Technische Universität Berlin

Fachbereich Informatik
Institut für Wirtschaftsinformatik

Prof. Dr. iur. Bernd Lutterbeck

MOBILER ZUGANG ZU GESICHERTEN NETZEN – LÖSUNGEN FÜR DIE ZUKUNFT

EVALUATION DES EINSATZES MOBILER ENDGERÄTE IM BMI

EXECUTIVE SUMMARY

(PRESSEVERSION)

Erstellt im Auftrag des Bundesministeriums des Innern

vorgelegt von der

Forschungsgruppe Internet Governance

Berlin, August 2003

Stephan Balszuweit (cand. Inform.)
Thomas Fritsch (cand. Inform.)
Robert Gehring (Diplom-Inform.)
Tilman Kamp (cand. Inform.)
Raphael Leiteritz (Diplom-Inform., Projektleiter)
Bernd Lutterbeck (Prof. für Informationsrecht, Jean Monnet Prof.)
Frank Pallas (cand. Inform.)
Torsten Pehl (cand. Inform.)
Nazan Yildiz (cand. Inform.)

1 Executive Summary

Grundlage dieses Dokuments ist ein Projekt der TU Berlin, Institut für Wirtschaftsinformatik, im Auftrag des Bundesministeriums des Innern. Die TU Berlin hat 2003 ein Evaluationsprojekt zum Thema mobile Technologien im BMI durchgeführt („MOB II"). Basis dieses Dokuments ist wiederum eine Studie über aktuell verfügbare Mobiltechnologien, die die TU Berlin im Auftrag des BMI 2002 angefertigt hat („MOB I"). Die folgenden Ergebnisse und Empfehlungen sind die zusammengefassten Resultate des aktuellen Projekts MOB II.

Mobile Endgeräte stellen für moderne Verwaltungen zunehmend eine wichtige Ergänzung zu klassisch stationären IT-Systemen dar. Der Schwerpunkt dieses Projekts liegt auf der Evaluation der Geräte des Herstellers HP[1] (iPAQs), die als beispielhafte Vertreter der PocketPC-Geräteklasse ausgewählt wurden. Ein Grund hierfür ist, dass diese Geräte heute im bereits im Einsatz sind und die Verbreitung in Zukunft weiter zunehmen wird. Daraus ergibt sich die Notwendigkeit, den Einsatz der mobilen Endgeräte unter der Berücksichtigung von Sicherheit, Bedienbarkeit, Administrierbarkeit und Kosten zu untersuchen und zu ermitteln, ob und unter welchen Bedingungen ein vermehrter Einsatz möglich und sinnvoll ist.

Im Rahmen dieses Projekts wurde eine Vielzahl von Konzepten und Methoden für Evaluation und Vergleich mobiler Endgeräte und damit zusammenhängender Synchronisierungs- und Managementprodukte entwickelt. Zusätzlich werden Vorgehensweisen wie z.B. ein flexibles Backup-/Imagekonzept beschrieben. Wir haben uns bemüht, unsere Schritte möglichst transparent und nachvollziehbar zu dokumentieren. Wir gehen davon aus, dass die Ergebnisse eine gute Grundlage sowohl für die interne IT-Abteilung als auch für zukünftige Projekte im Mobilbereich darstellen.

Ergebnisse

★ **Ergebnis 1: Die mobilen Endgeräte vom Typ iPAQ sind hinsichtlich verschiedener Leistungsparameter (u. a. Mobilität, Softwareausstattung, Sicherheit) den Anforderungen[2] im Behördenumfeld nicht gewachsen. iPAQs gehören zu den derzeit leistungsfähigsten Handheld-Systemen, sie sind aber keine „kleinen Laptops".**

Begründung: Die Mitarbeiter sind typischerweise an den Leistungsumfang von Microsoft Outlook in Kombination mit zentralen Messaging-Systemem wie z.B. Microsoft Exchange gewöhnt. Der auf dem PocketPC-Betriebssystem verfügbare Messaging-Client Pocket Outlook hat gegenüber Outlook allerdings erhebliche Einschränkungen: Die Terminverwaltung ist in den Funktionen deutlich beschränkt und es entstehen Probleme, sobald erweiterte Kalenderfunktionen wie z.B. die Einberufung von Meetings genutzt werden. Das System der „öffentlichen Ordner" zur strukturierten Freigabe von

[1] Ehemals Hewlett-Packard und Compaq, fusioniert zu HP.

[2] Die wichtigsten Untersuchungskriterien waren hierbei: Sicherheit, Bedienbarkeit, Synchronisationsfähigkeit mit MS Exchange, Administrierbarkeit, Kosten.

Dateien lässt sich momentan nicht auf den PocketPC-Clients abbilden.[3] Postfach-Unterordner sind nicht abgleichbar[4], was zu teilweise erheblichen Problemen führt.

Um den iPAQ mobil unabhängig von einem Arbeitsplatz-PC und einer Basisstation (Cradle) zu machen, ist ein sogenanntes „Rucksack"-Modul (Jacket) notwendig, das GSM/GPRS-Funktionen nachrüstet. Dieses Rucksack-Modul ist unhandlich und wirkt unausgereift, worunter die Akzeptanz auf Endbenutzerseite leidet.

Die auf dem iPAQ vorhandenen Office-Programme wie PocketWord und PocketExcel verfügen lediglich über Basisfunktionen[5] und sind mit den großen Office-Paketen auf dem Arbeitsplatz nicht ansatzweise vergleichbar. Der Browser ist aufgrund der geringen Displaygröße und des eingeschränkten Darstellungsvermögens nur für gelegentlichen Einsatz geeignet. Die Texteingabe per Stift ist gewöhnungsbedürftig, beim Einsatz einer externen Tastatur leidet die Mobilität und damit die Akzeptanz auf Endbenutzerseite.

★ **Ergebnis 2: Die PocketPC-Plattform ist im Auslieferungszustand ohne zusätzliche Software aus Sicherheitsgründen im Behördenumfeld nicht einsetzbar.**

Begründung: Handhelds, insbesondere die PocketPCs, sind hauptsächlich für den Consumermarkt entwickelt worden. Deshalb stehen eher die Funktionen für diese Zielgruppe im Vordergrund, die Anforderungen eines Unternehmens oder einer Verwaltung werden nur teilweise erfüllt.

Bei der Untersuchung der mobilen Endgeräte haben wir eine Reihe von Bedrohungsszenarien identifiziert. Die wichtigsten Bedrohungen der Sicherheit sind dabei u.a.

- Verlust/Diebstahl des Endgeräts (Grundschutzhandbuch[6]: Ebene IT-Systeme und übergreifende Aspekte)
- Manipulation der Software und Hardware (Ebene IT-Systeme)
- Bedrohung durch Trojaner und Viren (Ebene IT-Systeme und übergreifende Aspekte)
- unzureichende Identifikation des Benutzers und des Geräts (Ebene Übergreifende Aspekte)
- Angriffe auf Kommunikationsverbindungen (Ebene Netze).

Die PocketPC-Plattform hat im Auslieferungszustand keine ausreichenden Schutzmaßnahmen, die geeignet wären, die genannten Bedrohungsszenarien auszuschließen.[7]

---

[3] Problem: Funktionsumfang der Synchronisationskomponente und des Endgeräts

[4] Problem: Leistungsfähigkeit des PocketPC-Betriebssystems

[5] Verfügbar sind einfache Textverarbeitungsfunktionen wie z. B. Texteingabe, Textformatierungen, Suchen/Ersetzen, nicht verfügbar sind Kopf- und Fusszeilen, Fussnoten, Indizes und Kommentare. Des weiteren kann immer nur ein Dokument gleichzeitig geöffnet werden.

[6] Das Grundschutzhandbuch des Bundesamts für Sicherheit in der Informationstechnik. Im IT-Grundschutzhandbuch werden Standardsicherheitsmaßnahmen für typische IT-Systeme empfohlen http://www.bsi.bund.de/gshb/deutsch/menue.htm [15.04.2003]

[7] Forschungen der Universität München (Lachmund 2003) bestätigen dies: „PDAs sind als Personal Trusted Device (PTD) nicht geeignet".

Problematisch ist dabei insbesondere der fehlende Multiuserbetrieb, die fehlende Verschlüsselung des Dateisystems und die fehlende Absicherung gegen unbefugten Zugriff. Dabei ist insbesondere das biometrische Authentifizierungssystem des iPAQ h5450 nicht geeignet, eine zuverlässige Identifikation des Benutzers und eine Abwehr unbefugter Personen sicherzustellen.

Aus unserer Sicht ist die PocketPC-Plattform insgesamt noch nicht ausgereift und sie wird sich, wenn überhaupt[8], erst in den nächsten Jahren zu einer sicheren Systemplattform für den professionellen Einsatz entwickeln. In der Zwischenzeit ist der Einsatz von Drittsoftware dringend notwendig.

★ **Ergebnis 3: Die momentan erhältliche und von uns getestete Zusatzsoftware löst einige, aber keinesfalls alle Schwächen der PocketPC-Plattform.**

Begründung: Es existieren zahlreiche Produkte von Drittanbietern, die versprechen, einige der systemimmanenten Schwächen der PocketPC-Plattform zu beheben. Wichtige Funktionen dieser Produkte sind: Verschlüsselung des Dateisystems und der Speicherkarten, zusätzliche Authentifizierungsmerkmale, Absicherung der Verbindung, Sperrung des Gerätes bei unautorisiertem Zugriff und zentrale Administration des Geräts durch die IT-Abteilung.

Insgesamt haben uns nur wenige der getesteten Systeme wirklich überzeugt. Die Software wirkt größtenteils nicht ausgereift und hat teilweise erhebliche Mängel[9]. Verhältnismäßig gute Leistungen bieten einige Tools in den Bereichen Absicherung der Kommunikation (VPN) und Administration[10]. Allerdings existieren auch dort gewisse Einschränkungen. Insbesondere kritisch sind das Fehlen eines überzeugenden Sicherheitskonzeptes bei der Administrationssoftware[11] und die Bedienung für den Endbenutzer (Usability). Außerdem konnte kein Hersteller eine Firewallsoftware bereitstellen, die das iPAQ-Endgerät bei Internetzugriff auf Netzwerkebene schützt.[12]

Die Sicherheitsmängel der PocketPC-Plattform sind folglich nur teilweise behebbar, störend sind dabei vor allem der frühe Entwicklungsstand mancher Produkte sowie die fehlende Integration der Zusatzsoftware in das System.

---

[8] „Die Fortentwicklung der aktuellen Endgeräte lässt eher eine Verringerung der Eignung als Personal Trusted Device vermuten“ (Lachmund 2003).

[9] Als untauglich erwiesen haben sich z.B. die Produkte PDA Secure, SafeGuard PDA und Sign On.

[10] Die Management-Komponente von Afaria.

[11] Afaria

[12] Die nächste Betriebssystemversion, „Windows CE .Net operating system“, („McKendric“) soll eine Firewall bereits integriert haben (für Mitte 2003 angekündigt).
http://www.computerworld.com/softwaretopics/os/story/0,10801,77527,00.html [01.04.2003]

★ **Ergebnis 4: Mobile Endgeräte müssen, vor allem wenn sie in größerer Zahl im Behördenumfeld eingeführt werden, aus Sicherheitsgründen zentral administriert werden. Es ist keine Administrationskomponente verfügbar, die den notwendigen Leistungsumfang bietet und dabei keine neuen Sicherheitsprobleme schafft.**

Begründung: Die zentrale Administration mobiler Endgeräte ist von großer Bedeutung. Nur wenn die Geräte zentral verwaltet werden, können Sicherheitslücken auch aus der Ferne geschlossen werden und der administrative Aufwand im Rahmen gehalten werden.

Berücksichtigt man nur die Administration der Endgeräte, bietet die Administrationssoftware Afaria den notwendigen Leistungsumfang. Allerdings stellt der Hersteller im Moment keine Proxy-Komponente zur Verfügung, so dass eine sichere Integration in Firewallkonzepte nicht möglich ist.

★ **Ergebnis 5: Bei der Benutzung der iPAQ-Endgeräte besteht ein unlösbarer Konflikt zwischen Bedienbarkeit und Sicherheit. Selbst die von uns herausgearbeitete Gesamtlösung ist nur bedingt zu empfehlen. Um diese in der Praxis für einen normalen Mitarbeiter nutzen zu können, sind erhebliche Abstriche bei der Sicherheit und/oder Administration notwendig.**

Begründung: Ein Ziel unseres Projekts war die Entwicklung einer Empfehlung, die die einzelnen getesteten Komponenten zu einem aus verschiedenen Perspektiven bestmöglichen Gesamtsystem zusammenfasst. Im Hinblick auf die Sicherheit ist ein solches Gesamtsystem mit Einschränkungen möglich, ein uneingeschränkt empfehlenswertes System konnte allerdings nicht herausgebildet werden. Ergänzend zum sicheren Einsatz mobiler Endgeräte sind in jedem Fall die Entwicklung organisatorischer Maßnahmen inkl. einer Sicherheitspolicy[13] notwendig.

Besonders problematisch ist aus unserer Sicht allerdings die Tatsache, dass die Integration verschiedener Sicherheitskomponenten[14] nur auf Kosten der Sicherheit möglich ist. In der Konsequenz muss ein Endbenutzer bis zu sieben Kennwörter eingeben und benötigt bis zu fünf Minuten, um einen Datenabgleich durchzuführen.

Das Fehlen einer integrierten Sicherheitslösung zwingt den Anwender mit hohen Sicherheitsanforderungen dazu, auf ein Patchwork von Sicherheitslösungen auszuweichen.

[13] Unter anderem: Verbindliche Richtlinien für Einsatz und Handhabung der mobilen Endgeräte, umfangreiche Schulungen und Einweisungen, Dokumentation, Kontrolle der Einhaltung der Policy.

[14] Essentiell notwendig sind aus unserer Sicht Produkte für die Dateisystemverschlüsselung (File Crypto), die Kommunikationsabsicherung (z. B. NCP VPN) und die Synchronisation (XTND).

Empfehlungen

Basierend auf den von uns durchgeführten Evaluationen und Tests stellen wir im folgenden Teil die von uns erarbeiteten Empfehlungen vor.

★ **Empfehlung 1: Aufgrund der festgestellten Einschränkungen können wir grundsätzlich nur ein Minimalsystem für den Betrieb der Endgeräte als mobiles Adressbuch, mobiler Kalender und für den gelegentlichen Austausch von E-Mails empfehlen. Dieses Szenario ist sinnvoll bei vorrangig lesendem Zugriff.**

Begründung: Für einfache Anwendungen z. B. als mobiles Adress- und Notizbuch, für lesenden Kalenderzugriff und für gelegentliches E-Mail-Abfragen kann diese Lösung durchaus empfohlen werden. In diesem Fall würde man ohne Administrationskomponente und mit ein bis zwei zusätzlichen Sicherheitskomponenten arbeiten. Mittelfristig wäre es sinnvoll, diese Variante mit der Afaria-Managementkomponente zu erweitern und evtl. gemeinsam mit dem Hersteller eine Proxy-Komponente zu entwickeln.

★ **Empfehlung 2: Grundsätzlich empfehlen wir für die Nutzung der Endgeräte als „mobiles Büro“, also bei lesendem und schreibendem Zugriff über den Einsatz in Verbindung mit einem Arbeitsplatz-PC hinaus, Mini- oder Subnotebooks mit einer vollwertigen Hard- und Softwareausstattung.**

Für einen wirklich mobilen Einsatz, also mit ständigem Zugriff im Sinne eines „mobilen Büros“, ist die PocketPC-Geräteklasse aus unserer Sicht aufgrund oben genannter Einschränkungen nicht geeignet. Für diesen Fall empfehlen wir, den Mitarbeiter mit Geräten der Kategorie Mini-/Sub-Notebooks auszustatten. Wie sehen dabei folgende Vorteile:

- Volles Softwareangebot inkl. Word, Outlook und Browser
- Vollwertiges Betriebssystem
- Funktionierende Administrationskonzepte
- Vollwertige Tastatur
- Großes Hardwareangebot
- Erprobte Plattform mit vielen Erfahrungen
- Einfache Erweiterung mit WLAN/Bluetooth/GSM/GPRS
- Roaming Profiles u.ä. sind möglich
- Zugriff auf Terminalserver/Remote Desktop ist möglich.

Aus unserer Sicht wird die etwas geringere Mobilität infolge des höheren Gewichts und des größeren Formats durch diese Vorteile aufgewogen. Insbesondere mit den neuartigen Centrino/mobile Pentium-Chips erwarten wir eine weitere Miniaturisierung.

Vergleicht man das Preis-/Leistungsverhältnis, sind die Sub-/Mini-Notebooks mit den iPAQs inkl. Rucksack-Modul konkurrenzfähig.[15] [16]

★ **Empfehlung 3: Außer den untersuchten Plattformen gibt es noch eine Reihe alternativer Lösungen mit eigenen Vor- und Nachteilen. Wir empfehlen, diese Lösungen einer genauen Prüfung zu unterziehen.**

Begründung: Es gibt eine Reihe von alternativen Entwicklungen sowohl im Bereich Hardware als auch Software. Im Bereich Software sind erste Linux-Systeme auf Basis der iPAQ-Plattform verfügbar. Im Hardwarebereich könnten die neuen leistungsfähigen Palm-Handhelds eine Alternative darstellen.[17] Hinzu kommen andere Systeme mit vorinstalliertem mobile Linux.[18]

Wir empfehlen, diese Alternativsysteme in Zukunft anhand der in diesem Evaluationsprojekt erarbeiteten Kriterien und identifizierten Schwachstellen zu untersuchen.

[15] Eine interessante Entwicklung in dieser Gerätekategorie sind die TabletPCs, die für den mobilen Betrieb geeignet sind und über eine leistungsfähige Handschriftenerkennung verfügen.

[16] Vielversprechend ist auch das „Micro-Notebook“ der Firma Vulcan. Das Notebook im Taschenbuch-Format verfügt über vollwertige PC-Hardware und Windows XP und wird für Ende des Jahres erwartet. http://www.heise.de/newsticker/data/dal-21.04.03-000/ [10.04.2003]

[17] Tungsten-Reihe von Palm

[18] Sharp Zaurus mit der Qtopia-Umgebung von Trolltech