funktion zur Wiederauffindung des Telefons noch die Fernlöschung aktiviert werden. Zumindest die Fernlöschung kann auch über Exchange durchgeführt werden. Zune Musik und Xbox Services sind ebenso von der Windows Live ID abhängig. Anders als bei der Ortung kann also hierbei nicht mehr von aufrechter Nutzungsmöglichkeit gesprochen werden.

Während dieser Analyse sind unzählige Popups bezüglich der Ortung aufgetaucht. Als direkte Folge soll eine Analyse klären, ob Benutzer diese Warnungen überhaupt noch wahrnehmen.

7 Benutzer-Szenarien zur Sicherheit

In diesem Kapitel werden Angriff oder Verhaltensweisen beschrieben, die ein Schadenspotentials oder eine Problemstellung für den Benutzer in Bezug auf Sicherheit oder Privatsphäre bedeuten. Die Vorgehensweise richtet sich nach der in Kapitel 1.3.3 beschriebenen Methodik.

7.1 Remote Desktop App

Smartphones lassen sich auch zum Fernzugang („Remote access“) zu PCs oder Servern einsetzen.

7.1.1 Ausgangsbasis/Situation

Eine solche Technologie des Fernzugangs ist in Windows mit dem Remote Desktop Procol (RDP) inkludiert. Mit einem RDP-Client kann so auf andere Clients oder Windows Server zugegriffen werden. Für Windows Phone 7 standen allerdings keine RDP Clients zur Verfügung, da dafür eine Unterstützung über die Netzwerkschnittstelle, so genannte Sockets erforderlich waren. Zur Umgehung dieser Problematik gab es eine Reihe von Virtual Network Computing- (VNC-)Clients, die die Verbindung über eine eigene Serverkomponente über HTTPS realisierten. Problematik dabei: es ist nicht jedermanns Sache auf (Kunden-)Servern eine weitere Komponente zu installieren. Deswegen stach eine Anwendung heraus, die – ungeachtet der technischen Unmöglichkeit – einen RDP-Zugang versprach: „Remote Desktop“ von der Firma Topperware.

7.1.2 Angriff/Problematik

Topperware löste die Problematik, dass die Sockets nicht verfügbar waren, pragmatisch und ließ den Windows Phone Client über eine VNC-Verbindung zu einem selbst gehosteten Proxy-System verbinden, dieses baute dann die RDP-Verbindung zum Zielserver auf.

7.1.3 Bedrohungs-/Schadenspotential

Diese Vorgehensweise funktioniert zwar, bedingt allerdings, dass Topperware zum Verbindungsaufbau mit dem Zielsystem den Benutzername und Passwort im Klartext erhält und verarbeitet.

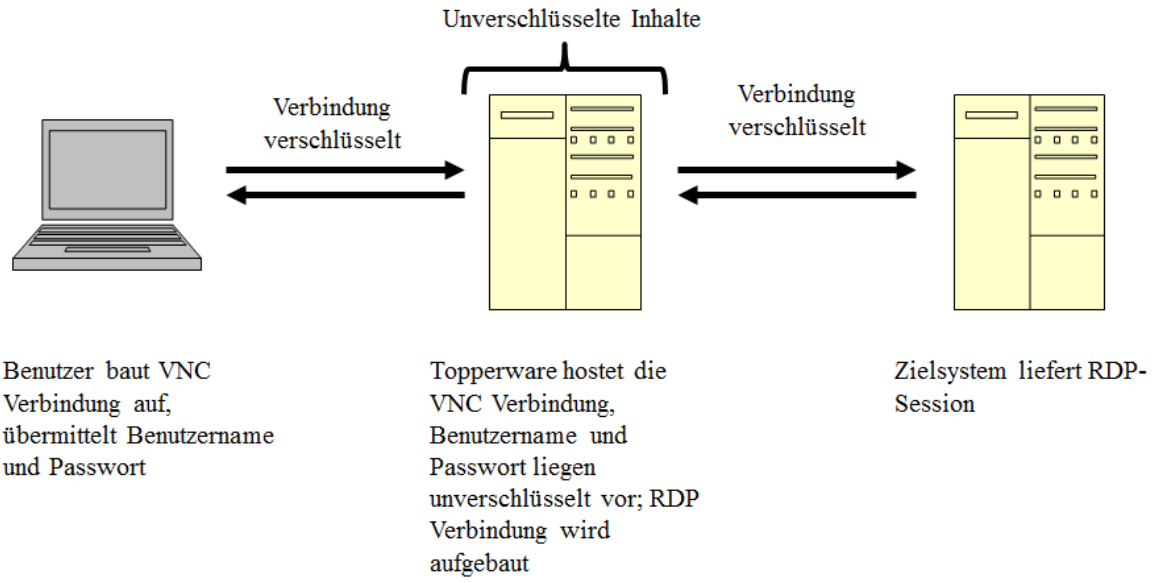


Abbildung 6 - Sicherheitsarchitektur, Quelle: Eigene Darstellung

Damit vertraut ein Benutzer unter Umständen das Kennwort des Domänenadministrators einer Firma an, die zumindest bis Oktober 2011 nicht einmal eine Adresse auf der

Homepage führte[18]. Zudem verbieten Sicherheitsrichtlinien zumeist aus naheliegenden Gründen Passwörter an Drittsysteme zu übergeben, man geht durch die Verletzung solcher Firmen-Richtlinien also noch zusätzliche Risiken ein.

7.1.4 Lösung/Milderung des Problems

Der Hersteller war sich dieser Sicherheitsproblematik bewusst und hat auch einen eigenständigen Server zum Download angeboten, dieser konnte als eigener Proxy dienen. Mittlerweile mit Erscheinen von Windows Phone 7.5, wo Sockets möglich sind, hat Topperware nachgebessert und unterstützt in seiner Software auf diesen Systemen den nativen Zugang über RDP. Das ändert jedoch nichts, dass laut Applikationsfeedback im Marketplace viele Personen diese Software in einer Art freiwilligem „Man-in-the-middle-attack"-Modus betrieben haben.

7.2 Angriff mittels gefälschter Zertifikate

Selbst erstellte Zertifikate müssen manuell in das System gespielt werden, und eigenen sich deshalb nur bedingt für Angriffe. Anders sieht die Situation aus, wenn man sich Zertifikate einer Root CA besorgen kann, vgl. die in Windows Phone vorinstallierten SSL Zertifikate [83].

7.2.1 Ausgangsbasis/Situation

Der Angreifer hat sich gefälschte Zertifikate eine über eine Zertifizierungsstelle („Trusted CA") erschlichen, vgl. dazu den Angriff auf Comodo, wo „ein Reseller Account dazu benutzt wurde, neue gefälschte Zertifikate auszustellen" [84] .

7.2.2 Angriff/Problematik

Mit diesen Zertifikaten wird eine „Man-in-the-middle"-Attacke durchgeführt, Microsoft selbst beschreibt das in Szenario in [85].

7.2.3 Bedrohungs-/Schadenspotential

Die Datenübertragung kann mitgelesen werden, eventuell kann der Benutzer auch zur Eingabe von Daten und Passwörtern gebracht werden („Phising") wodurch die Sicherheit von den entsprechenden Konten nicht mehr gewährleistet ist.

7.2.4 Lösung/Milderung des Problems

Als Benutzer lautet die Empfehlung Zertifikate nur dann einspielen, wenn diese aus einer vertrauenswürdigen Quelle kommen und sonst Updates zeitnahe einzuspielen – so dies möglich ist, siehe Kapitel 7.5. Für den Benutzer ist es jedoch nicht möglich zu erkennen, dass die SSL-gesicherte Verbindung nicht zum gewünschten, vermeintlichen Ziel aufgebaut wurde.

7.3 Apps, die die anonyme ID weniger anonym machen

Die Identität des Benutzers ist dem Anwendungsentwickler im Normalfall verborgen. Hier wird beschrieben, wie der Entwickler den noch Daten so verknüpfen kann, dass die Anonymität aufgehoben ist.

[18] Siehe http://www.topperware.co.uk/

7.3.1 Ausgangsbasis/Situation

In diesem Szenario hat ein Entwickler mehrere Applikationen. Aus bestimmten Gründen möchte er diese Applikationen bestimmten Benutzern zuordnen und im Idealfall mit einem bestehenden Account in Verbindung bringen. Dazu nutzt er zwei dokumentierte Funktionen von Windows Phone, die *DeviceUniqueId* und die *UserExtendedProperties*.

Die *DeviceUniqueId* ist ein 20 Byte großes Bytearray das einen einzigartigen Hashwert des Geräts enthält. „Die Device ID ändert sich bei einem Update des Betriebssystems nicht“ [86]. MSDN rät ab, diese ID zur Identifizierung des Benutzers zu verwenden, da die ID auch im Falle eines Besitzerwechsels gleich bleibt. Zur Unterscheidung der Benutzer sieht Microsoft die *UserExtendedProperties* vor, die eine anonymisierte, aus der Windows Live ID generierte 32 Zeichen lange ID zurückgeben können, siehe [87]:

```
string anid = UserExtendedProperties.GetValue("ANID") as string;
string anonymousUserId = anid.Substring(2, 32);
```

Zwar sollte diese Klasse nur bei Verwendung des Microsoft Advertising SDK for Windows Phone verwendet werden, es gibt allerdings keine Einschränkung diese auch ohne der Werbeplattform zu nutzen.

Damit diese Werte aber überhaupt erst ausgelesen werden können, müssen die entsprechenden Capabilities in der Datei *WMAppManifest.xml* gesetzt sein. Damit taucht auch der entsprechende Hinweis im Marketplace bei der App, dass diese Fertigkeiten zur Anwendung kommen [88]:

```
<Capabilities>
	...
	<Capability Name="ID_CAP_IDENTITY_DEVICE"/>
	<Capability Name="ID_CAP_IDENTITY_USER"/>
	...
</Capabilities>
```

Der Code zum Zugriff sieht dann so aus [88]:

```
public static byte[] GetDeviceUniqueID()
	{
		byte[] result = null;
		object uniqueId;
		if (DeviceExtendedProperties.TryGetValue("DeviceUniqueId", out
		uniqueId))
			result = (byte[])uniqueId;
		return result;
	}
public static string GetWindowsLiveAnonymousID()
	{
		string result = string.Empty;
		object anid;
		if (UserExtendedProperties.TryGetValue("ANID", out anid))
		{
```

```
        if (anid != null && anid.ToString().Length >= (ANIDLength +
        ANIDOffset))
        {
              result = anid.ToString().Substring(ANIDOffset, ANIDLength);
        }
        }
        return result;
  }
```

Es sei hier angemerkt, dass die Verwendung dieser beiden Funktionen für sich genommen weder die Privatsphäre bricht, noch in anderer Weise für sich alleine genommen einen Angriff darstellt. Erst in Kombination mit weiteren Schritt entsteht eine Problematik.

7.3.2 Angriff/Problematik

Die Kunst bei diesem Angriff besteht darin, in einer Applikation den Benutzer zur Eingabe von mehr Details zu bringen, beispielsweise durch Anmelden mit einem Account. Diese App, wo sich der Benutzer anmeldet, könnte auch von einer anderen Firma kommen (Briefkastenfirma, Deckname), somit würde der Benutzer auch erst gar nicht sehen können, dass die eine App mit einer anderen App in einer Beziehung steht. In dem Moment, in dem ein Entwickler eine ID mit mehr Information anreichern kann, bzw. diese und weitere Datenquellen miteinander verknüpft, kann dies als Angriff auf die Privatsphäre gewertet werden, da Microsoft ja absichtlich vorsieht, mittels anonymer ID den Benutzer zu schützen. Andernfalls wäre ja gleich die Windows Live ID abfragbar.

7.3.3 Bedrohungs-/Schadenspotential

Ein direktes Schadenspotential für den Benutzer entsteht erst, wenn diese Verletzung der Privatsphäre zu weiteren Aktionen führt, beispielsweise dem Verkauf von Profil- oder Nutzungsdaten.

7.3.4 Lösung/Milderung des Problems

Besonders bei Applikationen, die persönliche Informationen abfragen, sollte der Benutzer aufmerksam sein, am besten bevor eine solche Applikation überhaupt installiert wird. Die Hinweise auf die benötigten Funktionen im Marketplace sind leider nur bedingt hilfreich, da alleine schon jede gratis Anwendung, die die Microsoft Werbeplattform nutzt, auch die Capabilities IDENTITY_USER und ID_CAP_PHONEDIALER zulassen muss, denn bei einer Werbung könnte man ja direkt anrufen wollen. Der Tipp, man möge also auf Anwendungen verzichten, die diese Fertigkeiten anfordern würde bedeuten, dass man auf eine große Menge an kostenlosen Anwendungen verzichten müsste.

7.4 Positionsdaten missbrauchen

Mittels Windows Phone (ab Windows Phone 7.5) ist die Funktion, sich an einen Ort „einzuchecken“ sogar Bestandteil des Betriebssystems, viele weitere Apps können ebenso die Position einfließen lassen.

7.4.1 Ausgangsbasis/Situation

Ein Benutzer nutzt Dienste wie Twitter, Facebook oder Foursquare. Dabei sind die Funktionen „Meine Position posten“ aktiv. Dazu wird im Selbstversuch über drei Tage die Windows Phone Funktionalität und foursquare intensiver genutzt.

7.4.2 Angriff/Problematik

Bei ausreichender Regelmäßigkeit reichen die Daten aus, ein Bewegungsprofil zu erstellen. Voraussetzung bzw. Erleichterung eines Profiles ist der Freundschaftsstatus in den jeweiligen Diensten. Bei foursquare sollte der Angreifer zusätzlich den Abruf der Profilseite automatisieren, denn bei Freunden sind nur die letzten fünf Logins sichtbar – da könnte bei zu groß gewähltem Zeitabstand sonst der Detailgrad verloren gehen.

7.4.3 Bedrohungs-/Schadenspotential

Das mögliche Schadenszenario lautet hier: kompletter Verlust der Privatsphäre. Bei einem genauen Bewegungsprofil sind Rückschlüsse auf Arbeitszeiten denkbar, auf Freunde und andere Sozialkontakte – speziell wenn sich diese ebenso diese Services nutzen und vieles mehr.

7.4.4 Lösung/Milderung des Problems

Der Benutzer sollte genau wissen, wem und warum er diese Daten zur Verfügung stellen möchte. Im besten Fall stellt er diese Daten nur auf eigene Kosten und ohne weiteren Mehrwert dem Betreiber bzw. Sammler der Daten zur Verfügung, im schlimmsten Fall werden diese Daten aktiv missbraucht. Jedenfalls sollte sich der Benutzer über die Problematik genauestens informieren und – so dieser Verlust der Privatsphäre hingenommen wird - dann kann der Benutzer gleich darüber hinausgehende Dienste nutzen. Beispiel: Ein Anbieter bietet eine „Lebenstagebuchservice“[19] an, das heißt der Benutzer befüllt hier absichtlich sein Profil mit den aggregierten Daten aus twitter, foursquare, Picasa, Facebook und vielen mehr.

7.5 Verzögerte Updates

Dass ein Update prinzipiell verfügbar ist, heißt noch nicht, dass der Kunde dieses auch erhält.

7.5.1 Ausgangsbasis/Situation

Der Updatemechanismus (siehe Kapitel 4.14) funktioniert so, dass verschiedene beteiligte Parteien ihre Zustimmung zum Rollout eines Updates geben müssen, für jedes Endgerät muss die Zustimmung vorliegen.

- Hersteller der Hardware
- Mobile Operator
- Microsoft

Erst wenn das alles zutrifft, wird das Update für den Benutzer angeboten.

[19] Beispiel hierfür: http://memolane.com /

7.5.2 Angriff/Problematik

Die Koordination zwischen allen Mobile Operators, die Windows Phone führen, den Hardwareherstellern, mit allen Endgeräten und Versionen, Firmwares etc,.. und Microsoft lässt erahnen wie groß die Testmatrix hier sein muss und wie leicht es zu Verzögerungen kommen kann. Microsoft hat dies laut eigener Matrix größtenteils im Griff vgl. [89].

7.5.3 Bedrohungs-/Schadenspotential

Die Gefahr bei einer Verzögerung besteht darin, dass die Patches vorliegen und Angreifer über Reverse Engineering aufgrund des Patches einen Exploit schreiben können bzw. die Sicherheitslücke ausnützen versuchen.

Fallbeispiel: Jenes Update, das Windows Phone 7 auf Buildnummer 7392 brachte (von vorher 7390) diente dazu, die neun gefälschten Zertifikate von Comodo sofort zu den „Untrusted Storage“ [90] zu speichern. Dieser Patch wurde im Mai 2011 veröffentlicht, die spanische Telefonica hat diesen Patch auch im November 2011, also sechs Monate später noch nicht für alle Geräte veröffentlicht, die entsprechende Webseite berichtet „bis auf Omnia 7 Geräte, diese werden noch getestet“ [89]. Die Geräte dieser Kunden sind also für gefälschte Zertifikate anfällig, darunter solche von *mail.google.com* oder *login.live.com*.

7.5.4 Lösung/Milderung des Problems

In diesem Fall kann die Lösung nur lauten, dass Microsoft sicherheitsrelevante Patches auch ohne Zustimmung des Mobilfunkbetreibers freigibt. Die Situation, dass ein Mobile Operator aus Marketinggründen oder aus Angst vor erhöhtem Supportaufkommen die Freigabe eines für die Sicherheit unerlässlichen Fixes verzögert, scheint nicht akzeptabel.

7.6 VPN Tunnel

Mit Hilfe eines Virtual Private Networks (VPN) lässt sich eine sichere, verschlüsselte Verbindung in das Firmennetz aufbauen.

7.6.1 Ausgangsbasis/Situation

Die Anforderung kommt oftmals aus dem Firmenbereich, wo für den Zugang zu firmeninternen Ressourcen zwingend eine VPN-Verbindung vorgeschrieben sein kann. Mit Windows Phone soll nun so eine Verbindung geschaffen werden.

7.6.2 Angriff/Problematik

Eine verschlüsselte Verbindung lässt sich über den Browser oder eine HTTPS-basierende App aufbauen. Nicht möglich ist die Umleitung des gesamten Datenverkehrs über einen VPN-Tunnel.

7.6.3 Bedrohungs-/Schadenspotential

Durch diesen Umstand wird der Zugang zu den Ressourcen verwehrt, der Benutzer kann sein Smartphone nicht nutzen. Das Gefahrenpotential das sich dadurch auftut, liegt vor allem im Verhalten des Benutzers. Wenn es keinen offiziellen Weg gibt, dann werden unter Umständen nicht offiziell erlaubte aber technisch mögliche Umgehungswege gewählt. Diese nicht offiziell genehmigten Weg entsprechen den aktuellen Trends der

„Consumerization of IT“ (vgl. [91]), wo Mitarbeiter Geräte, Dienste und Technologien aus dem privaten Bereich für Firmenaufgaben nutzen. Dies geschieht dann nicht in böser Absicht, sondern um eine gestellte Aufgabe schneller und besser zu erledigen. Im vorliegenden Fall kann das dadurch bestehen, dass Dateien auf Hosting- und Synchronisationsdienste wie Dropbox oder SkyDrive abgelegt werden, wo diese dann problemlos mit einem Smartphone abgerufen werden können. Die eigentliche Intention der Sicherheitsrichtlinie, nämlich einen VPN-Zugang vorzuschreiben um mehr an Sicherheit zu schaffen, wird somit in der Umsetzung ins Gegenteil umgekehrt und kann zu unsicherem Verhalten führen.

7.6.4 Lösung/Milderung des Problems

Die Lösung besteht darin, den Mitarbeitern flexibel jene Zugänge zu verschaffen, mit denen sie produktiv und effizient arbeiten können. In diesem Fall kann mit Hilfe von Microsoft SharePoint Server ein sicherer Zugang zu Dokumenten gewährleistet werden (siehe Kapitel 4.15). Mit IRM (siehe Kapitel 4.7) zusammen wäre der Schutz der Information weit über das hinausgehend, was die reine Verschlüsselung der Verbindung selbst bewirkt hätte. Bleibt es jedoch bei der fixen Voraussetzung, dass das Gerät zwingend einen VPN-Zugang aufzubauen muss, dann erfüllt Windows Phone diese Anforderung nicht.

7.7 Personenmarkierungen auf Facebook

Aus Gründen des Schutzes der eigenen Privatsphäre könnte man auf ein Konto bei Facebook verzichten. Das schützt jedoch nur bedingt.

7.7.1 Ausgangsbasis/Situation

Benutzer A ist auf Facebook, Benutzer B nicht. Benutzer A schießt ein Foto und versieht es direkt am Telefon mit einem Namensschild, auch genannt „Tag“. Diese Tags dienen Facebook zur Zuordnung von Fotos zu Benutzern und zum Training der eigenen Gesichtserkennungssoftware.

7.7.2 Angriff/Problematik

Die Zuordnung, die von Benutzer A am Foto vorgenommen wurde, geschah ohne die Zustimmung von Benutzer B. Dennoch weiß Facebook nun den Namen und auch die Gesichtserkennung bekommt dieses Bild zu sehen.

7.7.3 Bedrohungs-/Schadenspotential

Eine selbstgewählte Abstinenz von sozialen Netzwerken wie Facebook wird durch Dritte konterkariert, die gewünschte Art der Privatsphäre wird dadurch nicht erreicht.

7.7.4 Lösung/Milderung des Problems

Die Einstellungen von Facebook erlauben, dass Fotos wo man zu sehen ist, nicht mit dem Namen getaggt werden können bzw. sind diese Markierung ohne Überprüfung zumindest nicht sichtbar. Das funktioniert freilich nur, wenn man selbst auf Facebook ist. Auch ohne Facebook-Konto können Fotos mit dem eigenen Namen von Dritten versehen werden, dagegen gibt es keinen Schutz.

7.8 Die unsichere Messenger App

Benutzer können nicht erkennen, welchen Grad an Sicherheit ein bestimmter Dienst oder eine App bietet. Dadurch ergeben sich unter Umständen massive Beeinträchtigungen bei der Sicherheit.

7.8.1 Ausgangsbasis/Situation

Ein Nutzer möchte SMS-Kosten sparen und lädt eine Messenger-App herunter, um mit seinen Freunden Textnachrichten über die Datenverbindung auszutauschen. Die Wahl fällt auf den KIK Messenger, da dieser für nicht nur für Windows Phone, sondern auch für iPhone, Android und Blackberry verfügbar ist. Laut KIK Darstellung wird der Dienst „von über vier Millionen Nutzern“ [92] in Anspruch genommen.

7.8.2 Angriff/Problematik

Wie Mike Cardwell [93] herausgefunden hat, nutzte KIK keinerlei Verschlüsselung. Mittels des Paketsniffers *Wireshark*[20] konnte er während des Login-Prozesses folgendes aufzeichnen:

```
<query xmlns="jabber:iq:register">
      <username>USERNAME</username>
      <password hashed="false">PASSWORD</password>
      <device-id>DEVICE-ID</device-id>
</query>

<query xmlns="jabber:iq:register">
      <node>USERNAME_yhm</node>
      <email confirmed="true">EMAIL-ADDRESS</email>
      <username>USERNAME</username>
      <first>FIRST-NAME</first>
      <last>LAST-NAME</last>
</query>
```

Ebenso unverschlüsselt ist der Text der Nachricht:

```
<message type="chat" to="RECIPIENTS-USERNAME_wti@talk.kik.com" id="********">
      <body>THE-PLAIN-MESSAGE-CONTENT</body>
      <kik push="true" qos="true" timestamp="1289087937787" />
      <request xmlns="kik:message:receipt" r="true" d="true" />
</message>
```

Demnach sind Benutzername, Passwort, E-Mail-Adresse und Text im Klartext mitzulesen.

7.8.3 Bedrohungs-/Schadenspotential

Wie die Umfrage in Kapitel 10 ergeben hat, werden Passwörter gerne bei mehr als einem Konto benutzt. Das heißt wiederum, dass ein Angreifer oft nur ein einziges Passwort benötigt, um in viele weitere Konten des Ziels eindringen zu können. Software, die wie hier die Daten völlig unverschlüsselt überträgt, macht Angreife leicht.

[20] Download unter http://www.wireshark.org/

7.8.4 Lösung/Milderung des Problems

Im Fall von KIK Messenger hat der Anbieter nachgebessert – allerdings hat er dafür vom Veröffentlichen des Artikels im November 2010 bis zum Juni 2011 gebraucht, in dieser Zeit waren Usernamen, Passworte und Nachrichten im Klartext lesbar. Die Anweisung an Benutzer kann deswegen nur lauten, Passwörter nicht mehrfach zu verwenden und vertrauliche Informationen nicht über solche Dienste zu senden.

7.9 Firmeneigene Software nur für die Firma verfügbar machen

Eine Firma möchte eine interne Firmenapplikation auch nur den Firmenangehörigen zugänglich machen.

7.9.1 Ausgangsbasis/Situation

Welche Methoden stehen der Firma zur Verfügung um zu bewerkstelligen, dass nur Firmenmitarbeiter die App installieren können? Ausgangsbasis ist eine Firma mit 40 Anwendern und einer selbst erstellten Zeiterfassungsapplikation.

7.9.2 Angriff/Problematik

Windows Phone bzw. der Marketplace kennen neben der öffentlichen Aufnahme in den Marketplace noch zwei weitere Methoden, wie Software über den Marketplace vertrieben werden können, vgl. [94].

Tabelle 6 - Vertriebsmöglichkeiten des, Quelle: Eigene Darstellung nach [94]

	„Beta“	Private	Öffentlich
Anzahl an Benutzern	100	Unlimitiert	Unlimitiert
Kostenpflichtige Apps	Nein	Möglich	Möglich
Laufen ab?	Ja, 90 Tage	Nein	Nein
App aktualisierbar?	Nein	Ja	Ja
Zertifizierung der App?	Nein	Ja	Ja
Öffentlich entdeckbar (Suche)	Nein	Nein	Ja
Zugriffskontrolle	Ja, Live ID	Nein	Nein

Der öffentliche Verteilmechanismus ist der gewöhnliche Marketplace wo Applikationen gelistet sind. Der private Verteilmechanismus funktioniert so: nur der, der den Deep-Link auf die App kennt, kann diese Anwendung heruntergeladen werden. Der Beta Distribution Service sieht vor, eine Beta-Version einer Anwendung einer Gruppe bestimmter Nutzer verfügbar zu machen.

7.9.3 Bedrohungs-/Schadenspotential

Öffentliche Apps kann jeder herunterladen. Bei privaten Apps besteht die Sicherheit einzig darin, dass der Link „geheim“ ist, also letztlich aus keinerlei Sicherheit, außer, dass die App nicht in der Suche auftaucht. Der Beta-Mechanismus wiederum ist auf 100 Nutzer beschränkt und die Anwendung kann nicht aktualisiert werden, läuft dafür aber nach 90 Tagen ab.

7.9.4 Lösung/Milderung des Problems

Mangels Softwareverteilung wäre die mögliche Lösung, dass die Windows Phones entsperrt werden (siehe Kapitel 5.1) und die XAP-Dateien manuell und einzeln auf die Geräte gespielt werden. Die Geräte sind dann allerdings auch für den Benutzer offen, er könnte sich dann auch weitere Anwendungen installieren, die nicht über Marketplace zu beziehen sind, inklusive potentieller Malware. Jedes Update der Anwendung müsste wieder manuell eingespielt werden. Eine Bewertung kann hier nur lauten: lautet die Anforderung, dass eine App tatsächlich ausschließlich einem bestimmten Nutzerkreis zur Verfügung steht, dann ist Windows Phone derzeit nicht geeignet, weil es keine Methode gibt, die Installation einer App auf einen bestimmten Nutzerkreis zu beschränken. Alternativ kann die App in den Marketplace gestellt werden, muss dann jedoch einen weiteren Authentifizierungsmechanismus in der App selbst vorsehen. Im Falle der Firma in der Ausgangssituation mit der Zeiterfassungslösung würde das bedeuten, dass die App selbst noch Benutzernamen und Passwort abfragt.

7.10 Marketplace-Fallen für Benutzer

Auch wenn sämtliche Applikationen im Marketplace der Kontrolle von Microsoft unterliegen, heißt es dennoch für den Benutzer nicht, dass es keine „Fallen“ gäbe.

7.10.1 Ausgangsbasis/Situation

Wie in Kapitel 3.6 beschrieben sieht Microsoft für Käufe im Marketplace keinerlei Rückgabemodalitäten vor, es gilt „Gekauft ist gekauft“. Diesen Umstand machen sich Entwickler zu Nutze um in einem Graubereich den Benutzer zu täuschen.

7.10.2 Angriff/Problematik

Im Marketplace finden sich Anwendungen mit Namen wie „I’m rich“ oder gar „I’m super rich“, welche es in acht so genannten „Episoden“ gibt. Die gesamte Funktionalität dieser Anwendungen besteht darin, ein Bild anzuzeigen. Vermeintlich will diese Anwendung dem Benutzer eine Exklusivität vermitteln in Form von „Wer diese App hat, der hat Geld“. Angesichts des geringen Jahresbeitrags von 99 EUR für die Entwickler-Mitgliedschaft, die einen berechtigt Anwendungen in den Marketplace zu laden, und der sehr überschaubaren Funktionalität dieser Apps ist der Entwickler bereits ab dem ersten Kunden in der Gewinnzone.

Eine andere Methode Benutzer zur Installation von Anwendungen zu bringen besteht darin, für Apps ähnliche Namen erfolgreicher Software zu verwenden. Beispiel: statt dem beliebten Spiel *Angry Birds* gibt es auch eine App namens *Angry at the Birds*.

7.10.3 Bedrohungs-/Schadenspotential

Der maximal mögliche Einzelschaden beträgt 426,49 €, das ist der maximale Betrag, den eine App kosten darf. Eine Untergrenze, also der geringste Schaden, besteht darin, dass eine werbefinanzierte App durch den Benutzer gestartet wird, wonach kein direkter monetärer Schaden eintritt, sondern lediglich Kosten für die Internetnutzung zum Download der Werbung selbst anfällt – was vernachlässigbar ist.

7.10.4 Lösung/Milderung des Problems

Da diese Apps nichts direkt Illegales tun und eine offensichtliche Täuschungsabsicht zu beweisen schwierig erscheint, kann und will der Marketplace-Betreiber Microsoft nicht gegen diese Anbieter vorgehen. Die Lösung wäre ein Rückgaberecht, das zumindest für kurze Zeit dem Kunden die Möglichkeit gibt, einen Fehler wieder auszubügeln. Das ist jedoch derzeit nicht vorgesehen, deshalb muss der Kunde vor dem Kauf genauestens prüfen, ob die App auch wirklich jene ist, die gewollt ist.

7.11 Sprachsteuerung trotz gesperrtem Bildschirm

Die Bildschirmsperre bietet Sicherheit vor unberechtigter Nutzung, diese Sicherheit kann allerdings durch die Spracherkennung aufgeweicht werden.

7.11.1 Ausgangsbasis/Situation

Windows Phone lässt sich auch per Sprachbefehle steuern. Dazu ist die Windows-Taste gedrückt zu halten, das Phone wechselt damit in den Erkennungsmodus. Tabelle 7 listet Beispiele für Sprachbefehle.

Tabelle 7 - Beispiele für Sprachbefehle, Quelle: Eigene Darstellung

Sprachkommando	Beschreibung
„Ruf Max Mustermann an“	Person aus den Kontakten anrufen. Sind für diesen Kontakt mehrere Nummern gespeichert, dann kommt man zu einer Auswahlliste. Das lässt sich auch abkürzen, indem man gleich sagt „Ruf Max Mustermann auf dem Handy an“ oder “…bei der Arbeit an“.
„Ruf 55512345 an“	Um eine Nummer anzurufen, die nicht in den Kontakten geführt wird, kann man dem Phone diese auch Zahl für Zahl diktieren.
„Öffne App“	Mit „Öffne Anwendung“, also beispielsweise „Öffne Kalender“, wird die dazugehörige App gestartet.

7.11.2 Angriff/Problematik

In den Einstellungen zur Spracherkennung lässt sich einstellen, dass die Sprachsteuerung auch bei gesperrtem Handy zugelassen wird. Dies hat allerdings zur Folge, dass jeder, der physischen Zugriff auf das eingeschaltete Telefon hat, ohne den PIN Code zu benötigen telefonieren kann. Beispiel: Windows-Taste gedrückt halten und sagen „Ruf 0900...“.

7.11.3 Bedrohungs-/Schadenspotential

Der potentielle Schaden liegt bei den Kosten für Auslandsgespräche und Mehrwertnummern, die der unberechtigte Nutzer verursacht, bis zur Sperre der SIM-Karte. Da das Telefon ja über ein Standard-USB-Netzteil aufgeladen werden kann, stellt die begrenzte Akkulaufzeit keine Obergrenze dar.

7.11.4 Lösung/Milderung des Problems

Hierbei handelt durch den Benutzer vorgenommene unsichere Konfiguration. Die Sperre von Mehrwertnummern beim Telefonanbieter würde immer noch die Kosten für etwaige Auslandsgespräche auflaufen lassen. Deswegen kann vom Setzen der unsicheren Option

nur abgeraten werden. Gekoppelte Bluetooth-Geräte wie Freisprecheinrichtungen können allerdings auch Anrufe initiieren – damit wäre derselbe Angriff unabhängig von der Einstellung in der Sprachsteuerung wieder möglich.

7.12 Backup- oder Umzugsszenario

In vielen Bereichen ist es üblich, mittels einer Sicherung (Backup) einen vorherigen Zustand wiederherzustellen.

7.12.1 Ausgangsbasis/Situation

Der Benutzer möchte einen früheren Zustand wieder herstellen oder auf ein neues Telefon umziehen. Kann ein Backup erstellt werden? Kann dieses Backup auf ein anderes Gerät aufgespielt werden?

7.12.2 Angriff/Problematik

Windows Phone kennt kein Komplett-Backup, mit dessen man schnell und unkompliziert einen früheren Stand wiederherstellen könnte. Zwar wird beim Einspielen eines Systemupdates ein Backup gemacht (siehe Kapitel 4.14), allerdings ist das nur ein Notfalls-Backup, das auch nicht manuell zwischendurch angestoßen werden kann, sondern eben nur im Falle eines Systembackups automatisch angelegt wird. Zwischen dem letzten Update bzw. Systembackup und der gewünschten Wiederherstellung können Monate liegen. Die so erstellten Updates können nur auf demselben Endgerät eingespielt werden, für den Umzug auf ein anderes Endgerät kann das Backup nicht benutzt werden.

7.12.3 Bedrohungs-/Schadenspotential

Ein Teil der Daten ist gesichert bzw. liegen die Daten serverseitig. Das betrifft vor allem E-Mails, Kontakte und Kalender die auf Exchange oder einem Exchange-ActiveSync fähigen Server liegen. Die Notizen in der entsprechenden Notizenanwendung OneNote liegen – möglicherweise – auf SkyDrive. Gekaufte Apps können mit derselben Live ID jederzeit nochmal installiert werden.

Verloren gehen allerdings Fotos in der Originalauflösung und Videos genauso wie sämtliche Applikationseinstellungen, Konto-Einstellungen oder Spielstände. Die Wiedereinrichtung auf einem neuen Endgerät bedingt also, dass man sämtliche Konten wieder einrichtet und einzeln jede App aus dem Marketplace lädt.

7.12.4 Lösung/Milderung des Problems

Eine regelmäßige Synchronisierung ist Pflicht, wenn man einen aktuellen Stand der Fotos haben möchte. Einen bequemen Weg die Einstellungen und Anwendungen nach einem Reset oder bei einem neuen Gerät zu übernehmen, kennt Windows Phone nicht. Eine – allerdings nicht Endkunden-taugliche – Lösung besteht in der Verwendung von Homebrew-Software. Für den tatsächlichen Einsatz dieser Software ist jedoch abzuraten, da Microsoft Updates z.B. der Zune Software die Backups unbrauchbar machen können bzw. das Zurückspielen verhindern können [21].

[21] Eine solche Software findet sich unter: http://forum.xda-developers.com/showthread.php?t=1103011

7.13 Experiment: Unbekannter erlangt auf Facebook Freundesstatus

Für bestimmte Angriffe, ist es notwendig, vorab so viel wie möglich über eine Person in Erfahrung zu bringen, dazu bietet es sich natürlich an, in das Facebook-Profil des Ziels Einblick zu nehmen. Dieses Kapitel zeigt, wie eine völlig unbekannte, dritte Person Zugang zu den Facebook-Details eines Ziels bekommt, die sonst nur Freunden vorbehalten sind.

7.13.1 Ausgangsbasis/Situation

Der fiktive Angreifer ist dabei vorerst nicht mit dem Ziel auf Facebook befreundet. Um real in keine strafrechtlich relevanten Problemstellungen zu kommen, wurden als Ziele fünf Freunde des Autors ausgewählt, die zwar vorab nicht informiert wurden, bei Erfolg des Angriff wäre jedoch nicht mehr Information preisgegeben worden, als ohnehin schon durch die „Freundschaft“ auf Facebook dem Autor bekannt gewesen. Die Zielpersonen wurden abschließend informiert und befragt.

Ziel des Angriffs war es, „Freund“ der Person zu werden. Der Angriff gilt als erfolgreich, wenn die Freundschaftseinladung innerhalb von fünf Tagen angenommen wurde und Einsicht in die Timeline, die Fotos und persönliche Daten wie Geburtsdatum möglich waren.

7.13.2 Angriff/Problematik

Zeitraum des Angriffs war September 2011, zur Vorbereitung wurde die Facebook-Seite eines Freundes des Ziels besucht. Von dort wurde das Profilbild genommen und dann das Profil „kopiert“ – also ein neues Profil angelegt, das den Namen des Freundes und dessen Bild erhält. Facebook erfordert, dass neue Profile verifiziert werden und will hierzu eine SMS auf eine anzugebende Mobilfunknummer schicken. Für diesen Angriff ist ein verifizierter Account jedoch nicht notwendig. Die „Strafe“, die Facebook für nicht verifizierte Konten vorsieht, besteht darin, dass bei Aktionen wie Kommentaren, Freundschaftseinladungen oder „Gefällt mir“-Angaben ein so genanntes CAPTCHA zu lösen ist. CAPTCHA steht für „Completely Automated Public Turing test to tell Computers and Humans Apart“ und steht laut [95] „für einen Turing-Test, der Computer und Menschen unterscheiden soll”.

Der eigentliche „Angriff“ bestand dann darin, mit diesem neuen Profil eine Freundschaftsanfrage an das Ziel zu senden zusammen mit einer Nachricht mit diesem Inhalt: „Habe eine neues Profil, bitte bestätigen…“.

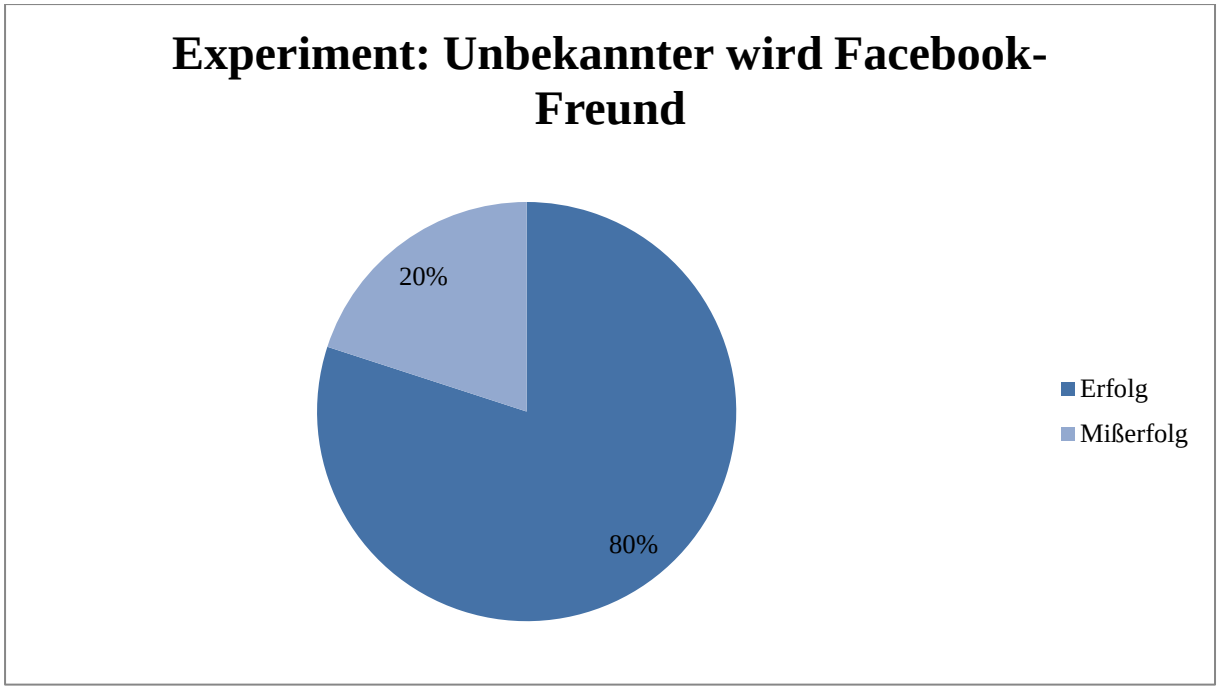


Abbildung 7 - Diagramm Experiment Facebookfreund

Ergebnis des Experiments: bei vier von fünf Zielen wurde die Freundschaftsanfrage innerhalb von zwei Tagen positiv beantwortet. Die fünfte Person antwortete innerhalb der Frist des Experiments von fünf Tagen nicht. Nach Aufklärung über die Hintergründe der Aktion wurden die „Opfer“ informiert und befragt. Die fünfte Person klärte auch auf, warum der Angriff nicht funktionierte: genau zu dem Zeitpunkt, als die Einladung des vermeintlichen Freundes über Facebook kam, saß der reale Freund direkt neben der Zielperson – hier hatte der Angreifer einfach Pech gehabt, wenige Minuten später oder früher und es hätte laut Zielperson auch in diesem Fall geklappt.

Den fünf Zielen wurde noch diese Frage gestellt: „Habt ihr zum Zeitpunkt der Freundschaftsannahme jemals nachgeprüft, ob das tatsächlich die vermeintliche Person ist?“.

Abbildung 8 - Diagramm Freundschaftsanfragen, Quelle: Eigene Darstellung

Durch das Ergebnis dieses Angriffs wird diese Fragestellung mit einem größeren Sample noch einmal aufgegriffen, siehe Kapitel 10.

7.13.3 Bedrohungs-/Schadenspotential

Der mögliche Schade ist hier der Verlust der Privatsphäre gegenüber Dritten, denen man sonst diese Einblicke nicht gegeben hätte. Daraus ergibt sich weitere Angriffsmöglichkeiten, z.B. Social Reengineering Attacken oder auch Stalking.

7.13.4 Lösung/Milderung des Problems

Ein echter Angriff hätte lediglich die zusätzliche Hürde aufgewiesen, dass man eventuell die Freundesliste nicht einsehen kann. Das wäre hier bei zwei von fünf Zielen der Fall gewesen. Hier müsste der Angreifer einen weiteren Schritt vornehmen und zuerst eventuelle Freunde oder Arbeitskollegen herausbekommen. Auch das dürfte kein Problem darstellen, einerseits kann man Suchmaschinen benutzen um auf Personen im Umkreis des Ziels schließen zu können. Man kann in weiteren sozialen Netzwerken wie z.B. XING oder Foursquare nachsehen – schließlich braucht man nur einen einzigen Namen, die Wahrscheinlichkeit den zu bekommen steigt natürlich mit der Anzahl der Netzwerke, die das Ziel aktiv nutzt. Aber auch Offline-Angriffe sind schnell und zeiteffizient durchzuführen, so kann man die Arbeitsstelle anrufen und bei der Telefonvermittlung nachfragen: „Ich hätte gerne den Kollegen von Hr. N.N. gesprochen, wie war doch gleich sein Name…“. Spätestens dann hat man einen Namen eines Kollegen, den man auf wiederum auf Facebook oder XING suchen kann und für diesen Angriff benutzen kann. Letztlich kann also dieser Angriff tatsächlich nur Abgemildert werden, wenn man tatsächlich vor einer Bestätigung einer Freundschaftsanfrage bei der betreffenden Person nachfragt.

8 Effizienz der Benutzeroberfläche von Windows Phone im Vergleich

Microsoft sieht die Oberfläche von Windows Phone als großen Pluspunkt. Ein eigener Test soll dies unterstreichen.

8.1 Vergleich in Schritten – Weniger ist mehr Sicherheit

Bei einem Schritt-für-Schritt-Vergleich soll in bestimmten Szenarien nachgewiesen werden, dass man mit Windows Phone weniger Einzelschritte benötigt, als bei vergleichbaren Systemen. Bezüglich der mobilen Usabilty sei es in Bezug auf die Sicherheit wichtig, angepasste Applikationen zu erstellen „die die nativen UI-Elemente des Phones nutzen“ [96].

Beispiel mit Extremen: aus Sicht der Usability wäre die beste Passwortlänge: Null. Aus diesem Grund haben Personen erst gar keine PIN-geschützte Bildschirmsperre auf ihrem Smartphone. Aus Sicht der Sicherheit müsste der PIN-Code unendlich lang sein.

Als Grundlage dient ein Vergleich mit anderen Systemen. Die These lautet: wenn zur Durchführung eines tagtäglichen Szenarios signifikant weniger Schritte als bei einem Vergleichssystem notwendig sind, dann ist dieses System mit hoher Wahrscheinlichkeit aus das sicherere.

Dieser im Juli 2010 erfolgte Vergleich wurde bei einem „Windows Phone Train-the-Trainer“-Training im Juli 2010 in Redmond, vgl. [97], vorgestellt und erfolgte zwischen einem Windows Phone 7, laufend auf einer Engineering Hardware (Samsung Taylor), einem iPhone 4 und dem auf Android 2.1 basierenden HTC Incredible mit HTC Sense Oberfläche. Der US-Test inkludierte außerdem auch ein RIM BlackBerry Modell (Storm 2) und ein Nokia-Gerät (N97), diese hatten jedoch für den lokalen Markt keine Bedeutung, da die Ausrichtung von Windows Phone 7 in der ersten Version rein auf den Endkonsumenten geplant war, während RIM und Nokia Smartphones auf den Business-Anwender zielen.

Zur Überprüfung wurde der Testaufbau im September 2010 lokal nachgestellt um die Ergebnisse zu verifizieren. Die lokale Verifizierung der Ergebnisse wurden mit einem leicht veränderten Setup durchgeführt. Als Windows Phone kam das LG GW910 zum Einsatz, bei Android ersetzte das HTC Desire das in Europa nicht erhältlich gewesene HTC Incredible. Beim iPhone 4 wurde dasselbe Modell gewählt. Es wurde darauf geachtet, dieselben Versionen einzusetzen, einzig bei Windows Phone ist das nicht der Fall gewesen, der ursprüngliche Test wurde mit einer Beta-Version des Betriebssystems gemacht, die Verifizierung dann mit der finalen Version von Windows Phone 7. Dies hatte allerdings keinen Einfluss auf den Test.

8.2 Erwartungshaltung

Erwartungshaltung war die Bestätigung der US Ergebnisse um die entsprechenden Werbebotschaften lokal in Österreich im Marketing verwerten zu können. Es sollte ein

deutlicher, messbarer und nachvollziehbarer Vorteil von Windows Phone gegenüber anderer Systeme nachweisbar sein.

8.3 Aufgabenstellung und Testszenarien

In drei verschiedenen Aufgabenstellungen rund um elementare Smartphone Themen soll der Vergleich gemacht werden. Diese Themen beinhalten „E-Mail und Kalender“, „Soziale Netzwerke“ und ein Szenario rund um „Suche und Karten“.

8.3.1 Szenario 1: E-Mail und Kalender

In diesem Szenario soll eine erhaltene E-Mail bzw. Einladung geöffnet werden. Eine Kontrolle im Kalender soll zeigen, ob die Besprechungseinladung in Konflikt mit einem bestehenden Termin steht. In diesem Fall soll eine neue Zeit vorgeschlagen werden.

Windows Phone iPhone Android

Abbildung 9 - Szenario 1 Schritt 1, Quelle: Bearbeitung nach [97]

Outlook-Kachel auswählen Mail-Icon auswählen Mail-Icon auswählen

Abbildung 10 - Szenario 1 Schritt 2, Quelle: Bearbeitung nach nach [97]

Zur Nachricht scrollen Posteingang anwählen Zur Nachricht scrollen

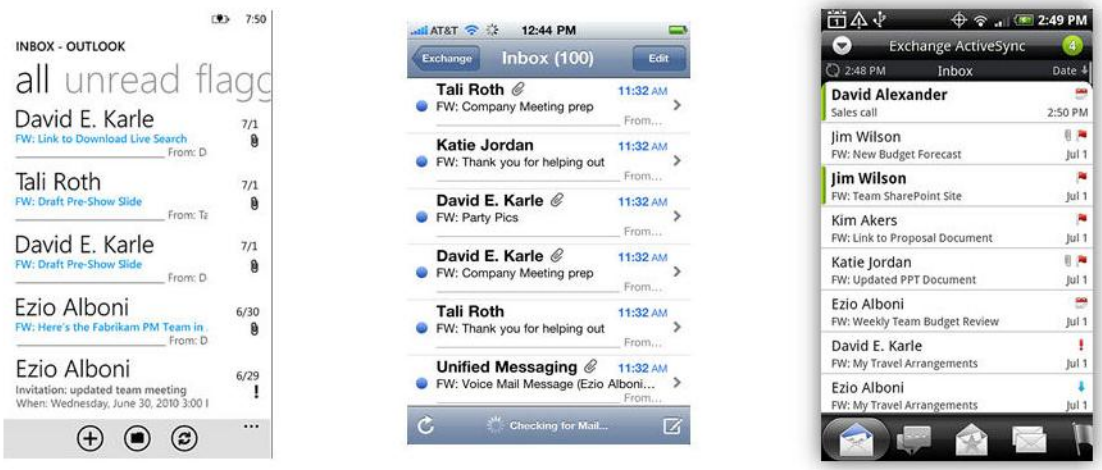


Abbildung 11 - Szenario 1 Schritt 3, Quelle: Bearbeitung nach [97]

E-Mail-Nachricht mit Einladung anklicken

Zur Nachricht scrollen

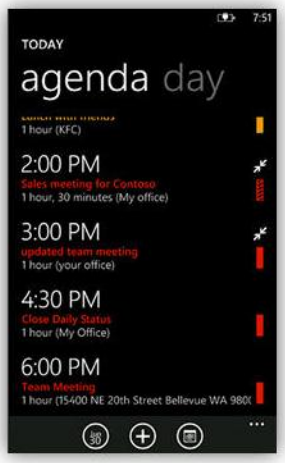
E-Mail-Nachricht mit Einladung anklicken

Abbildung 12 - Szenario 1 Schritt 4, Quelle: Bearbeitung nach [97]

Auf „Planungskonflikt anzeigen“ klicken

E-Mail-Nachricht mit Einladung anklicken

Zum Menü wechseln



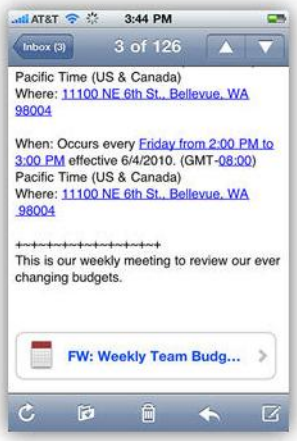


Abbildung 13 - Szenario 1 Schritt 5, Quelle: Bearbeitung nach [97]

Termin anklicken	Termin anklicken	Kalender anwählen

Abbildung 14 - Szenario 1 Schritt 6, Quelle: Bearbeitung nach [97]

Auf Antworten klicken	Hinunter scrollen	Entsprechenden Tag anklicken um alle Termine zu sehen

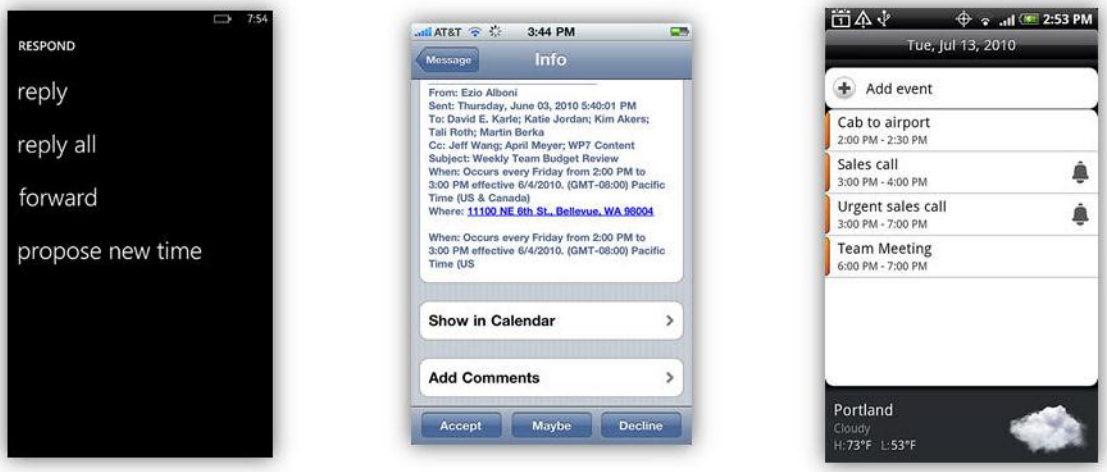


Abbildung 15 - Szenario 1 Schritt 7, Quelle: Bearbeitung nach [97]

„Neue Zeit vorschlagen“ anklicken

„In Kalender anzeigen“ anklicken

Zum Startmenü wechseln

Abbildung 16 - Szenario 1 Schritt 8, Quelle: Bearbeitung nach [97]

In das „Zeit“-Feld klicken

Blauen Pfeil anwählen

Mail Icon anklicken

Abbildung 17 - Szenario 1 Schritt 9, Quelle: Bearbeitung nach [97]

Neue Zeit einstellen „Einladung von“ anklicken Zur Nachricht scrollen

Abbildung 18 - Szenario 1 Schritt 10, Quelle: Bearbeitung nach [97]

Auf „Fertig“ klicken E-Mail anklicken E-Mail-Nachricht mit Einladung anklicken

Abbildung 19 - Szenario 1 Schritt 11, Quelle: Bearbeitung nach [97]

Auf senden drücken

Betreff eingeben

Zum Menü wechseln

Abbildung 20 - Szenario 1 Schritt 12, Quelle: Bearbeitung nach [97]

Damit ist Windows Phone fertig.

Drei weitere Schritte:

1. Nachricht anklicken
2. Nachricht schreiben
3. Senden drücken

13 weitere Schritte:

1. Neue Zeit vorschlagen
2. Startdatum anklicken
3. Vorgeschlagenes Datum ändern
4. Ok klicken
5. Startzeit anklicken
6. Vorgeschlagene Zeit ändern
7. Ok klicken
8. Endzeit anklicken
9. Vorgeschlagene Zeit ändern
10. Ok klicken
11. Nachricht eingeben

12. Menüknopf drücken
13. Senden

8.3.2 Auswertung und Beurteilung von Szenario 1

Basierend auf den Zahlen von Microsoft würde das Ergebnis lauten:

- Windows Phone: 11 Schritte
- iPhone: 14 Schritte
- Android: 24 Schritte

Es wurden Abweichungen festgestellt: bei Android und iPhone wurde extra noch eine Nachricht eingeben – das war bei Windows Phone nicht der Fall und ist auch nicht zwingend notwendig. Zusätzlich wurde bei Android auch das Datum eingegeben – das war nicht nachstellbar. Unter Berücksichtigung dieser festgestellten Abweichungen lautet das Ergebnis also:

- Windows Phone: 11 Schritte
- iPhone: 12 Schritte
- Android: 20 Schritte

Unter Berücksichtigung des aktuellen Entwicklungsstandes ist dieser Test nicht mehr aussagekräftig, da die größte Abweichung bei Android durch die damals fehlende Möglichkeit hervorgerufen wurde, Planungskonflikte anzuzeigen, wodurch hier die Mailapplikation verlassen werden musste um zwischenzeitlich in die Kalender-App zu wechseln.

8.3.3 Szenario 2: Soziale Netzwerke und Kontakte

In diesem Szenario soll von einem bestimmten Kontakt die letzte Neuigkeit angezeigt werden, anschließend soll der eigene Status bzw. die Statusmeldung auf Facebook neu gesetzt werden.

Windows Phone iPhone Android

Abbildung 21 - Szenario 2 Schritt 1, Quelle: Bearbeitung nach [97]

So der Kontakt an der Startseite angepinnt ist – fertig.

Facebook-Icon anwählen

Facebook-Icon anwählen

Abbildung 22 - Szenario 2 Schritt 2, Quelle: Bearbeitung nach [97]

Auf Kontakte klicken

Auf das Menü über der Kamera klicken

Auf Freunde klicken

Abbildung 23 - Szenario 2 Schritt 3, Quelle: Bearbeitung nach [97]

Von links nach rechts wischen (Geste) | Auf Freunde klicken | Zum Kontakt scrollen

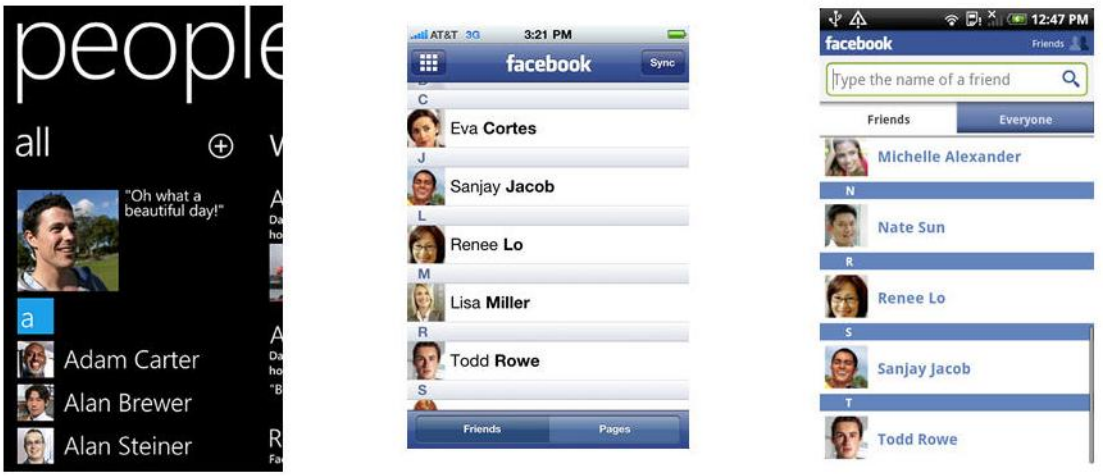


Abbildung 24 - Szenario 2 Schritt 4, Quelle: Bearbeitung nach [97]

Auf das eigene Bild klicken | Zum Kontakt scrollen | Kontakt auswählen

Abbildung 25 - Szenario 2 Schritt 5, Quelle: Bearbeitung nach [97]

In die Textbox klicken | Kontakt auswählen | Zurück-Knopf (Hardware) drücken

Abbildung 26 - Szenario 2 Schritt 6, Quelle: Bearbeitung nach [97]

Status eingeben | Auf Freunde drücken | Zurück-Knopf (Hardware) drücken

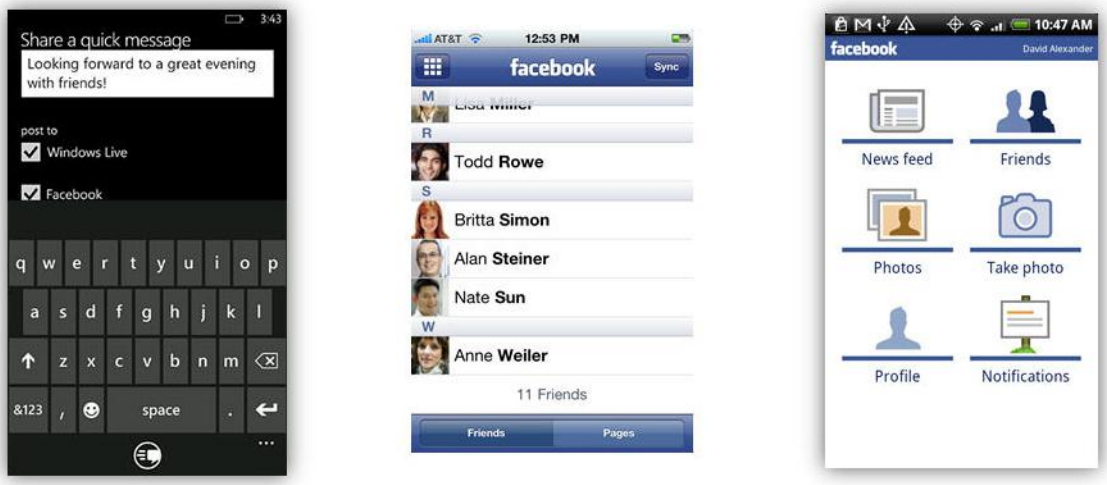


Abbildung 27 - Szenario 2 Schritt 7, Quelle: Bearbeitung nach [97]

Facebook auswählen bzw. in diesem Fall: Windows Live abwählen	Menü auswählen	Profil auswählen

Abbildung 28 - Szenario 2 Schritt 8, Quelle: Bearbeitung nach [97]

Senden	Auf News Feed klicken	In Textbox klicken

Abbildung 29 - Szenario 2 Schritt 9, Quelle: Bearbeitung nach [97]

Fertig.

Weitere drei Schritte notwendig:

1. In Textbox klicken
2. Status eingeben
3. Teilen drücken

Weitere zwei Schritte notwendig:

1. Status eingeben
2. Teilen drücken

8.3.4 Auswertung und Beurteilung von Szenario 2

Eine Besonderheit von Windows Phone macht hier den Vergleich schwer: das Herausziehen von einzelnen Personen auf die Startseite um hier Updates von dieser Person direkt anzuzeigen, ein so genanntes Live Tile. Dadurch ist die erste Aufgabenstellung sofort geschafft, unter der Voraussetzung, dass man in der Teststellung zulässt, dass der entsprechende Kontakt auf diese Art und Weise bereits auf die Startseite gelegt werden durfte. Wäre das nämlich nicht der Fall, würde sich der gesamte Test von den Schritten her nicht von dem des iPhones unterscheiden.

Microsoft kommt zu diesem Ergebnis:

- Windows Phone: 8 Schritte
- iPhone: 11 Schritte
- Android: 10 Schritte

Interessanterweise hat Microsoft an anderer Stelle auf die Eigenheiten des eigenen Systems nicht Bezug genommen, der Klick auf Kontakte um den eigenen Status zu setzen ist überflüssig, stattdessen hätte man gleich auf die „Ich“-Kachel klicken können, das hätte einen Schritt gespart. Unter Berücksichtigung dieser Optimierung lautet das Ergebnis:

- Windows Phone: 7 Schritte
- iPhone: 11 Schritte
- Android: 10 Schritte

8.3.5 Szenario 3: Suche und Karten

In diesem Szenario geht es darum, ein Restaurant auszumachen und sich dort hin leiten zu lassen. Das Restaurant soll einerseits aufgrund der Nähe gewählt werden, andererseits sollen in die Wahl die Bewertungen und Kritiken anderer Benutzer einfließen.

Windows Phone	iPhone	Android
		

Abbildung 30 - Szenario 3 Schritt 1, Quelle: Bearbeitung nach [97]

Klick auf Suche (Hardware-Taste)	Auf Safari klicken	Klick auf Suche (Hardware-Taste)
		

Abbildung 31 - Szenario 3 Schritt 2, Quelle: Bearbeitung nach [97]

Auf Suchfeld klicken	Auf Suchfeld klicken	Restaurants eingeben

Abbildung 32 - Szenario 3 Schritt 3, Quelle: Bearbeitung nach [97]

Restaurants eingeben Google.com eingeben Restaurants auswählen

Abbildung 33 - Szenario 3 Schritt 4, Quelle: Bearbeitung nach [97]

Restaurants auswählen Auf Go klicken Auf "Lokal" klicken

Abbildung 34 - Szenario 3 Schritt 5, Quelle: Bearbeitung nach [97]

Ein Restaurant aus der Liste wählen

Auf “Lokal” klicken

Auf Standort festlegen klicken

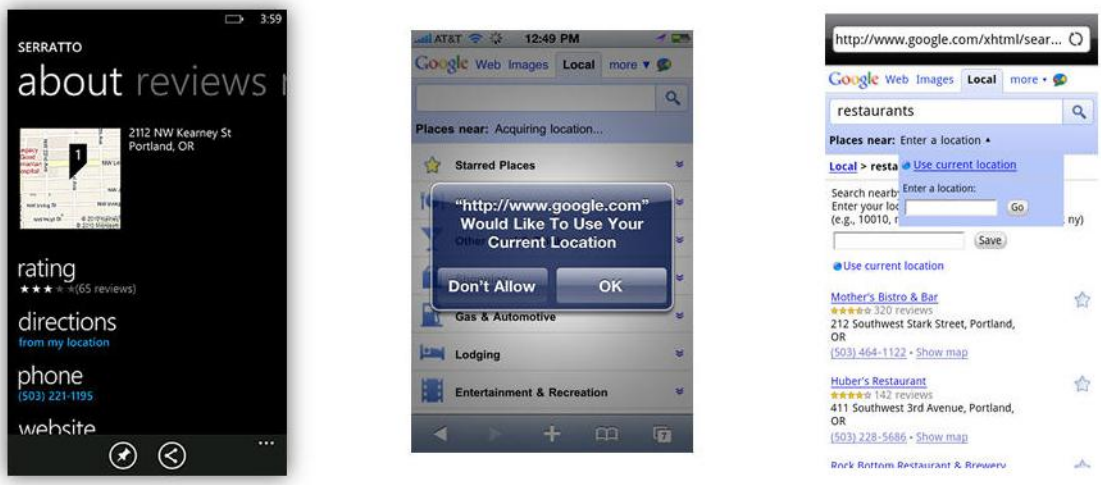


Abbildung 35 - Szenario 3 Schritt 6, Quelle: Bearbeitung nach [97]

Wischen um Kritiken anzuzeigen

Ok klicken um Standortdaten zu verwenden

Derzeitigen Standort auswählen

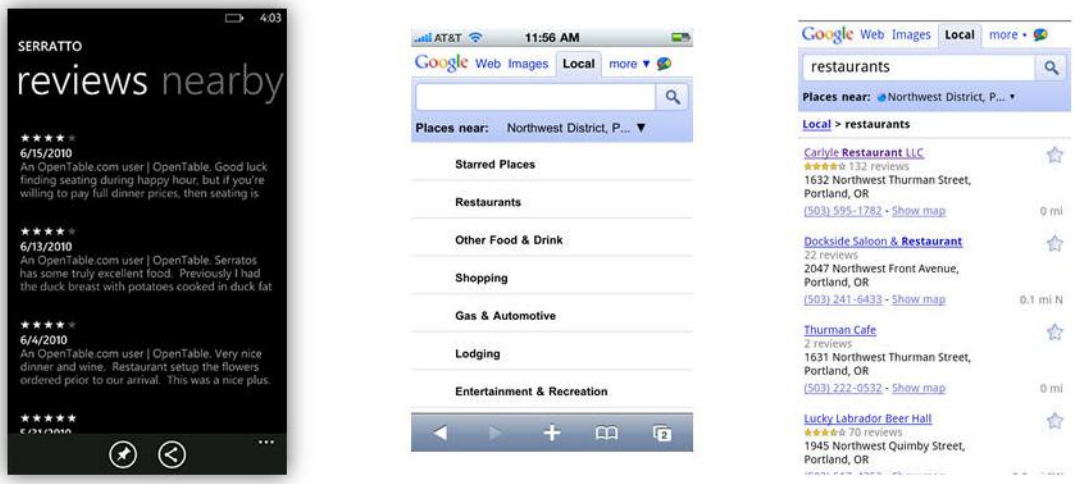


Abbildung 36 - Szenario 3 Schritt 7, Quelle: Bearbeitung nach [97]

Wischen um wieder zur Übersicht zu kommen

Auf Restaurants klicken

Auf gewünschtes Restaurant klicken

Abbildung 37 - Szenario 3 Schritt 8, Quelle: Bearbeitung nach [97]

Wegbeschreibung klicken um die Navigation zu starten

Art des Restaurants auswählen

Zu den Kritiken scrollen

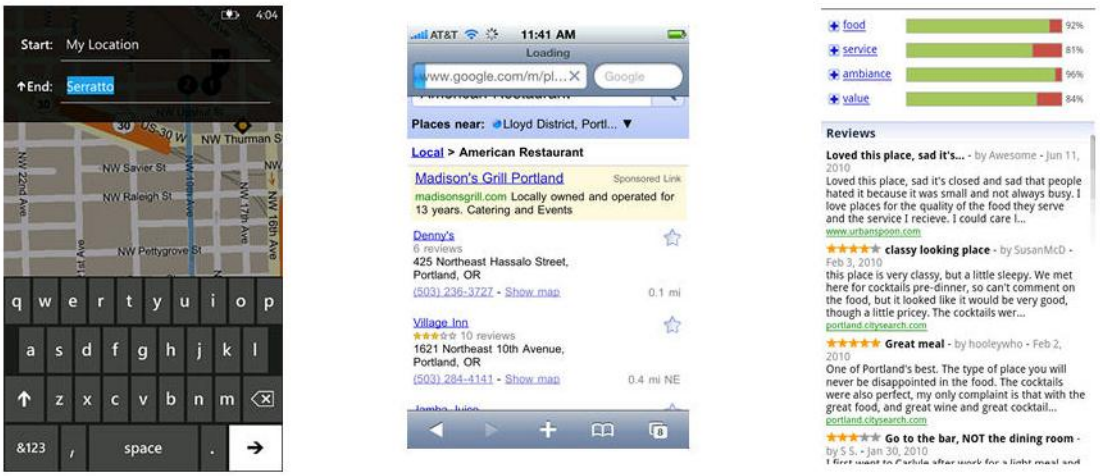


Abbildung 38 - Szenario 3 Schritt 9, Quelle: Bearbeitung nach [97]

Eingabetaste drücken

Auf gewünschtes Restaurant klicken

Wieder hinauf scrollen

Abbildung 39 - Szenario 3 Schritt 10, Quelle: Bearbeitung nach [97]

Auf 1 klicken um die erste Weganweisung anzuzeigen

Zu den Kritiken scrollen

Auf Karte klicken

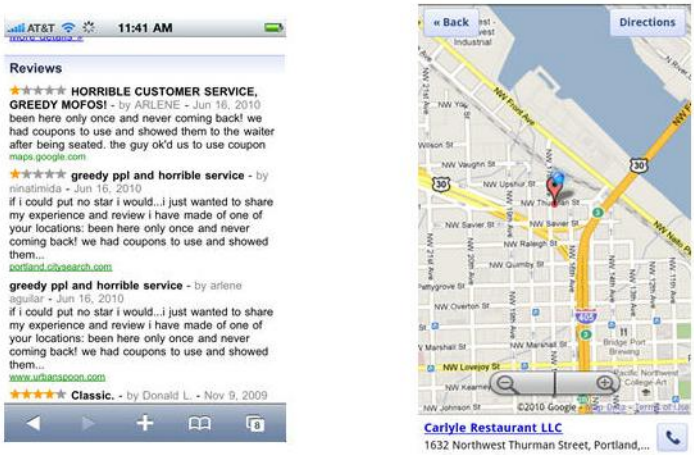


Abbildung 40 - Szenario 3 Schritt 11, Quelle: Bearbeitung nach [97]

Windows Phone fertig

Weitere 7 Schritte:

1. Wieder hinauf scrollen
2. Auf Karte klicken
3. Auf Routenplanung klicken um iPhone App zu starten
4. In Startfeld klicken
5. Jetzige Position angeben
6. Auf Weiter klicken
7. Auf Routenplan klicken

Weitere 3 Schritte:

1. Auf Routenplan klicken
2. Karten anklicken
3. Auf Routenplan klicken

8.3.6 Auswertung und Beurteilung von Szenario 3

Basierend auf den Zahlen von Microsoft würde das Ergebnis lauten:

- Windows Phone: 10 Schritte
- iPhone: 17 Schritte
- Android: 13 Schritte

Dieses Szenario konnte nicht nachgestellt werden bzw. lokal nicht nachgestellt werden. Es funktioniert bei Orten in den USA, nicht jedoch in Österreich. Microsoft greift bei den Location Based Services auf den Datenbestand von BING zu. In diesem kommt Österreich nicht vor, weswegen eine Suche nach einem Restaurant ohne Ergebnis endet.

- Windows Phone: Nicht geschafft.
- iPhone: 17 Schritte
- Android: 13 Schritte

Es müsste auf Windows Phone daher entweder eine spezielle Navigation-App verwendet werde, die lokale Informationen bereitstellt oder aber – wie hier auf den beiden anderen Systemen – auf Google zugegriffen werden. Dann ergibt sich allerdings kein Unterschied zu den Vergleichssystemen.

8.4 Erkenntnisse

Während der US-Test vielversprechend war, war die lokale Verifikation ernüchternd. Die Erwartungshaltung wurde nicht erfüllt.

- Release-Zyklen, speziell bei Android, sind schneller als jene von Microsoft. Der Test wurde im September 2010 nachgestellt, hier war schon die nächste Android Version verfügbar (2.2 „Froyo“), während der US-Test im Juli noch 2.1 „Eclair“ verwendet wurde. Wenig später, im Dezember 2010, veröffentlichte Google bereits 2.3 „Gingerbread“. Zum Vergleich Microsoft: hier hat es über ein Jahr gedauert, bevor nach Windows Phone 7.0 die Version 7.1 (Marketingversionsnamen: 7.5) folgte. Auch wenn es bei Android bedingt durch ein anderes Update-Modell dauernd kann, bis jeder Nutzer das Update zur Verfügung gestellt bekommt, müsste man sich ja dennoch auf die jeweils aktuellste Version berufen. Somit hätte ein Test zwar jeweils ein zum jeweiligen Zeitpunkt historisch korrektes Ergebnis, spiegelt aber nicht den realen oder „kaufbaren“ Zustand wieder, was die Verwendung solcher Vergleiche als Marketinginstrument einschränkt.
- Bei dem Test wurden nur mit dem System mitgelieferte Applikationen wie Browser oder Karten benutzt. Außer Acht gelassen wurde, dass Apps die gestellten Aufgaben eventuell besser erledigen können, das betrifft zum Beispiel die Suche nach einem Restaurant in Szenario 3. Auf Android oder iOS könnte man hier gleich spezialisierte Apps nutzen, was zu komplett anderen Ergebnissen führt.

- Die Auswahl der Szenarien hat ebenso eine massive Auswirkung auf das Ergebnis, was bei Beispiel 3 überdeutlich wurde: mit österreichischen Einstellungen ist das Szenario gar nicht zu schaffen. Die unterschiedliche Verfügbarkeit von Services (siehe dazu auch Kapitel 3.8) zwingt den Windows Phone Benutzer zumindest alternative Apps zu benutzen – oder den Browser, womit in Szenario 3 kein Unterschied zu anderen System wäre. Erkenntnis aus diesem Vergleich: Dort wo Aufgaben durch in Windows Phone tief integrierte Dienste erledigt werden können, kann eine höhere Effizienz nachgewiesen werden, als in den Vergleichssystemen. Geht das nicht, so ist entweder kein Vorteil messbar oder das Szenario als Ganzes nicht zu absolvieren.

Aus diesen Gründen wurde auf die weitere Verfolgung dieses Ansatzes für das lokale Marketing verzichtet, ein Vergleich der Systeme, vor allem auch in Hinblick auf „mehr“ oder „weniger“ Sicherheit im direkten Vergleich lässt sich so nicht erstellen.

9 Videogestützte Analyse zu Usability und Privatsphäre

Ortungsdaten gelten als besonders schutzwürdige, persönliche Daten, ließen sich doch mit diesen Daten Bewegungsprofile erstellen und daraus eine Menge aus dem persönlichen Leben rückschließen. Doch in wie weit schützt der Benutzer sich und beachtet entsprechende Hinweise, vor allem dann, wenn diese öfter auftauchen?

9.1 Setup

Der ursprüngliche Plan sah die in Abbildung 41 abgebildeten zehn gleich konfigurierte Endgeräte vor, die ident aufgesetzt, mit Kreditkarten und SIM-Karten ausgestattet wurden. Die Benutzer sollten dann das Szenario durchgehen, während sie von Videokameras gefilmt wurden.

Abbildung 41 - Vorbereitung für den ersten Testaufbau, Quelle: Eigene Darstellung

Doch gleich der erste Testlauf mit nur einem Benutzer hat verschiedene Schwierigkeiten ergeben:

- Einer Person, die keine Windows Phone Erfahrung hat, muss hin und wieder eine Hilfestellung gegeben werden um das Szenario zu beenden.
- Der Download von großen Applikationen (Spielen), wie ursprünglich vorgesehen, hätte zu lange gedauert.
- Verwendet wurde eine Camcorder zur Videoaufnahme, es gelang nicht, die Kamera so zu positionieren, dass jederzeit eine Sicht auf den Bildschirm gegeben war (z.B. wenn ein Foto gemacht wird) ohne den Benutzer merklich einzuschränken. Dazu wäre ein anderes Setup notwendig gewesen.

Aus diesen beiden Gründen würde die Benutzerbeobachtung umgestellt und hintereinander an vier Tagen mit einem Video-Out Gerät (LG GW910) durchgeführt. Änderungen am ursprünglichen Script bzw. Aufgabenstellung waren auch dadurch notwendig, weil am Video-Out-Gerät eine ältere Version des Betriebssystems lief (Windows Phone 7 Build 7004) und nicht Windows Phone 7.5. Ein Update für dieses Gerät war nicht verfügbar, es handelte sich bei GW910 um ein Betagerät der ersten Windows Phone Generation. Dadurch war kein Internet Explorer 9 installiert, der ebenso Ortungsdaten an Webseiten übermitteln kann. Dafür erlaubte das Video-Out-Gerät die

Umleitung des Videobilds auf einen PC. So konnten sich die Benutzer mit dem Phone fast völlig frei (am Sitzplatz) bewegen, das Telefon wurde mit einem USB-Kabel einen Laptop angeschlossen. Dieser PC diente dazu, dem Benutzer „über die Schulter zu sehen“, ohne dass dies für den Benutzer allzu angesehen wurde und damit das Testergebnis verfälscht. Somit konnten die für die Zeitmessung entscheidenden Handlungen mitverfolgt werden. Erleichtert wurde dies dadurch, dass in der Bildübertragung auch die Fingerberührung am Handybildschirm gezeigt werden, somit konnte sehr exakt gemessen werden, siehe Abbildung 41.

Abbildung 42 - Berührungen sind exakt sichtbar, Quelle: Eigene Darstellung

Die Messung selbst erfolgte auf einem dritten PC mittels Stoppuhr[22] - die so erzielten Werte wurden nach Beendigung in ein Excel-Sheet übertragen. Ein dritter Laptop schließlich zeigte in Richtung des Benutzers und zeigte den jeweils nächsten Schritt an, das wurde in PowerPoint realisiert.

Gemessen werden sollte die Zeit, die der Benutzer bei sichtbarem Hinweis zu den Ortungsdaten verbringt. Außerdem wird gemessen bzw. gezählt, wenn ein Benutzer bei dem Hinweis, dass eine App die Ortungsdaten nutzt, auf die Datenschutzbestimmungen klickt oder die Zustimmung verweigert. Das wäre vor allem beim letzten Schritt angebracht, wo eine Software heruntergeladen wird, die zwar nicht schädlich ist, aber aufgrund ihres Inhaltes eventuell nicht mit persönlicher Information gefüttert werden sollte. Bei der App handelt es sich um *Hangover Helper*, einer Software die Hilfestellung bietet, wenn man einen Kater hat. Will ein Benutzer einer solchen Software sogar mit

[22] http://www.online-stopwatch.com/split-timer/

aktueller Position mitteilen, dass er eventuell betrunken war, oder wäre hier mehr Privatsphäre angebracht?

Zum Vergleich werden die Benutzer in zwei Gruppen zu je fünf Personen eingeteilt. Beim Telefon konfiguriert waren bereits Sprache, Datum und Uhrzeit sowie Telefon- und Internetzugang. Ausschließlich bei der Gruppe 2 war die Nutzung von Ortungsdaten für Karten, Fotos und Suche bereits erlaubt. Ansonsten unterschieden sich die Gruppen nicht. Bei der Auswahl der Benutzer wurde darauf geachtet, dass keine Windows Phone Benutzer unter den Teilnehmern sind. Das hat hauptsächlich den Grund, dass die Ergebnisse nicht durch Vorkenntnisse verfälscht werden.

9.2 Aufgabenstellung

Dem Benutzer wurde vorab keine Einführung über Windows Phone gegeben, es ging los dem Verlesen dieses Textes: „Das ist wie besprochen eine Untersuchung über die Bedienung von Windows Phone. Du bekommst Aufgaben bzw. Szenarien gestellt, die Du erfüllen sollst. Lass Dir ruhig Zeit, es ist kein Wettbewerb. Nimm Dir die Zeit für jeden Schritt, den Du benötigst. Auch wenn wir Demodaten verwenden, gehe davon aus, es wäre Dein persönlicher Zugang, also deine E-Mail, dein Facebook-Konto und dergleichen. Wenn Dir ein Schritt nicht zusagt, so kannst Du diesen jederzeit ablehnen oder überspringen.“

Die Einzelszenarien, die dem Benutzer schrittweise über PowerPoint gezeigt wurden:

- E-Mail Konto einrichten: Richte Dir Dein E-Mail Konto ein!
- Benutzername Susi2011d@live.at Passwort FF452@70a (Daten in Form eines Demo Accounts wurden bereitgestellt, dieser Account war bei Windows Live und Facebook erstellt)
- Dein Telefon könnte verloren gehen, schau mal in den Einstellungen auf „Finde mein Telefon“.
- Kartenanwendung: wo liegt denn Fiji?
- Das Internet weiß mehr: Suche nach Fiji!
- Wer Urlaub macht, muss auch Fotos machen – schieße ein Foto.
- Wer zu viel Urlaub macht, braucht „Hangover Helper“. Lade diese App herunter.

Die Anzahl an Schritten, die in jedem Szenario zu erledigen sind, ist unterschiedlich, weil es mehrere Wege gibt, die jeweiligen Aufgabenstellungen zu lösen.

9.3 Erwartungshaltung

Es wird erwartet, dass kein Benutzer auf die Datenschutzbestimmungen bei der Einrichtung von Konten klickt. Bezüglich der Ortung lautet die Erwartungshaltung: bei fünf Mal derselben Abfrage wird nicht mehr auf diese Warnung oder den Hinweis geschaut, sondern völlig automatisch weggeklickt. Bei weniger Meldungen wird vermutet, dass die Meldung bei der App aus dem Marketplace mehr Gewicht hat und länger über die Konsequenzen nachgedacht wird.

9.4 Auswertung

Betrachtet man die Gruppe eins, so sieht man folgende Verteilung:

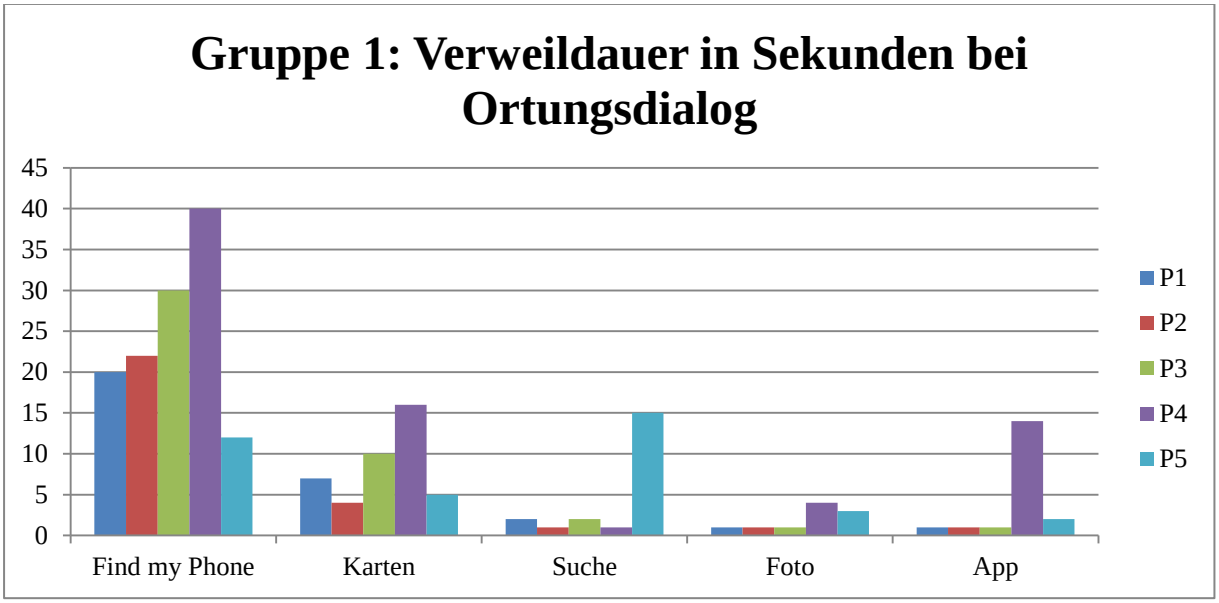


Abbildung 43 - Diagramm Verweildauer Gruppe 1, Quelle: Eigene Darstellung

Wie man in der Auswertung erkennen kann: spätestens bei der dritten gleichlautenden Abfrage ist es mit der Überlegung vorbei. Eine einzige Person war der Ortungsthematik generell skeptisch und hat zwei der Ortungsanfragen negativ beantwortet.

Bei der Einzelauswertungen in der Gruppe 2, wo bei Karten, Suche und Fotos die Ortungsabfrage nicht kam, weil sie vorab schon akzeptiert wurde, sieht man eine deutliche stärkere Beschäftigung mit dem letzten Szenario, höher sogar als beim zweiten Szenario der ersten Gruppe 1.

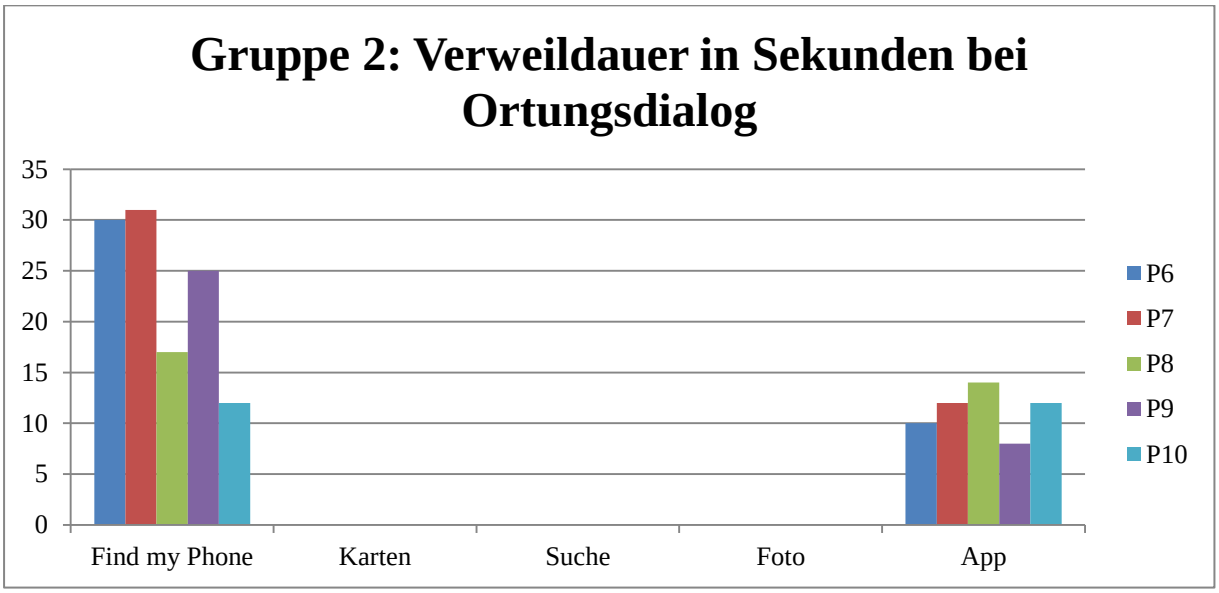


Abbildung 44 - Diagramm Verweildauer Gruppe 2, Quelle: Eigene Darstellung

Im direkten Vergleich das erste und das letzte Szenario anhand der Durchschnittswerte der Gruppen 1 und 2:

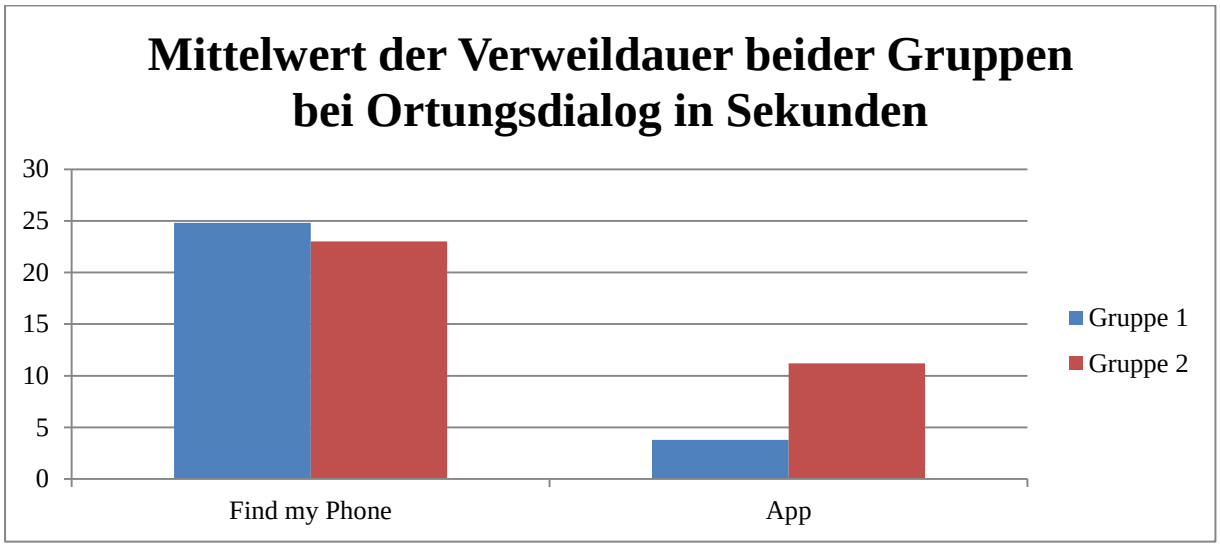


Abbildung 45 - Diagramm Mittelwert Verweildauer, Quelle: Eigene Darstellung

Während bei der ersten Frage die beide Gruppen mit 24,8 und 23 Sekunden nahezu idente Ausgangswerte haben, so ist der Unterschied beim letzten Szenario deutlicher: hier sind es 3,8 Sekunden zu 11,2.

9.5 Erkenntnisse

Die Erwartungshaltung erfüllt, ein mehr an Warnungen oder Hinweisen führt nicht zu erhöhter Aufmerksamkeit. Zwar war die Aufmerksamkeit bei der zweiten Gruppe signifikant höher, das hat jedoch nicht dazu geführt, dass im Rahmen des Szenarios der Applikation die Ortung verweigert worden wäre. Somit kann in diesem Test zwar festgestellt werden, dass sich die Benutzer bei weniger Warnungen länger mit einzelnen Hinweisen beschäftigen, aber zumindest in dieser Teststellung dennoch wie die Vergleichsgruppe die App installieren.

Als Verbesserung empfiehlt sich, dass eine zentrale Übersicht seitens Microsoft implementiert wird, woraus ersichtlich ist, welche Anwendungen auf dem Phone nun beispielsweise Zugriff auf die Ortungsdaten haben, eine solche Ansicht fehlt.

10 Umfrage zum Verhalten

Diese Umfrage soll klären, in wieweit Benutzer durch ihr Verhalten das Sicherheitsniveau beeinflussen.

10.1 Setup

Die Umfrage wurde intrawebbasiert über Microsoft SharePoint Server 2010 durchgeführt, dieser bietet im Rahmen von so genannten Teamseiten die Möglichkeit an, eine Umfrage mit verschiedenen Antwortmöglichkeiten und Excel-Export der Resultate zu erstellen. Dadurch, dass jeder Umfrageteilnehmer über Active Directory authentifiziert war, konnte

ausgeschlossen werden, dass jemand mehrfach an der Umfrage teilnimmt. Dennoch wurden die Umfragedaten anonym erhoben, wenngleich zumindest „eine Person mit erhöhten Rechten den entsprechenden Benutzer identifizieren könnte“ [98]. Durchgeführt wurde die Umfrage in einem mittelständischen IT-Unternehmen mit 350 Mitarbeitern. Dieses Unternehmen stellt seinen Mitarbeitern Windows Phone als Arbeitsgerät zur Verfügung und eignete sich dadurch für diese Untersuchung, die erforderte, dass die Teilnehmer Windows Phone aktiv benutzen.

Die Umfrage sollte 100 Antworten bringen und nach Erreichen dieser Zahl geschlossen werden. Zur Teilnahme wurde mittels Rundmail aufgefordert, als Anreiz wurde die Verlosung eines Windows Phones (HTC Trophy) geboten. Nach Abschluss der Umfrage gab es ein weiteres, optionales Formular auszufüllen, wo man sein E-Mail Adresse zur Verlosung des Phones eingeben konnte, dieses speicherte in eine separate, von der Umfrage getrennte Liste.

Aussendung der E-Mail war am 12.09.2011, eine Erinnerung erfolgte eine Woche später am 19.09.2011. Die Zahl n=100 wurde am 22.09.2011 erreicht.

10.2 Aufgabenstellung

Die Teilnehmer konnten die Umfrage in einem Browser durchführen, insgesamt waren 13 Fragen zu beantworten:

- Q1: Männlich oder weiblich?
- Q2: Ist dein Job eher technisch oder nicht-technisch?
- Q3: Bist Du auf Facebook?
- Q4: Wenn Du auf Facebook bist: Schon mal nachgeprüft, ob eine Freundschaftsanfrage wirklich von dieser Person und nicht von jemandem anderen (Fake-Profil, Bösewicht) kommt?
- Q5: Wohnen Kinder im Alter jünger als 6 Jahre in Deinem Haushalt?
- Q6: Wohnen Kinder im Alter zwischen 6 und 10 in Deinem Haushalt?
- Q7: Wohnen Kinder im Alter zwischen 11 und 15 in Deinem Haushalt?
- Q8: Wohnen Kinder älter als 15 Jahre in Deinem Haushalt?
- Q9: Speicherst Du GPS Daten in Bildern?
- Q10: Stellst Du Bilder auf Facebook?
- Q11: Benutzt Du ein Passwort bei als einem Konto, also z.B. bei Amazon und eBay?
- Q12: Weiß ein Familienmitglied oder Dein Partner den PIN Code Deines Windows Phones?
- Q13: Wenn ja, warum?

Alle Fragen waren geschlossene Auswahl-Fragen, deren Beantwortung erforderlich war, die Antworten wurden mit den Werten 1 und 0 gespeichert. Eine Ausnahme bildete nur die letzte Frage, hier handelte es sich um eine offene, optionale Frage, die mit freiem Text zu beantworten war.

10.3 Erwartungshaltung

Es werden verschiedene Fragen zum Verhalten gestellt, so wird erwartet, dass der überwiegende Teil der Teilnehmer auf Facebook ist und diese auch zum Fotoupload nutzt. Außerdem wird der in Kapitel 7.13 beschriebene Angriff nochmals mit dem höheren Sample geprüft, erwartet wird hier eine Bestätigung, dass dieser Angriff eine hohe Erfolgswahrscheinlichkeit hat. Zudem wird erwartet, dass es in Familien mit Kindern eher zu einer familieninternen Weitergabe des Passwortes kommt, als bei Personen, die in Haushalten ohne Kinder leben.

10.4 Auswertung

Die Teilnehmer der Umfrage verteilen sich ungefähr zu gleichen Teilen auf männliche und weibliche Teilnehmer, es entfallen auf 45% weibliche Teilnehmer und 55% auf männliche. Ein Unterschied ist allerdings bei der Einstufung der eigenen Jobs zu sehen, so sehen sich mit 74,5% deutlich mehr Männer in einem technischen Beruf als Frauen mit 28,9%.

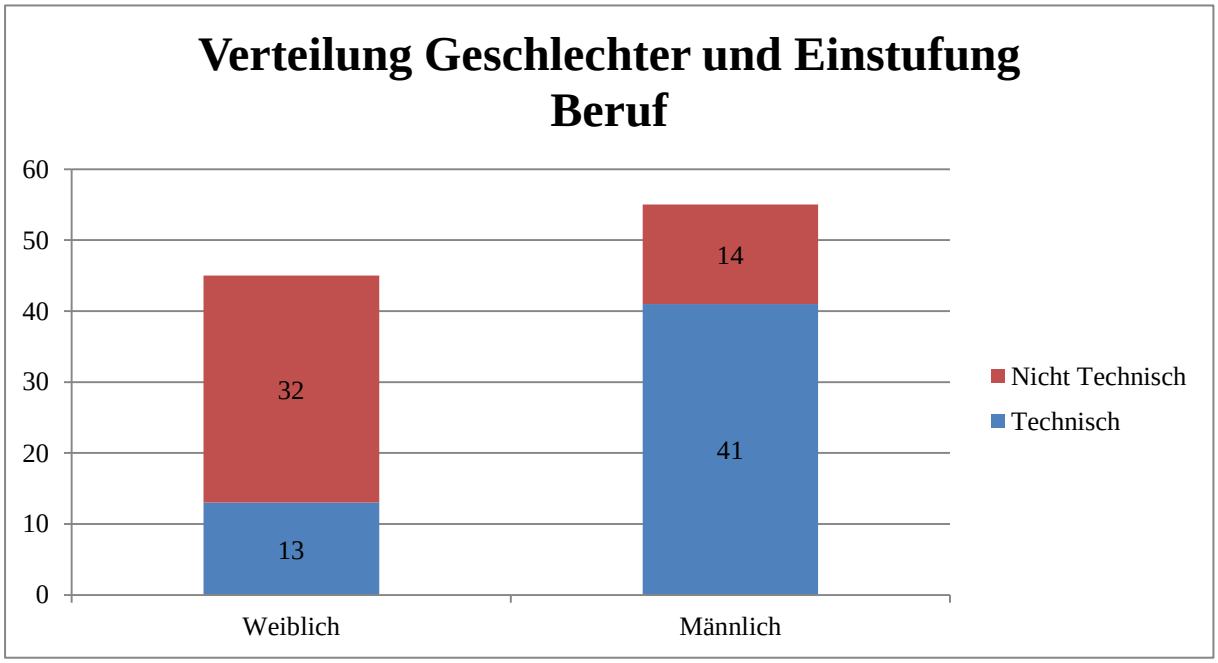


Abbildung 46 - Diagramm Geschlechterverteilung, Quelle: Eigene Darstellung

75% der Teilnehmer befinden sich auf Facebook, davon stellen 85,3% auch Bilder auf Facebook. Bezüglich der Überprüfung des Experiments aus Kapitel 7.13 ergab sich das in Abbildung 47 ersichtliche Bild.

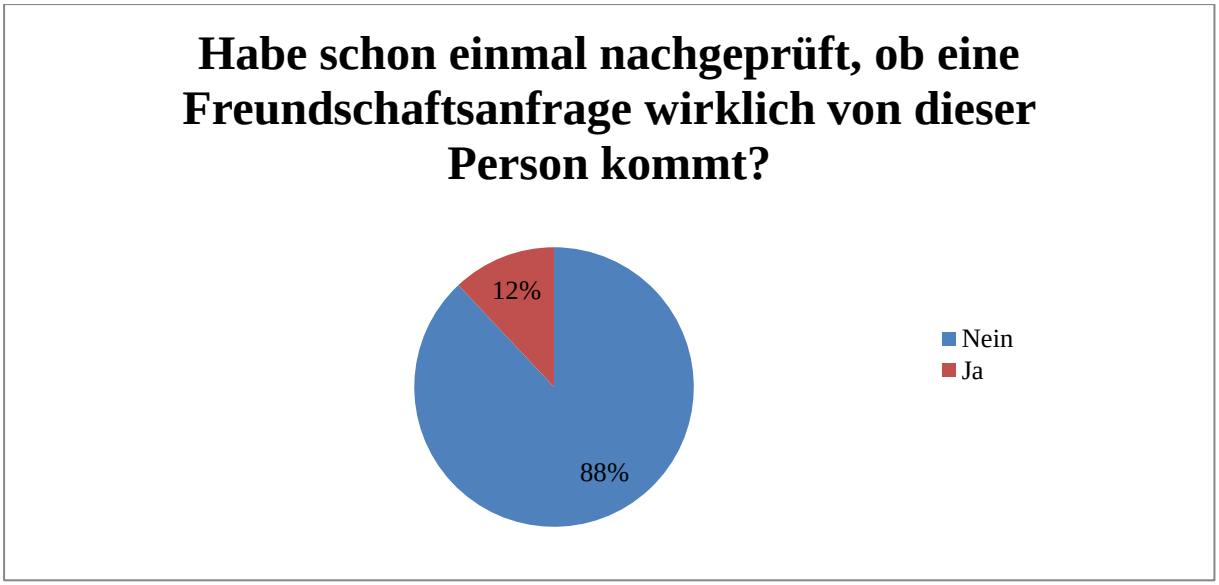


Abbildung 47 - Diagramm Nachgeprüfte Anfragen , Quelle: Eigene Darstellung

Immerhin 12% der Facebook-Benutzer (neun in absoluten Zahlen) geben an, dass sie bereits einmal nachgefragt haben, ob eine Person wirklich jene ist, die sie vorgibt zu sein.

Bezüglich des Verhaltens bei Passwörtern konnte festgestellt werden, dass 65% der Teilnehmer Passwörter mehrfach nutzen, also bei verschiedenen Dienstleistern dasselbe Passwort Verwendung fand. Bei mehr als einem Drittel der Befragten wusste ein Familienmitglied den PIN-Code des Windows Phones.

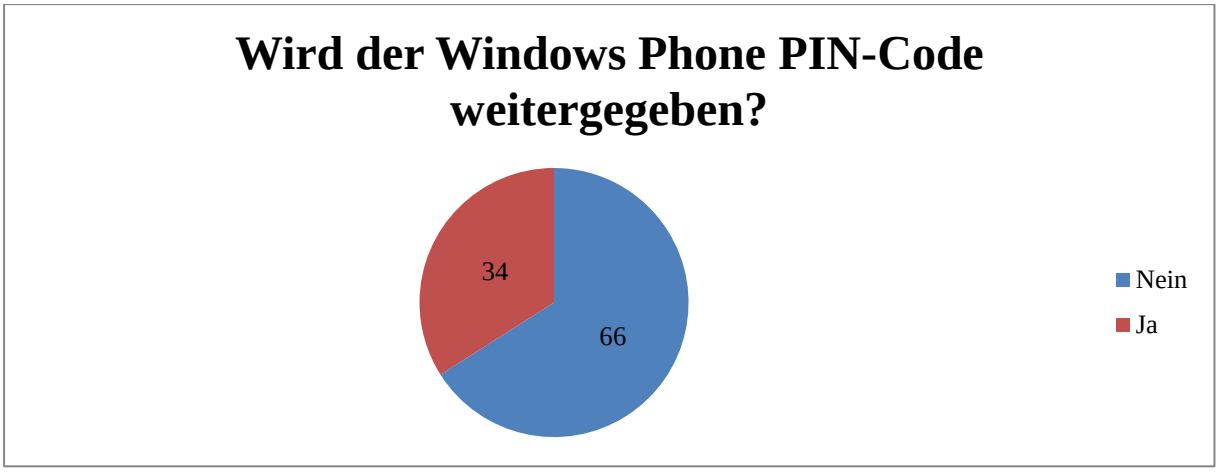


Abbildung 48 - Diagramm PIN-Code Weitergabe, Quelle: Eigene Darstellung

Die sich daraus ergebende Vermutung war, dass das mit den Kindern zu tun hat. Tatsächlich ergibt die Aufsplitterung folgendes Bild:

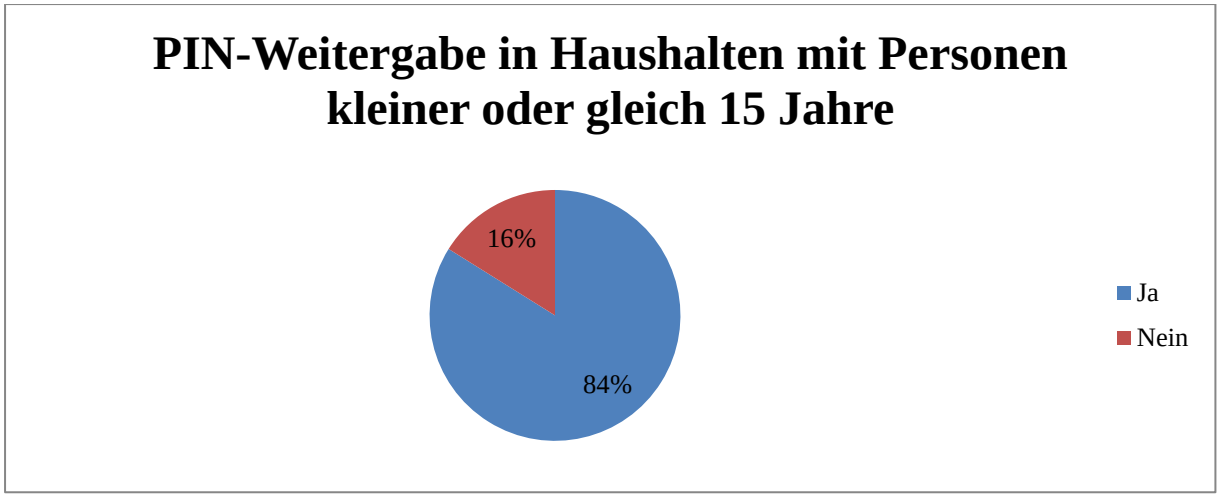


Abbildung 49 - Diagramm Haushalten mit Kindern, Quelle: Eigene Darstellung

Leben im Haushalt Kinder mit oder unter 15 Jahren, was bei 31 der Haushalten der Fall war, so erfolgte hier zu 83,9% eine Weitergabe des PIN-Codes.

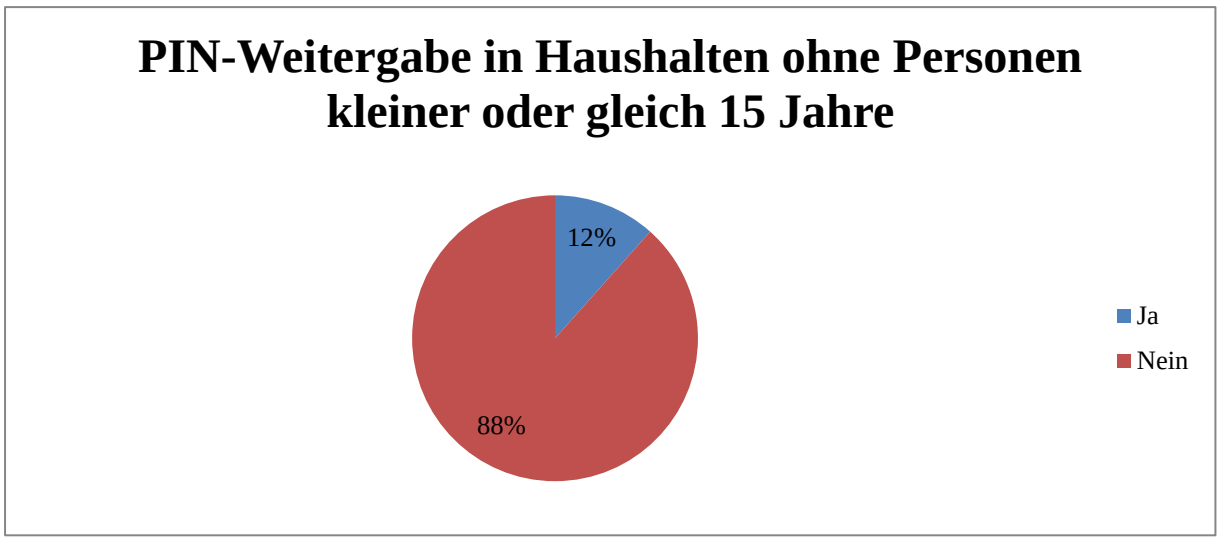


Abbildung 50 - Diagramm Haushalten ohne Kinder, Quelle: Eigene Darstellung

Bei den 69 Haushalten ohne Personen mit oder unter 15 Jahren zeigt sich ein nahezu umgedrehtes Ergebnis, hier erfolgte die Weitergabe zu 11,6%, aber 88,4% geben den PIN-Code nicht weiter.

10.5 Erkenntnisse

Teils wurde die Erwartungshaltung erfüllt, die Frage nach der Überprüfung von Freundschaftsanfragen lagen im Bereich der Erwartung, ebenso die Teilnahme an Facebook selbst, hier war der Wert mit 75% eventuell sogar niedrig, dafür wurde bei der Nachprüfung, ob eine Anfrage tatsächlich von dieser Person kommt, sogar ein schlechterer Wert erwartet. Dennoch kann auch hier festgestellt werden, dass ein Angriff, um den Freundschaftsstatus zu erreichen, mit 88% eine sehr hohe Erfolgswahrscheinlichkeit ausweist.

Allerdings wurde die Erwartungshaltung bezüglich der Passwort- bzw. PIN-Weitergabe bei weitem übertroffen. Mit einem Ergebnis von über acht von zehn Personen, die den PIN-Code weitergeben, wurde nicht gerechnet. Um dieses Ergebnis abzusichern wurden dann noch zusätzliche Stichprobengespräche und Interviews mit Mitarbeitern mit Kindern geführt. Diese bestätigen das erhobene Bild und zeigen, dass die Implementierung der EAS-Richtlinien (siehe Kapitel 4.4) in dem Unternehmen, wo die Umfrage durchgeführt wurde, dieses Verhalten ausgelöst hatte, allerdings erst mit folgenden zusätzlichen Umständen:

- Windows Phone ist zum Spielen geeignet, es gibt auch kindertaugliche bzw. für Kinder reizvolle Spiele.
- Vor dem Löschen gibt es keinerlei Warnung oder Kindersicherung.
- Es gibt keine Backup-Möglichkeit, das Wiedereinrichten ist ein zeitraubender und mühsamer Prozess, da jede einzelne Applikation erneut heruntergeladen werden muss und sämtliche Einstellungen sind erneut zu treffen.

Es wurde hier also beobachtet, wie eine zu strenge Richtlinie statt mehr Sicherheit zu liefern, das komplette Gegenteil erreicht, nämlich, dass kleine Kinder den PIN-Code für das Smartphone haben und damit den Zugang zu Unternehmensressourcen und auch vertraulichen, möglicherweise sogar IRM-geschützten Dokumenten (siehe Kapitel 4.7). Im Extremfall könnte dies sogar eine Gefahr für Leib und Leben der Kinder bedeuten.

Mögliche Lösungen um diesen Umstand zu verbessern könnten darin bestehen, dass Microsoft zumindest eine Tippsperre implementiert, die das Löschen durch Kinder („wild drauf los tippen“) entschärft. So könnte beispielsweise nach dem zweiten Fehlversuch ein Wort eingegeben werden oder eine Rechnung gelöst werden, erst dann darf der letzte Code versucht werden.

Eine andere, vermutlich jedoch aufwändigere Änderung der Systemarchitektur könnte einen sicheren „Unternehmens- und Berufsteil“ im Smartphone vorsehen, der einen speziellen Zugang mit PIN benötigt und einen ungesicherten Teil, wo Spiele zugänglich sind.

Für das Unternehmen, das hier untersucht wurde, könnte eine kurzfristige Lösung sein, Mitarbeitern mit Kindern eigene Phones für die Familie im Rahmen einer vergünstigten Mitarbeiteraktion zur Verfügung zu stellen. Das könnte den Prozentsatz der Personen, die das Passwort weitergeben, senken.

Für weitere Untersuchungen wäre noch Raum z.B. haben die Stichprobengespräche offenbart, dass es nicht zwingend die Kinder sind, die den PIN wissen, sondern auch der Partner, der den Code dann für die Kinder eingibt („Sonntags mal länger schlafen“). Außerdem könnte das Alter der Kinder exakter erfasst werden, die Abstände der Altersstufen hier sind groß, eine Präzisierung könnte hier eine detaillierte Übersicht geben. So wird ein zweijähriges Kind den PIN vermutlich nicht wissen, ein 13 Jahre altes Kind wird schon ein eigenes Mobiltelefon haben. Eine weitere Fragestellung könnte

untersuchen, ob sich dieses Verhalten auch auf andere Bereiche der IT auswirkt. Wissen die Kinder z.B. auch den das Passwort für den Firmen-PC oder ist so ein Verhalten nur bei Mobiltelefonen zu beobachten?

11 Kinderschutz

Basierend auf den Erkenntnissen aus Kapitel 10.5 war die Folgefrage: wenn Kinder Windows Phone gerne nutzen, kann dieses überhaupt für die Nutzung von Kindern eingerichtet werden?

11.1 Setup

Microsoft kennt bei einzelnen Produkten und Services Jugendschutzeinstellungen, so zum Beispiel ist in Windows 7 ein Jugendschutzsystem inkludiert, das Zeitlimits und Applikations-White- sowie Blacklists erlaubt. Bei Spielen kann außerdem auf Rating-Systeme zurückgegriffen werden.

Darüber hinaus kann dieses System mit den Windows Live Essentials erweitert werden. Das ist Softwarepaket, dass die Funktionalität von Windows für Windows Live ID Benutzer durch zusätzliche Programme erweitert, etwa um einen Chat-Client (Windows Live Messenger) oder ein eigenes E-Mail-Programm (Windows Live Mail). Dieses Paket enthält auch die Family Safety. Damit kann man beispielsweise Freundeslisten der Kinder verwalten, diese können dann nur noch mit vorher genehmigten Kontakten per Windows Live Messenger chatten oder über Windows Live Hotmails E-Mails austauschen. Ebenso kann der Web-Verkehr mitgeloggt und kontrolliert werden. Vergleichbare Einstellungen finden sich in Zune (Alterfreigabe für Videos) und Xbox Live (Spiele und Marketplacezugang).

11.2 Aufgabenstellung

Ausgangsbasis war folgendes Szenario: Ein Elternteil möchte für seine sechs Jahre alte Tochter ein Windows Phone so präparieren, dass eine altersadäquate Nutzung oder zumindest ein Schutz vor Pornographie oder Gewaltspielen möglich ist. Dazu wurde für eine neue Eltern-Windows Live ID angelegt und anschließen über Windows Live Family Safety *fss.live.com* eine Kinder Live ID hinzugefügt. Für diese Live ID sollen bestimmte Rechte und Einschränkungen definiert werden, so sollen für Spiele- und Filme erlaubt werden, die eien Freigabe von 3+ Jahren aufweisen. Im Web soll *www.disney.de* erlaubt sein. Bei Kontakten sind lediglich die Eltern für Chat- und E-Mailverkehr zu gestatten. Es gilt als Erfolg, wenn diese Einschränkungen eingehalten werden.

11.3 Erwartungshaltung

Die Erwartungshaltung war, dass diese Einschränkungen auf Windows Phone durch die starke Bindung auf die Windows Live ID eingehalten werden, zumal Microsoft schon jahrelange Erfahrung im Umgang mit jüngeren Spielern auf der Xbox sammeln konnte.

11.4 Auswertung

Es darf stark in Zweifel gezogen werden, ob der durchschnittliche und unter Umständen nicht technik-affine Benutzer schafft die richtigen Schritte zu finden. Die Jugendschutzeinstellungen können an sechs verschiedenen Stellen erstellt und geändert werden:

- Xbox 360 (Konsole)
- *Xbox.com* (Browser)
- Zune Software
- *Zune.net* (Browser)
- Windows 7 (wenn das Konto mit einem Benutzerkonto auf einem PC verbunden ist, auf dem Family Safety Settings installiert sind)
- Family Safety *fss.live.com* (Browser)

Hierbei überschneiden sich manche Einstellungen („Erlaube Marketplace Zugang"), wogegen manche allerdings völlig unabhängig voneinander sind (z.B. Zeitlimits am Windows-PC sind unabhängig von jenen auf der Xbox). Trotz Kinder-Live ID war der Zugang zum Browser uneingeschränkt, ebenso der Videoplayer, eine erotische Site mit HTML5-basierten Videos konnte abgerufen und abgespielt werden. Auch der Mail-Client hat ohne Einschränkung E-Mails an nicht-erlaubte Adressen verschickt. Ebenso möglich war der Zugang zum Marketplace, inklusive der Ansicht von Screenshots der Applikationen. Die Installation der Apps schlug allerdings fehl – hier griffen die Einstellungen von *Xbox.com* bzw. der Zune Software, wo der Marketplacezugang eingeschränkt werden konnte.

Zune weist in der Hilfe auf ein Bewertungssystem hin, demnach Spielefreigaben geblockt werden können und spricht dort vom „Freigabestandard: Pan-European Game Information (PEGI)" [99] , mit dem man Spiele über den Marketplace zwar zulassen kann, aber nur dem Alter entsprechend. Dieses Pan European Game Information (PEGI) wird von Xbox, Zune, Windows 7 und Family Safety unterstützt. Die Eigendefinition laut PEGI [100]: „Das System der Altersempfehlungen soll sicherstellen, dass bei Unterhaltungsmedien wie Filmen, Videos, DVDs und Computerspielen deutlich angegeben wird, für welche Altersgruppe ihre Inhalte geeignet sind. Altersempfehlungen stellen so für die Konsumenten (insbesondere die Eltern) eine Hilfe bei der Entscheidung dar, ob sie ein bestimmtes Produkt kaufen sollten oder nicht."

Es ist wahrscheinlich, dass die Zune in der Hilfe der Zeit voraus ist, und die Inkludierung des PEGI-Systems für die Zukunft geplant ist oder aber, dass das System zum Testzeitpunkt im September 2011 noch nicht online war. Online waren nur ein Feedbackformular zur Bewertung[23] und eine zusätzliche App[24], die für Eltern gedacht ist und die PEGI-Datenbank durchforsten kann. Diese App hat allerdings nur

[23] Ratingseite unter https://wp-rating.pegi.eu/Games/Submit
[24] Download unter http://www.windowsphone.com/de-at/apps/2c7a9f07-089b-e011-986b-78e7d1fa76f8

Informationscharakter und verhindert keinen Download oder keine Installation. Ein System das Spiele für Windows Phone altersabhängig blockiert, war nicht zu entdecken.

Die Erwartungshaltung wurde in zwei von drei wesentlichen Punkten (E-Mail, Browser) nicht erfüllt, bei der Applikationsinstallation konnte nur alles verhindert werden, nicht jedoch basierend auf einer Altersstufe.

11.5 Erkenntnisse

Basierend auf der Auswertung muss die Bewertung negativ ausfallen: Windows Phone ist im momentanen Zustand nicht kindertauglich. Ein Kind erhält mit einem Windows Phone uneingeschränkten Zugang ins Internet, ohne jegliche Schutzfunktion was den Browser betrifft.

Nicht bewertet, aber ebenso unzulänglich: Es können durch das Kind beliebige weitere Konten am Gerät hinzugefügt werden, darunter natürlich auch ein Facebook-Account, der nicht weiter kontrollierbar ist. Auch die Kamera steht dem Kind ohne Einschränkung zur Verfügung, inklusive der Funktion, Bilder sofort auf Facebook zu laden. Die Privatsphäreneinstellung (z.B. GPS, siehe 6.5) sind ausschließlich lokal zu treffen und können nicht vorgegeben werden.

Nicht bewertet wurde die Problematik beim Bezahlsystem. Da die Bezahlung im Marketplace ausschließlich über Kreditkarte funktioniert (siehe Kapitel 3.6), würde das bedeuten, dass man einem Kind eine Kreditkarte hinterlegt. Zumindest hier kann man eine akzeptable Lösung vorschlagen, die nur geringe Kosten verursacht: statt das Kind mit einer „echten“ Kreditkarte auszustatten oder jene eines Elternteils zu verwenden, können auch virtuelle Kreditkarten bzw. Prepaid-Kreditkarten eingesetzt werden, wie sie von den Kreditkartenunternehmen angeboten werden. Es ist allerdings darauf zu achten, dass sich die Karten als VISA, MasterCard oder American Express-Karten ausgeben, denn andere Karten-Typen kennt Microsoft nicht. Außerdem muss die Kreditkarte auf das Land gemeldet sein, auf das die Windows Live ID eingestellt ist (siehe 3.8).

12 Zusammenfassung und Ausblick

Die These dieser Arbeit lautete, dass moderne Smartphones den grundlegenden Anforderungen an Sicherheit, Datenschutz und Privatsphäre nicht gerecht werden. Die Arbeit konnte in Teilbereichen diese These nicht falsifizieren sondern den Beweis erbringen, dass Lücken im Bereich der Sicherheit und Gefahren für Datenschutz und Privatsphäre bestehen.

Aus technischer Sicht konnte die Arbeit Microsoft ein in weiten Teilen akzeptables Ergebnis nachweisen, so erforderten die in Kapitel 5 beschriebenen Angriffe den physischen Zugang zum Smartphone. Das Sicherheitsmodell von Windows Phone wurde als sehr stark beschrieben, als problematisch erwies sich hat sich die Zeitspanne, die es benötigen kann, bis ein Update (siehe Kapitel 4.14) für eine Sicherheitslücke am Endgerät des Benutzers auftaucht (siehe Kapitel 7.5). Für Firmen, die ein Gerätemanagement haben

wollen, sind die in 4.8 vorgestellten Möglichkeiten definitiv noch nicht genug, das wird alleine bei dem Beispiel der Software Verteilung in Kapitel 7.9 sichtbar.

Im Bereich von Datenschutz und Privatsphäre wurde die rechtliche Situation des Speicherortes beschrieben und wo Windows Phone sich an soziale Netzwerke bindet. Die durchgeführte Untersuchung, die Ortung zu unterbinden war jedoch erfolgreich. Dennoch zeigte diese Untersuchung aber das Problem auf, dass die Einstellungen zur Wahrung der Privatsphäre oftmals gar nicht am Smartphone getroffen werden, sondern beim jeweiligen Anbieter, beispielsweise auf der Einstellungsseite von Facebook, wo Neuerungen und Updates neue Situationen bezüglich der Privatsphäre entstehen lassen, die eine Neubewertung der Sicherheit und des Verhaltens seitens des Benutzers notwendig machen.

Eine einzige App reicht, wie etwa in 7.8 beschrieben, reicht aus, damit die gesamte Sicherheit des Benutzers in Gefahr gerät, zumal sich auch, wie die Untersuchung ergeben hat, die Passwörter des Benutzers nicht zwischen Konten verschiedener Anbieter unterscheiden.

Die in dieser Arbeit untersuchten größten Gefahren für die Privatsphäre gehen demnach also durch Handlungen und Verhalten des Benutzers aus. Dazu zählt vor allem der beschriebene Umgang mit Ortungsdaten und sozialen Netzwerken. So konnte beschrieben werden, dass mit Hilfe von öffentlichen oder für „Freunde“ einsehbaren Daten, Bewegungsprofile erstellt werden konnten. Außerdem wurde mittels Versuch nachgewiesen, dass für einen Angreifer, einem unbekannten Dritten, kein Problem ist, Zugang in geschützte Freundeskreise zu erhalten. Dieser Versuch wurde zusätzlich durch die durchgeführte Umfrage bestätigt, wonach 88% der Teilnehmer niemals nachgefragt haben, ob sich hinter einer Freundschaftsanfrage tatsächlich die vermutete Person befindet. In Bezug auf die Benutzeroberfläche im Vergleich zu anderen Systemen konnte diese Arbeit keinen direkten Vorteil gegenüber anderen Systemen nachweisen, bei geänderter Aufgabenstellung wäre das allerdings ein Punkt für weitere Untersuchungen.

Als im Ergebnis wenig zufriedenstellend musste der Versuch bezüglich der Usability und der Privatsphäre in Kapitel 8 bewertet werden, die Genehmigungsdialoge verloren binnen kürzester Zeit ihre Wirkung und werden vom Benutzer automatisch weggeklickt.

Die Arbeit konnte schließlich nachweisen, dass zu strenge Sicherheitsrichtlinien, zu unsicherem Verhalten führen. Zuerst war das bereits bei VPN in Kapitel 7.6 angedeutet: Wenn Mitarbeiter nicht auf ihre Daten zugreifen könne, dann finden sie alternative Wege, wie jenen der Datenübertragung über webbasierte Speicherdienste. In der Umfrage wurde dann offenbart, dass in einem Unternehmen eine Sicherheitsrichtlinie direkt dazu führt, dass der PIN-Code für die Bildschirmsperre weitergegeben wird, wenn Kinder im selben Haushalt leben. Eine fortführende Untersuchung hat dann zudem feststellen müssen, dass die Kinder- und Jugendschutzeinstellungen unzureichend sind.

Als Ausblick bieten sich verschiedene weitere Untersuchungsgegenstände an, wie etwa die Entwicklung eines System zur zentralen Verwaltung der Privatsphären-Präferenzen

des Benutzers über die verschiedenen Anbieter hinweg. Verallgemeinert man die Ergebnisse aus Kapitel 9, nämlich dass Benutzer die einzelnen Warnhinweise nach zwei oder dreimaligen Auftauchen sowieso ignorieren, so muss das bisherige System als unzulänglich bezeichnet und ersetzt werden. Ein zu entwickelndes System sollte vorsehen, dass der Benutzer einmalig seine gewünschten Einstellungen festlegt, in diesem Fall seine Vorstellungen von Privatsphäre. Das System sollte dann nicht mehr nachfragen, solange die Handlungen bzw. Applikationen diesen Vorstellungen gerecht werden.

Weitere Untersuchungen von der Auswirkung von Kindern der Mitarbeiter auf die Unternehmens-IT könnten weitere Wechselwirkungen der in Kapitel 7.6.3 angeschnittenen Konsumerisierung der IT und deren Bedeutung auf die Sicherheit in Unternehmen erklären.

13 Quellenverzeichnis

[1] R. Cozza, "Forecast: Mobile Communications Devices by Open Operating System, Worldwide, 2008-2015," Gartner Research, 5 April 2011. [Online]. Available: http://www.gartner.com/DisplayDocument?ref=clientFriendlyUrl&id=1619615. [Accessed 3 Juni 2011].

[2] A.-D. Schmidt, F. Peters, F. Lamour and C. Scheel, "Monitoring smartphones for anomaly detection," *Mobile Networks and Applications*, vol. 14, no. 1, pp. 92-106, 2009.

[3] P. Mohan, V. N. Padmanabhan and R. Ramjee, "Nericell: rich monitoring of road and traffic conditions using mobile smartphones," in *SenSys '08: Proceedings of the 6th ACM conference on Embedded network sensor systems*, Bangalore, 2008.

[4] T. Pereira, B. Fonseca, H. Paredes and M. Cabo, "Exploring Iconographic Interface in Emergency for Deaf," in *ASSETS '11 The proceedings of the 13th international ACM SIGACCESS conference on Computers and accessibility*, New York, 2011.

[5] A. K. Karlson, S. T. Iqbal, B. Meyers, G. Ramos and J. C. Tang, "Mobile taskflow in context: a screenshot study of smartphone usage," in *CHI '10 Proceedings of the 28th international conference on Human factors in computing systems* , New York, 2010.

[6] H. Falaki, D. Lymberopoulos, R. Mahajan, S. Kandula and D. Estrin, "A first look at traffic on smartphones," in *IMC '10 Proceedings of the 10th annual conference on Internet measurement* , New York, 2010.

[7] H. Falaki, R. Mahajan, S. Kandula, D. Lymberoopoulos, R. Govindan and D. Estrin, "Diversity in smartphone usage," in *MobiSys '10 Proceedings of the 8th international conference on Mobile systems, applications, and services*, New York, 2010.

[8] G.-J. Ahn, M. Shehab and A. Squicciarini, "Security and Privacy in Social Networks," *Internet Computing, IEEE*, vol. 15, no. 3, pp. 10-12, 2011.

[9] H. Gao, J. Hu, T. Huang, J. Wang and Y. Chen, "Security Issues in Online Social Networks," *Internet Computing, IEEE*, vol. 15, no. 4, pp. 56-63, 2011.

[10] M. Huber, M. Mulazzani, E. R. Weippl, G. Kitzler and S. Goluch, "Friend-in-the-middle Attacks: Exploiting Social Networking Sites for Spam," *IEEE Internet Computing: Special Issue on Security and Privacy in Social Networks*, 2011.

[11] M. Huber, M. Mulazzani and E. R. Weippl, "Who On Earth Is Mr. Cypher? Automated Friend Injection Attacks on Social Networking Sites," in *Proceedings of the IFIP International Information Security Conference 2010: Security and Privacy*, 2010.

[12] A. Gkoulalas-Divanis, V. S. Verykios and D. Eleftheriou, "PLOT: Privacy in Location Based Services: An Open-Ended Toolbox," in *Mobile Data Management: Systems, Services and Middleware, 2009. MDM '09. Tenth International Conference on*, Taipei, 2009.

[13] S. T. Peddinti, A. Dsouza and N. Saxena, "Cover locations: availing location-based services without revealing the location," in *WPES '11 Proceedings of the 10th annual ACM workshop on Privacy in the electronic society* , New York, 2011.

[14] L. Liu, "Privacy and Location Anonymization in Location-based Services," *SIGSPATIAL Special*, vol. 1, no. 2, pp. 15-22, 2009.

[15] G. Portokalidis, P. Homburg, K. Anagnostakis and H. Bos, "Paranoid Android: Versatile Protection For Smartphones," in *ACSAC '10 Proceedings of the 26th Annual Computer Security Applications Conference*, New York, 2010.

[16] A. Distefano, A. Grillo, A. Lentini and G. F. Italiano, "SecureMyDroid: Enforcing Security in the Mobile Devices Lifecycle," in *CSIIRW '10 Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research* , New York, 2010.

[17] A. P. Felt, M. Finifter, E. Chin, S. Hanna and D. Wagner, "A survey of mobile malware in the wild," in *SPSM '11 Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices*, New York, 2011.

[18] K. Wain Yee Au, Y. F. Zhou, Z. Huang, P. Gill and D. Lie, "Short Paper: A Look at SmartPhone Permission Models," in *SPSM '11 Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices*, New York, 2011.

[19] "Android Permissions Demystified," in *CCS '11 Proceedings of the 18th ACM conference on Computer and communications security*, New York, 2011.

[20] A. K. Karlson, A. B. Brush and S. Schechter, "Can I Borrow Your Phone? Concerns When Sharing Mobile Phones," in *CHI '09 Proceedings of the 27th international conference on Human factors in computing systems*, New York, 2009.

[21] R. Ouch and B. Rouse, "Developing a Driving Training Game on Windows Mobile Phone Using C# and XNA," in *2011 16th International Conference on Computer*

Games (CGAMES), 2011.

[22] J. A. Rode, "Digital Parenting: Designing Children's Safety," in *BCS-HCI '09 Proceedings of the 23rd British HCI Group Annual Conference on People and Computers: Celebrating People and Technology*, Swinton, 2009.

[23] E. Stobert, "Usability and strength in click-based graphical passwords," in *CHI EA '10 Proceedings of the 28th of the international conference extended abstracts on Human factors in computing systems*, New York, 2010.

[24] E. R. Weippl and B. Riedl, "Security, Trust, and Privacy on Mobile Devices and Multimedia Applications," in *Handbook of Research on Mobile Multimedia*, Hershley, IGI Global, 2009, pp. 115-132.

[25] J. M. Quinn and T. Q. Tran, "Attractive Phones Don't Have To Work Better: Independent Effects of Attractiveness, Effectiveness, and Efficiency on Perceived Usability," in *CHI '10 Proceedings of the 28th international conference on Human factors in computing systems*, New York, 2010.

[26] K. Church and B. Smyth, "Understanding the intent behind mobile information needs," in *IUI '09 Proceedings of the 14th international conference on Intelligent user interfaces* , New York, 2009.

[27] T. Sohn, K. A. Li, W. G. Griswold and J. D. Hollan, "A Diary Study of Mobile Information Needs," in *CHI '08 Proceeding of the twenty-sixth annual SIGCHI conference on Human factors in computing systems*, New York, 2008.

[28] C. Coursaris and D. J. Kim, "A Meta-Analytical Review of Empirical Mobile Usability Studies," *Journal of Usability Studies,* vol. 6, no. 3, pp. 117-171, 2011.

[29] A. D. P. Service, "Was ist das 'Recht auf Widerspruch'?," ARGE Daten Privacy Service, [Online]. Available: http://www2.argedaten.at/php/cms_monitor.php?q=PUB-TEXT-ARGEDATEN&s=96311vtp. [Accessed 7 August 2011].

[30] B. Gates, N. Myhrvold and P. Rinearson, The road ahead, 1. ed., New York: Viking Penguin, 1995.

[31] Microsoft Corporation, "What is MS Plus! for Windows 95?," Microsoft Corporation, 1995. [Online]. Available: http://technet.microsoft.com/en-us/library/cc768075.aspx. [Accessed 02 Oktober 2011].

[32] T. Barclay, J. Gray and D. Slutz, The Microsoft TerraServer, Redmond, Washington: Microsoft Research, 1998.

[33] J. Kuri, "Microsoft: Firmenkunden bringen Geld, Windows schwächelt," Heise Verlag, 21 Oktober 2011. [Online]. Available: http://www.heise.de/newsticker/meldung/Microsoft-Firmenkunden-bringen-Geld-Windows-schwaechelt-1364386.html. [Accessed 26 Oktober 2011].

[34] G. Binder, "Windows Phone App: XING," WindowsBlog.at, 24 Juli 2011. [Online]. Available: http://www.windowsblog.at/post/2011/07/24/Windows-Phone-App-XING.aspx. [Accessed 24 Juli 2011].

[35] J. Rodriguez, "Windows phone capabilities security model," Microsoft Corporation, 30 April 2010. [Online]. Available: http://blogs.msdn.com/b/jaimer/archive/2010/04/30/windows-phone-capabilities-security-model.aspx. [Accessed 25 September 2011].

[36] Microsoft Corporation, "Feature and service availability," Microsoft Corporation, [Online]. Available: http://www.microsoft.com/windowsphone/en-us/howto/wp7/basics/feature-and-service-availability.aspx. [Accessed 4 Oktober 2011].

[37] A. Birch, "Windows Phone 7 Feature Availability Matrix: The Mango Edition," Andre Tech Help, 29 Mai 2011. [Online]. Available: http://www.andrewtechhelp.com/andrews-tech-opinions/126-windows-phone-7-feature-availability-matrix-the-mango-edition. [Accessed 16 September 2011].

[38] P. Torr, "Windows Phone Multitasking," Microsoft Corporation, 16 September 2011. [Online]. Available: http://channel9.msdn.com/events/BUILD/BUILD2011/APP-823T. [Accessed 18 September 2011].

[39] Microsoft Corporation, "Windows Phone 7.5 Update startet ab heute," Microsoft Corporation, 27 September 2011. [Online]. Available: http://www.microsoft.com/austria/presse/news1825.mspx?ID=b35cfef8-6c5e-4ea7-80d5-1bd5b4b00a24. [Accessed 20 Oktober 2011].

[40] Microsoft Corporation, "Multitasking for Windows Phone," 23 September 2011. [Online]. Available: http://msdn.microsoft.com/en-us/library/hh202866(v=vs.92).aspx. [Accessed 4 Oktober 2011].

[41] Microsoft Corporation, "Windows Phone 7.5 Guides for IT Professionals," 18 Oktober 2011. [Online]. Available: http://www.microsoft.com/download/en/details.aspx?id=27743. [Accessed 20 Oktober 2011].

[42] M. Howard and D. LeBlanc, Wrinting Secure Code, Redmond, Washington:

Microsoft Press, 2003.

[43] Microsoft Corporation, "SSL Root Certificates for Windows Phone," Microsoft Corporation, 23 September 2011. [Online]. Available: http://msdn.microsoft.com/en-us/library/gg521150(v=VS.92).aspx. [Accessed 29 September 2011].

[44] G. Binder, "Windows Phone 7 und selbstsignierte Zertifikate," WindowsBlog.at, 9 Dezember 2010. [Online]. Available: http://www.windowsblog.at/post/2010/12/09/Windows-Phone-7-und-selbstsignierte-Zertifikate.aspx. [Accessed 04 Oktober 2011].

[45] Microsoft Corporation, "Understanding Exchange ActiveSync," Microsoft Corporation, 2 September 2011. [Online]. Available: http://technet.microsoft.com/en-us/library/aa998357.aspx. [Accessed 10 Oktober 2011].

[46] Microsoft Corporation, "Windows Phone 7 and Exchange Server," 20 Dezember 2010. [Online]. Available: http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=8842. [Accessed 23 August 2011].

[47] Microsoft Corporation, "Understanding Information Rights Management," 11 Februar 2011. [Online]. Available: http://technet.microsoft.com/en-us/library/dd638140.aspx. [Accessed 24 August 2011].

[48] Microsoft Corporation, "Understanding Transport Protection Rules," Microsoft Corporation, 21 Januar 2010. [Online]. Available: http://technet.microsoft.com/en-us/library/dd298166.aspx. [Accessed 10 Oktober 2011].

[49] Microsoft Corporation, "Understanding Information Rights Management in Exchange ActiveSync," Microsoft Corporation, 14 Februar 2011. [Online]. Available: http://technet.microsoft.com/en-us/library/ff657743.aspx. [Accessed 10 Oktober 2011].

[50] B. Posey, "System Center: Managing Mobile Devices," Microsoft Crporation, Juli 2011. [Online]. Available: http://technet.microsoft.com/en-us/magazine/hh316170.aspx. [Accessed 14 Oktober 2011].

[51] Microsoft Corporation, "Windows Internet Explorer Mobile on Windows Phone 7," 20 Dezember 2010. [Online]. Available: http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=8842. [Accessed 10 Oktober 2011].

[52] Microsoft Corporation, "Von Windows Phone unterstützte Bluetooth-Profile," Microsoft Corporation, 18 Oktober 2011. [Online]. Available: http://support.microsoft.com/kb/2449475/de. [Accessed 25 Oktober 2011].

[53] Microsoft Corporation, "Windows Phone 7 Security Model," 20 Dezember 2010. [Online]. Available: http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=8842. [Accessed 3 Oktober 2011].

[54] Microsoft Corporation, "Application Manifest File for Windows Phone," Microsoft Corporation, 23 September 2011. [Online]. Available: http://msdn.microsoft.com/en-us/library/ff769509(v=vs.92).aspx#BKMK_Capabilities. [Accessed 14 Oktober 2011].

[55] athompson, "Undocumented Capabilities in WMAppManifest.xml WP7," XDA Developers, 27 Oktober 2010. [Online]. Available: http://forum.xda-developers.com/showthread.php?t=820455. [Accessed 13 Oktober 2011].

[56] Microsoft Corporation, "Windows Phone 7 security and management," 20 Dezember 2010. [Online]. Available: http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=8842. [Accessed 4 Oktober 2011].

[57] Technical Committee SD Card Association, "SD Specifications Part 1 Physical Layer Simplified Specification Version 3.01," 18 Mai 2010. [Online]. Available: https://www.sdcard.org/downloads/pls/simplified_specs/Part_1_Physical_Layer_Simplified_Specification_Ver_3.01_Final_100518.pdf. [Accessed 10 September 2011].

[58] Microsoft Corporation, "How to: Encrypt Data in a Windows Phone Application," Microsoft Corporation, 23 September 2011. [Online]. Available: http://msdn.microsoft.com/en-us/library/hh487164(v=VS.92).aspx. [Accessed 6 Oktober 2011].

[59] E. Hautala, "Windows Phone 7.5 “Mango” update begins," Microsoft Corporation, 27 September 2011. [Online]. Available: http://windowsteamblog.com/windows_phone/b/windowsphone/archive/2011/09/27/windows-phone-7-5-mango-update-begins.aspx. [Accessed 10 Oktober 2011].

[60] "SharePoint 2010 Products and SharePoint Workspace Mobile," Microsoft Corporation, 31 Januar 2011. [Online]. Available: http://blogs.technet.com/b/tothesharepoint/archive/2011/01/31/sharepoint-2010-products-and-sharepoint-workspace-mobile.aspx. [Accessed 19 September 2011].

[61] R. Rivera, C. Walsh and L. Zheng, "ChevronWP7 Labs is reaching the finish line!," ChevronWP7, 14 Oktober 2011. [Online]. Available: http://www.chevronwp7.com/post/11457150629/chevronwp7-labs-is-reaching-the-finish-line. [Accessed 26 Oktober 2011].

[62] HeathCliff74, "XDA Developers," 21 September 2011. [Online]. Available: http://forum.xda-developers.com/showthread.php?t=1271963. [Accessed 18 Oktober 2011].

[63] Schaps, "Registry Editor for Windows Phone 7 Beta Testing," TouchXperience, 19 Januar 2011. [Online]. Available: http://forum.touchxperience.com/viewtopic.php?f=20&t=593. [Accessed 16 September 2011].

[64] Surur, "Debranding tutorial for LG phones," WMPowerUser.com, 23 März 2011. [Online]. Available: http://wmpoweruser.com/debranding-tutorial-for-lg-phones-to-hurry-nodo-along-needs-to-dev-unlock/. [Accessed 14 Oktober 2011].

[65] WP7_User, "Massenspeichermodus bei Windows Phone 7-Geräten," PocketPC.ch, 28 Januar 2011. [Online]. Available: http://www.pocketpc.ch/windows-phone-7-allgemein/119833-tutorial-massenspeichermodus-windows-phone-7-geraeten.html. [Accessed 14 Oktober 2011].

[66] P. Thurrott, "DO NOT use Windows Phone 7 as a mass storage device," Windows Phone Secrets, 19 November 2010. [Online]. Available: http://windowsphonesecrets.com/2010/11/19/do-not-use-windows-phone-7-as-a-mass-storage-device/. [Accessed 13 Oktober 2011].

[67] Nudua, "[Nes Emulator] vNesLight," XDA Developers, 28 Juni 2011. [Online]. Available: http://forum.xda-developers.com/showthread.php?t=1144561. [Accessed 13 Oktober 2011].

[68] G. Binder, "Screenrecording von Windows Phone," WindowsBlog.at, 08 Oktober 2011. [Online]. Available: http://www.windowsblog.at/post/2011/10/08/Screenrecording-von-Windows-Phone.aspx. [Accessed 12 Oktober 2011].

[69] G. Binder, "HowTo: Screenshots mit Windows Phone 7.5," WindowsBlog.at, 23 Oktober 2011. [Online]. Available: http://www.windowsblog.at/post/2011/10/23/HowTo-Screenshots-mit-Windows-Phone-75.aspx. [Accessed 23 Oktober 2011].

[70] D. Rubino, "Windows Phone Marketplace app-security cracked: Proof-of-concept," WPcentral, 29 Dezember 2010. [Online]. Available: http://www.wpcentral.com/windows-phone-marketplace-app-security-cracked-

proof-of-concept-video. [Accessed 3 Oktober 2011].

[71] G. Binder, "Internet Sharing nun auch für Geräte der ersten Generation," WindowsBlog.at, 27 Oktober 2011. [Online]. Available: http://www.windowsblog.at/post/2011/10/27/Windows-Phone-Internet-Sharing-nun-auch-fur-Gerate-der-ersten-Generation.aspx. [Accessed 27 Oktober 2011].

[72] Goofystyle, "LG Optimus 7 E900 Debranden," PocketPC.ch, 24 Februar 2011. [Online]. Available: http://www.pocketpc.ch/lg-e900-optimus-7/123029-lg-optimus-7-e900-debranden.html. [Accessed 10 Oktober 2011].

[73] Microsoft Corporation, "Microsoft-Dienstleistungsvertrag," Microsoft Corporation, März 2010. [Online]. Available: http://mid.live.com/terms.aspx?mkt=de-de&__ufps=214055#InitPos. [Accessed 10 Oktober 2011].

[74] Microsoft Corporation, "Windows Phone 7 étoffe son bouquet de services avec une nouvelle version de Windows Live Messenger," Microsoft Corporation, 24 November 2010. [Online]. Available: http://www.microsoft.com/france/hub-presse/communiques-de-presse/fiche-communique.aspx?EID=7fb03cc3-14fb-4dc7-897d-5c8eb44f00c4. [Accessed 10 Dezember 2010].

[75] H. Bleich, "Des Nutzers neue Kleider," *c't Magazin für Computertechnik*, pp. 98-101, 10 Oktober 2011.

[76] Microsoft Corporation, "Vertrauensstellungscenter: Sicherheits-, Datenschutz- und Konformitätsinformationen für Microsoft Online Services: Geografische Grenzen," [Online]. Available: http://www.microsoft.com/online/legal/v2/?docid=25&langid=de-de. [Accessed 20 Oktober 2011].

[77] C. Kirsch, "US-Behörden dürfen auf europäische Cloud-Daten zugreifen," Heise.de, 30 Juni 2011. [Online]. Available: http://www.heise.de/newsticker/meldung/US-Behoerden-duerfen-auf-europaeische-Cloud-Daten-zugreifen-1270455.html. [Accessed 06 Oktober 2011].

[78] Micrososoft Corporation, "Location Overview for Windows Phone," Microsoft Corporation, 23 September 2011. [Online]. Available: http://msdn.microsoft.com/en-us/library/ff431800(v=VS.92).aspx. [Accessed 5 Oktober 2011].

[79] Microsoft Corporation, "Windows Phone 7 Privacy Statement," Microsoft Corporation, September 2011. [Online]. Available: http://www.microsoft.com/windowsphone/en-us/privacy.aspx. [Accessed 20 Oktober 2011].

[80] Microsoft Corporation, "How to: Get Data from the Location Service for Windows Phone," Microsoft Corporation, 23 September 2011. [Online]. Available: http://msdn.microsoft.com/en-us/library/ff431782(v=VS.92).aspx. [Accessed 4 Oktober 2011].

[81] J. Wirtgen, "Wirbel um Bewegungsprofile im iPhone und iPad," *c't Magazin für Computertechnik,* pp. 18-20, 11 2011.

[82] Microsoft Corporation, "Location and my privacy FAQ," Microsoft Corporation, September 2011. [Online]. Available: http://www.microsoft.com/windowsphone/en-us/howto/wp7/web/location-and-my-privacy.aspx. [Accessed 11 Oktober 2011].

[83] Microsoft Corporation, "SSL Root Certificates for Windows Phone," Microsoft Corporation, 23 September 2011. [Online]. Available: http://msdn.microsoft.com/en-us/library/gg521150(v=VS.92).aspx. [Accessed 1 Oktober 2011].

[84] Comodo, "Comodo detected and thwarted an intrusion on 26-MAR-2011," Comodo, 26 März 2011. [Online]. Available: http://www.comodo.com/Comodo-Fraud-Incident-2011-03-23.html. [Accessed 18 August 2011].

[85] Microsoft Corporation, "Microsoft Security Advisory (2607712): Fraudulent Digital Certificates Could Allow Spoofing," Microsoft Corporation, 29 August 2011. [Online]. Available: Fraudulent Digital Certificates Could Allow Spoofing. [Accessed 8 September 2011].

[86] Microsoft Corporation, "DeviceExtendedProperties Class," Microsoft Corporation, 23 September 2011. [Online]. Available: http://msdn.microsoft.com/en-us/library/microsoft.phone.info.deviceextendedproperties(v=VS.92).aspx. [Accessed 6 Oktober 2011].

[87] Microsoft Corporation, "UserExtendedProperties.GetValue Method," Microsoft Corporation, 23 September 2011. [Online]. Available: http://msdn.microsoft.com/en-us/library/microsoft.phone.info.userextendedproperties.getvalue(v=VS.92).aspx. [Accessed 5 Oktober 2011].

[88] D. N. Egan, "WP7 Getting Unique Device and User," The sociable geek, 5 Oktober 2011. [Online]. Available: http://thesociablegeek.com/2011/10/05/wp7-getting-unique-device-and-user/. [Accessed 20 Oktober 2011].

[89] Microsoft Corporation, "Where's my phone update?," Microsoft Corporation, 31 Oktober 2011. [Online]. Available: http://www.microsoft.com/windowsphone/en-

us/features/update-schedule-world.aspx. [Accessed 1 November 2011].

[90] Microsoft Corporation, "Microsoft Security Advisory (2524375): Fraudulent Digital Certificates Could Allow Spoofing," Microsoft Corporation, 23 März 2011. [Online]. Available: http://technet.microsoft.com/en-us/security/advisory/2524375. [Accessed 14 Oktober 2011].

[91] D. Moschella, D. Neal, P. Opperman and J. Taylor, "Leading Edge Forum: The Consumerization of Information Technology," 18 November 2004. [Online]. Available: http://lef.csc.com/publications/497. [Accessed 05 Juni 2011].

[92] Kik, "Our Story," [Online]. Available: http://www.kik.com/ourstory. [Accessed 08 Oktober 2011].

[93] M. Cardwell, "Kik Messenger Insecure," 7 November 2010. [Online]. Available: https://grepular.com/Kik_Messenger_Insecure. [Accessed 8 Oktober 2011].

[94] T. Brix, "Making Money with your Application on Windows Phone," Microsoft Corporation, 14 April 2011. [Online]. Available: http://channel9.msdn.com/events/MIX/MIX11/DVC05. [Accessed 20 September 2011].

[95] D. Dembach and B. Wellhöfer, "Anbauten," *iX Magazin für professionelle Informationstechnik*, pp. 85-87, Januar 2010.

[96] J. Oberheide and F. Jahanian, "When Mobile is Harder Than Fixed (and Vice Versa): Demystifying Security Challenges in Mobile Environments," in *HotMobile '10 Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications*, New York, 2010.

[97] Microsoft Corporation, *Internal Study: Side-by-Side Scenario Comparisons*, Juli, 2010.

[98] N. Baum, "SharePoint Surveys – Overview and Links," Microsoft Corporation, 15 Juli 2009. [Online]. Available: http://blogs.msdn.com/b/natebaum/archive/2009/07/15/sharepoint-surveys-overview-and-links.aspx. [Accessed 20 September 2011].

[99] Microsoft Corporation, "Zune Blockierte Spielefreigaben," Microsoft Corporation, [Online]. Available: http://www.zune.net/de-at/support/zunemarketplace/about/blockedgames.htm. [Accessed 15 September 2011].

[100] Pan European Game Information, "Was sind Altersempfehlungen?," PEGI, [Online]. Available: http://www.pegi.info/de/index/id/44/. [Accessed 4 Oktober

2011].

14 Anhang

14.1 Quelldaten zu Videoanalyse

Die Datenerfassung der Zeitnehmung erfolgte in Excel, hier befindet sich der gesamte Inhalt des Excelsheets:

Person	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10
Geschlecht	m	w	w	m	w	m	m	w	w	m
Alter	33	34	22	68	28	30	30	31	70	38
IT-affin	1	0	0	1	1	0	0	1	0	0
Nutzungsbestimmungen Klick	0	0	0	0	0	0	0	0	0	0
Find my Phone abgebrochen?	0	0	0	1	0	0	0	0	0	0
Find my Phone Ortung erlaubt?	1	1	1	0	1	1	1	1	1	1
Find my Phone Ortung Zeit	20	22	30	40	12	30	31	17	25	12
Karten abgebrochen	0	0	0	0	0					
Karten Ortung erlaubt?	1	1	1	1	1					
Karten Ortung Zeit	7	4	10	16	5					
Suche abgebrochen	0	0	0	0	0					
Suche Ortung erlaubt?	1	1	1	1	1					
Suche Ortung Zeit	2	1	2	1	15					
Foto abgebrochen	0	0	0	0	0					
Foto Ortung erlaubt?	1	1	1	1	1					
Foto Ortung Zeit	1	1	1	4	3					
App abgebrochen	0	0	0	1	0	0	0	0	0	0
App Ortung erlaubt?	1	1	1	0	1	1	1	1	1	1
App Ortung Zeit	1	1	1	14	2	10	12	14	8	12

14.2 Quelldaten der Umfrage zum Nutzungsverhalten

Export der SharePoint-Quelldaten für die Umfrage in Kapitel 10.

Datum	**Q01**	**Q02**	**Q03**	**Q04**	**Q05**	**Q06**	**Q07**	**Q08**	**Q09**	**Q10**	**Q11**	**Q12**	**Q13**
12.09.2011	1	1	1	0	0	0	1	0	1	1	0	1	Damit ichSonntags schlafen kann
12.09.2011	1	1	1	0	0	0	1	0	1	1	1	1	
12.09.2011	0	1	1	0	0	0	1	0	1	1	1	1	Sohn & Xbox
12.09.2011	0	1	1	0	0	0	1	0	0	1	0	1	
12.09.2011	0	0	1	0	0	1	0	0	1	1	1	1	Wipe
12.09.2011	1	0	1	0	0	1	0	1	1	1	1	1	
12.09.2011	1	1	1	0	1	0	0	0	1	1	1	1	
12.09.2011	1	1	1	0	1	0	0	0	1	1	1	1	
12.09.2011	0	0	0	0	1	0	0	0	1	0	1	1	

12.09.2011	0	0	1	0	0	0	0	0	1	0	1	1	Werner spielt gerne
12.09.2011	1	1	1	0	0	1	0	0	1	1	1	0	
12.09.2011	1	1	1	0	0	0	0	0	1	1	0	0	
12.09.2011	1	1	1	1	0	0	0	0	1	1	0	0	
12.09.2011	1	1	1	0	0	0	0	0	0	1	1	0	
12.09.2011	0	0	1	0	0	0	0	0	1	1	1	0	
12.09.2011	0	1	1	0	0	0	0	0	1	1	1	0	
12.09.2011	1	1	1	0	0	0	0	0	1	1	0	0	
12.09.2011	1	1	1	1	0	0	0	0	1	1	1	0	
12.09.2011	1	1	1	0	0	0	0	0	0	1	1	0	
12.09.2011	0	1	1	0	0	0	0	0	1	1	1	0	
12.09.2011	1	1	1	0	0	0	0	0	1	1	1	0	
12.09.2011	1	1	1	0	0	0	0	0	1	1	1	0	
12.09.2011	0	1	1	0	0	0	0	0	0	1	0	0	
12.09.2011	1	1	1	0	0	0	0	0	1	1	0	0	
12.09.2011	1	1	1	1	0	0	0	0	1	1	1	0	
12.09.2011	1	0	1	1	0	0	0	0	0	1	1	0	
12.09.2011	1	0	1	0	0	0	0	0	0	0	0	0	
12.09.2011	1	1	1	0	0	0	0	0	1	1	1	0	
12.09.2011	1	0	0	0	0	0	0	0	1	0	1	0	
12.09.2011	0	0	0	0	0	0	0	0	0	0	1	0	
12.09.2011	0	0	0	0	0	0	0	0	1	0	0	0	
12.09.2011	1	1	1	0	0	0	0	1	1	1	1	0	
12.09.2011	1	1	1	0	0	0	0	1	0	1	1	0	
12.09.2011	0	0	0	0	0	0	0	1	1	0	1	0	
13.09.2011	0	0	0	0	1	0	1	0	1	0	1	1	
13.09.2011	0	1	1	0	0	1	0	0	1	1	0	1	Wegen der Spiele
13.09.2011	1	1	1	0	1	0	0	0	1	1	1	1	SPiele
13.09.2011	1	1	1	0	0	0	0	0	0	1	0	1	
13.09.2011	1	1	1	1	0	0	0	0	1	0	1	0	
13.09.2011	1	1	1	0	0	0	0	0	0	1	1	0	
13.09.2011	0	0	1	1	0	0	0	0	1	1	1	0	
13.09.2011	1	0	1	0	0	0	0	0	1	0	1	0	
13.09.2011	1	0	1	0	0	0	0	0	1	1	0	0	
13.09.2011	1	1	1	0	0	0	0	1	1	1	0	0	
14.09.2011	0	1	1	0	1	0	0	0	1	1	1	0	
14.09.2011	1	1	1	0	0	0	0	0	1	1	1	0	
14.09.2011	1	0	1	0	0	0	0	0	1	0	1	0	
14.09.2011	0	0	1	0	0	0	0	0	0	1	0	0	
15.09.2011	1	0	1	0	0	1	0	0	1	1	1	1	
15.09.2011	1	1	1	0	0	0	0	0	0	0	0	0	
15.09.2011	1	0	1	0	0	0	0	0	0	1	1	0	
19.09.2011	0	1	1	0	1	0	1	0	1	1	0	1	Die Kinder spielen gerne

19.09.2011	0	0	0	0	1	1	0	0	1	0	1	1	
19.09.2011	1	1	1	0	0	1	0	0	1	1	1	1	Zweimal neu aufsetzen reicht
19.09.2011	0	0	0	0	0	1	0	0	1	0	0	1	
19.09.2011	1	1	1	0	1	0	0	0	1	1	1	1	
19.09.2011	0	1	1	0	0	0	0	0	1	0	1	1	
19.09.2011	1	1	1	0	0	0	0	0	1	1	1	1	
19.09.2011	1	1	1	0	0	0	0	0	1	1	0	1	
19.09.2011	1	0	1	0	0	1	0	0	1	1	0	0	
19.09.2011	1	1	1	0	0	0	0	0	1	1	1	0	
19.09.2011	0	1	1	0	0	0	0	0	1	1	0	0	
19.09.2011	1	1	1	0	0	0	0	0	1	1	1	0	
19.09.2011	1	0	1	0	0	0	0	0	0	1	1	0	
19.09.2011	1	0	1	0	0	0	0	0	0	1	1	0	
19.09.2011	1	1	1	0	0	0	0	0	1	1	0	0	
19.09.2011	0	0	1	0	0	0	0	0	1	1	0	0	
19.09.2011	1	1	1	0	0	0	0	0	1	1	0	0	
19.09.2011	1	1	1	0	0	0	0	0	1	1	1	0	
19.09.2011	1	1	1	1	0	0	0	0	1	1	1	0	
19.09.2011	1	1	1	1	0	0	0	0	0	1	1	0	
19.09.2011	0	0	0	0	0	0	0	0	1	0	1	0	
19.09.2011	0	0	0	0	0	0	0	0	1	0	1	0	
19.09.2011	0	0	0	0	0	0	0	0	1	0	1	0	
19.09.2011	0	0	0	0	0	0	0	0	0	0	1	0	
19.09.2011	1	1	1	1	0	0	0	1	1	1	1	0	
19.09.2011	0	0	0	0	0	0	0	1	1	0	0	0	
19.09.2011	0	0	0	0	0	0	0	1	1	0	0	0	
19.09.2011	0	0	0	0	0	0	0	1	1	0	0	0	
20.09.2011	0	0	0	0	1	0	1	0	0	0	0	1	Handy wird sonst gelöscht
20.09.2011	0	1	1	0	0	1	0	0	1	0	1	1	
20.09.2011	0	0	0	0	0	1	0	0	1	0	1	1	Wegen reset
20.09.2011	1	1	1	0	0	0	0	0	1	1	1	0	
20.09.2011	0	0	0	0	0	0	0	0	1	0	0	0	
20.09.2011	1	1	1	0	0	0	0	1	1	0	1	0	
21.09.2011	1	1	1	0	1	1	0	0	0	1	1	1	Kids Access
21.09.2011	0	0	0	0	0	1	0	0	0	0	1	1	
21.09.2011	0	0	0	0	0	1	0	0	1	0	1	1	3x flasch eingeben…
21.09.2011	0	0	0	0	0	1	0	0	1	0	1	1	
21.09.2011	0	0	1	0	0	0	0	0	1	1	1	1	
21.09.2011	1	1	1	0	0	0	0	0	0	1	0	1	
21.09.2011	1	0	1	0	1	0	0	0	1	1	0	0	
21.09.2011	0	1	1	0	1	0	0	0	1	0	0	0	
21.09.2011	0	1	1	0	0	0	0	0	1	1	0	0	
21.09.2011	0	0	0	0	0	0	0	0	1	0	0	0	

22.09.2011	0	0	1	0	0	1	0	0	1	1	1	1	Sonst wird es gelöscht
22.09.2011	0	0	0	0	0	0	0	0	0	0	1	1	Spiele
22.09.2011	0	0	1	0	0	0	0	0	1	0	0	0	
22.09.2011	0	0	0	0	0	0	0	0	1	0	1	0	

14.3 Lebenslauf

Persönliche Daten	Georg Binder Favoritenstraße 17/11, 1040 Wien
Geburtsdatum	01. Juni 1977
Schwerpunkt seit 2001 (selbständig)	Firmen-Endanwender Schulungen im Bereich Windows und Office v.a. im Zuge von Migrationen Vorträge und Trainings Inhaltliche Betreuung von Social Media Projekten
Seit Januar 2010	Partner Sales Factory OG (PSF), Geschäftsführer Die PSF bietet Pre-Sales-Dienstleistungen für Microsoft Partner
Seit November 2006	www.windowsblog.at, Blogger Inhaltliche Gestaltung, Content-Erstellung und Userbetreuung. Das Projekt wurde zu Microsofts erfolgreichstem Blog im deutschsprachigen Raum.
Seit September 2005	FH Krems, Lektor IT-Kurse in englischer Sprache in den Fachrichtungen Tourismus und Biotechnologie
Vor 2001	2000: GWD: Heeresdatenverarbeitungsamt 1998 -2000 Trainerassistent bei Präsentationstechnikseminaren (HPS) 1995 – 2000 IT-Betreuung, Webdesign Juli 1993 u. 1994 – Ferialjob Alcatel, Leiterplattenfertigung
Hochschulstudium	Wirtschaftsinformatik, Universität Wien,

	Akademischer Grad “Bakk.rer.soc.oec.”
Schulausbildung	AHS Matura
Aktuelle Vorträge und Workshops	Speaker auf der größten Veranstaltungsserie von Microsoft in Österreich (März/April 2011) Microsoft Office Umstiegstrainings, Social Media, Cloud Computing