



**„Einsatz mobiler Endgeräte – Risiko oder Chance?“
Erkennen von Risiken und Lösungsansätze für den effizienten Einsatz**

**Ein Positionspapier der Themengruppe
„Mobilität und Sicherheit“**

TeleTrusT Deutschland e.V.
Chamissostraße 11
99096 Erfurt



Inhaltsverzeichnis

1.	Einleitung	5
2.	Mobile Mediengesellschaft	5
3.	Mobile Endgeräte	5
3.1.	Aktive mobile Endgeräte	5
3.2.	Passive mobile Endgeräte	6
4.	Potentielle Bedrohungen und Gegenmaßnahmen	6
4.1.	Generelle Risiken und Gegenmaßnahmen.....	7
4.2.	Spezielle Risiken und Gegenmaßnahmen.....	10
4.2.1.	Privates mobiles Endgerät bei ausschließlich privater Nutzung.....	10
4.2.2.	Privates mobiles Endgerät bei dienstlicher Nutzung	11
4.2.3.	Dienstliches mobiles Endgerät bei privater Nutzung.....	12
4.2.4.	Dienstliches mobiles Endgerät bei dienstlicher Nutzung.....	13
4.3.	Checkliste der Sicherheitsmaßnahmen	15
5.	Zusammenfassung	17
6.	Glossar	18
7.	Über TeleTrust Deutschland e.V.	20
8.	Unterstützende Unternehmen	21



Das vorliegende Dokument wurde im Rahmen der Themengruppe „Sicherheit und Mobilität (MuS)“ unter der Mitwirkung folgender Firmen bzw. Institutionen und Autoren (alphabetische Reihenfolge) erstellt:

**Fraunhofer-Institut für Sichere
Informationstechnologie SIT**
Rheinstraße 75
64295 Darmstadt
www.sit.fraunhofer.de

Herr Mario Hoffmann
mario.hoffmann@sit.fraunhofer.de



**NetSys.IT
Information & Communication GbR**
Weimarer Str. 28
D-98693 Ilmenau
www.netsys-it.de

Herr Daniel Fischer
dfischer@netsys-it.de



noventum consulting GmbH
Münsterstraße 111
D-48155 Münster
www.noventum.de

Herr Stephan Wappler
stephan.wappler@noventum.de



Teleca Systems GmbH
Neumeyerstrasse 50
D-90411 Nürnberg
www.telecasystems.de

Herr Michael Bock
michael.bock@telecasystems.de



TeleTrusT Deutschland e.V.
Chamissostraße 11
D-99096 Erfurt
www.teletrust.de

Herr Peter Steiert
peter.steiert@teletrust.de



Utimaco Safeware AG
Hohemarkstraße 22
D-61440 Oberursel
www.utimaco.de

Herr Andreas Philipp
andreas.philipp@utimaco.de





Abkürzungen

CD	Compact Disc
DVD	Digital Versatile Disc
GB	Giga Byte
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
IrDA	Infrared Data Association
IT	Informationstechnologie
LAN	Local Area Network
MMC	Multi Media Card
PC	Personal Computer
PDA	Persönlicher Digitaler Assistent
PIN	Personal Identification Number
SD	Secure Digital
UMTS	Universal Mobile Telecommunications Systems
USB	Universal Serial Bus
WLAN	Wireless LAN



1. Einleitung

Die Unternehmen in Deutschland unterliegen einem steten Wandel. Der Dienstleistungsbereich wächst und mit ihm gewinnt die optimale Kundenbetreuung an Bedeutung. Die Rationalisierung in weiten Dienstleistungsbereichen erzwingt das Präsentieren und Verarbeiten aktueller Daten direkt vor Ort.

2. Mobile Mediengesellschaft

Mobilität ist nicht erst seit Versteigerung der milliardenteuren UMTS Lizenzen in den Vordergrund des allgemeinen Interesses gerückt. Wussten viele mit dem Wort „Multimedia“ Anfang der 90er Jahre noch nichts anzufangen, so ist Multimedia im Zuge der sich immer weiter verbreitenden PC's seit Anfang dieses Jahrzehnt ein fester Bestandteil in unserem Leben geworden.

Die Geschichte geht weiter und waren Laptops und Notebooks noch vor kurzem groß, schwer, teuer und langsam, so findet man heute in PDA's bereits mehr Rechenleistung und Speicherkapazität vor, wie am Anfang der mobilen Personalcomputer. Zum einen geht der Trend hin zur Miniaturisierung und zum anderen zu immer leistungsfähigeren Endgeräten, die durch die Mobilfunknetze der zweiten (GSM-Netze) und kommenden dritten Generation (UMTS-Netze) mit der ganzen Welt verbunden sind. So sind Tabellenkalkulation und das Navigieren im Internet mit den kleinen Assistenten kein Problem mehr. Die auf dem PC bekannten und bewährten Betriebssysteme finden sich auf den mobilen Geräten wieder und mit ihnen kommen auch die Applikationen wie Web-Browser, Textverarbeitung oder Tabellenkalkulation dazu.

3. Mobile Endgeräte

Mobile Endgeräte lassen sich in die Kategorien „Aktiv“ und „Passiv“ einteilen. Während Notebooks, PDA's und Smartphones auch Benutzereingaben zulassen, können die passiven Geräte wie z.B. MP3-Player, transportable Speichermedien und Digitalkameras vor allem zum Datenaustausch benutzt werden.

3.1. Aktive mobile Endgeräte

Die aktiven Endgeräte bringen für das Unternehmen dahingehend Vorteile, als sie bei Kundenbesuchen eingesetzt werden können und auch Dateneingaben zulassen. So können Aufträge vor Ort aufgenommen und über Mobiltelefon oder Festverbindung in den Betrieb zur Weiterverarbeitung übertragen werden. Ferner besteht neben der Möglichkeit E-Mails zu empfangen und abzusetzen auch Zugriff auf den elektronischen Kalender, der über Synchronisationsmechanismen mit der Betriebsumgebung abgeglichen wird.

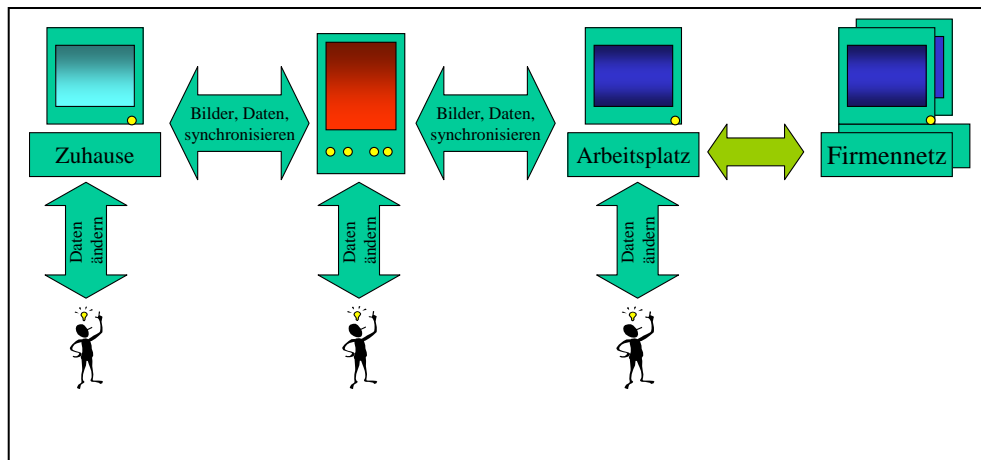


Abbildung 1: Übersicht Einsatzumgebung aktiver mobiler Endgeräte

3.2. Passive mobile Endgeräte

Zu den passiven mobilen Endgeräten zählen sämtliche Geräte, die über keine Eingabemöglichkeit des Benutzers verfügen und kein PC-Ersatz sind. Beachtet werden muß die Tatsache, das einige Geräte über mehrzeilige Displays verfügen und neben ihrer eigentlichen Aufgabe wie z.B. das Abspielen von Musik, auch die Mail- und Kalenderdatensynchronisation anbieten.

4. Potentielle Bedrohungen und Gegenmaßnahmen

Ziel des Dokuments ist auf die Gefahren hinzuweisen und Entscheidungshilfen zu geben, die sich durch die neue Herausforderung der bewussten oder unbewussten Einbeziehung mobiler Endgeräte in den Geschäftsprozess ergeben.

Für die Untersuchung potentieller Bedrohungsszenarien hinsichtlich des beschriebenen Gesamtsystems ist im ersten Schritt die Darstellung als Angriffsbaum¹ gewählt worden. Der hier entworfene Angriffsbaum ist bewusst ein pragmatischer Ansatz um eine erste fokussierte Sichtweise auf das Bedrohungspotential des Gesamtsystems zu erlangen.

¹ Schneier 1999

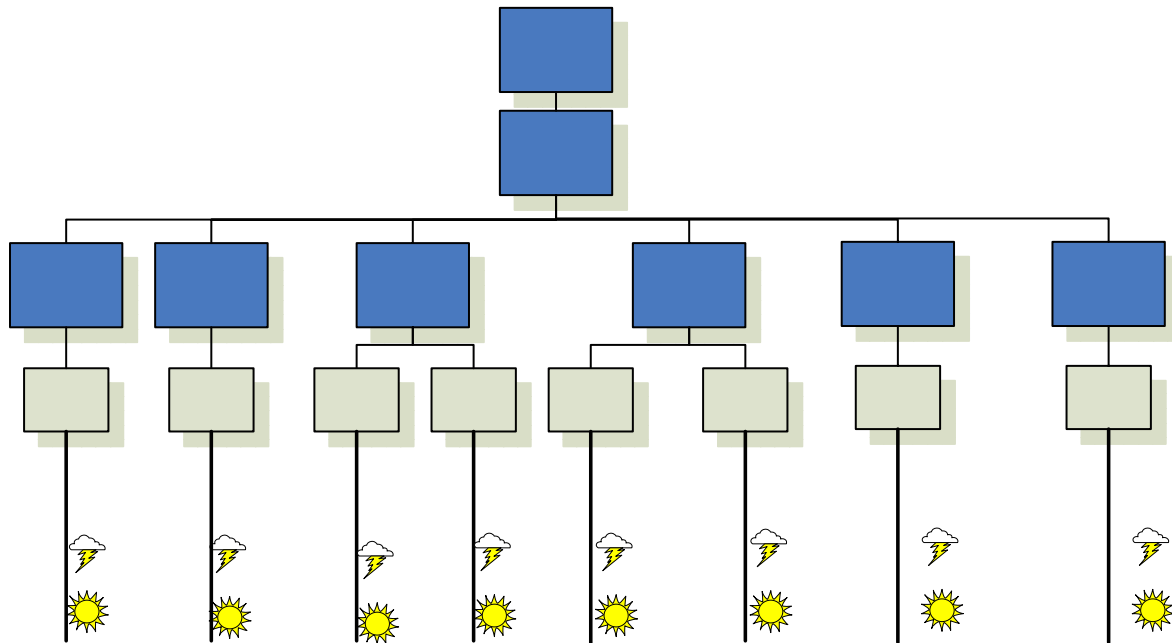


Abbildung 2: Übersicht Angriffsbaum mobiler Endgeräte

Die gewählte Darstellung der möglichen Bedrohungsszenarien in Form des „Angriffsbaums“ wurde von Bruce Schneier entwickelt. Durch die strukturierte Darstellung der in einem komplexen System beteiligten Komponenten (in dem vorliegenden Fall nur das Endgerät), und die Identifikation der einzelnen Anwendungen und Kommunikationsverbindungen, ist es möglich sich sehr schnell einen ersten umfassenden Überblick über die Sicherheit eines System zu verschaffen. Nach der Analyse der Systeme ist dann im weiteren eine Identifikation der möglichen Bedrohungen durchzuführen (in dem vorliegenden Fall ist der Fokus auf die die Nutzdaten und die Kennwörter gelegt), und diese schon dann im einem ersten Schritt zu beschreiben.

Der dargestellte „Angriffbaum“ erhebt allerdings keinen Anspruch auf Vollständigkeit, es wurden bewusst nur eine erste Übersicht über die allgemein zu definierenden Bedrohungen erstellt, da spezifische Anwendungen und Kommunikationswege nur projektspezifisch abzuleiten sind.

Betriebssysteme

Hardware

4.1. Generelle Risiken und Gegenmaßnahmen

Jedes mobile Endgerät birgt aufgrund der Bauweise, seinem Verwendungszweck (mobiler Datenspeicher) und dem Umgang mit dem mobilen Endgerät einige generelle Gefahren und Risiken für den Anwender bzw. für die Unternehmen.

Diese lassen sich nach den Zweigen des Angriffsbaums klassifizieren:

- Betriebssystem
- Nutzdaten/
Kennwörter
- Nutzdaten/
Kennwörter
- Nut
Ken



- Durch die Installation zusätzlicher Software auf dem mobilen Endgerät können Betriebssystemdateien modifiziert werden, so dass das mobile Endgerät verseucht ist mit
 - i. Trojanern,
 - ii. Viren oder
 - iii. Würmern
- Durch die Installation zusätzlicher Software auf dem mobilen Endgerät können Betriebssystemdateien so modifiziert werden, so dass das mobile Endgerät nicht mehr gebootet oder resetet werden kann und das Gerät defekt ist. Dies entspricht einem Denial of Service auf die Firmware.
- Hardware
 - Bei Verlust des mobilen Endgerätes kann das Gehäuse geöffnet und die Daten können direkt aus dem Speicher ausgelesen werden.
 - War das mobile Endgerät abgängig und wird dann als gefunden gemeldet, dann besteht die Möglichkeit, dass unberechtigte Dritte die Hardware so manipuliert haben, dass zum Beispiel die Wireless-Verbindungen immer im ungesicherten offenen Modus arbeiten, unabhängig von der Konfigurationseinstellungen des Anwenders.
- Authentisierung
 - In der Regel erfolgt die Authentisierung an einem mobilen Endgerät per PIN-Eingabe. Bei einem Gerät mit Touch-Screen können nach einiger Zeit die PIN-Möglichkeiten anhand der Kratzspuren auf dem Display eingegrenzt werden.
 - Nach erfolgreicher PIN-Eingabe hat der Anwender derzeit Administrationsrechte und somit uneingeschränkten Zugriff auf das mobile Endgerät.
- Applikation / Datenspeicherung
 - Da in der Regel keine Rechteverwaltung auf den derzeitigen mobilen Endgeräten implementiert ist, können alle Dateien vom mobilen Endgerät auf ein anderes Gerät, wie zum Beispiel einen privaten oder dienstlichen PC kopiert werden.
 - Wenn das mobile Endgerät auch nur kurze Zeit in einer unsicheren Umgebung außerhalb der Kontrolle des Anwenders ist und die Daten auf Wechselmedien gespeichert sind, z.B. SD-Cards oder Compact-Flash-Cards,
 - i. dann können die auf diesen Medien gespeicherten Daten sehr einfach durch Entnahme des Mediums, Auslesen der Daten und erneutes Stecken der Karte kopiert werden, ohne dass der Anwender dies bemerkt.
 - ii. dann können auf diesen Medien selbst installierende Programme durch unberechtigte Dritte gespeichert werden, die sich beim nächsten Einschalten des Geräts automatisch im Hintergrund installieren, ohne dass der Anwender dies bemerkt.



- Durch die gewollte oder auch ungewollte Installation von zusätzlicher Software auf dem mobilen Endgerät kann Schadsoftware aufgebracht werden,
 - i. die als Trojaner arbeitet,
 - ii. die alle Daten ausliest und per Internet an einen Dritten überträgt,
 - iii. kann der Firmen-PC bzw. das ganze Netzwerk angegriffen werden, ohne dass das mobile Endgerät selbst angegriffen wurde. Das mobile Endgerät funktioniert als Wirt in diesem Falle.
- Netzwerke
 - Eine elegante Möglichkeit zum Zugriff auf die mobil gespeicherten Daten ergibt sich, sobald das mobile Endgeräte über eine Wireless-Verbindung, (z.B. Bluetooth™) mit anderen Geräten wie zum Beispiel einem Mobiltelefon in einer unsicheren Umgebung (z.B. im Zug oder bei Kunden vor Ort) kommuniziert. Der Angriff auf das mobile Endgerät kann dann über verschiedene Punkte erfolgen.
 - i. Ein anderes Gerät kann bei einer ungesicherten offenen Verbindung Schadsoftware (Trojaner, Virus....) an das mobile Endgerät übertragen. Das mobile Endgerät kann als Wirt benutzt oder selbst angegriffen werden.
 - ii. Über die Wireless-Verbindung können weitere Geräte auf das mobile Endgerät zugreifen und Fehler in der Software ausnutzen.
 - iii. Die Datenübertragung zwischen den mobilen Endgeräten des Anwenders kann durch einen Dritten mit Hilfe eines Sniffers abgehört werden.

Jedoch lassen sich zum Schutz der privaten bzw. der Unternehmensinfrastruktur und der vertraulichen Daten Gegenmaßnahmen ableiten und gezielt einsetzen, um die beschriebenen allgemeinen Gefahren und Risiken auf eine kalkulierbares und akzeptables Minimum zu reduzieren:

- Die Anwender mobiler Endgeräte sind hinsichtlich ihrer höheren Eigenverantwortung und eines bewussteren Einsatzes gezielt aufzuklären, zu schulen und zu sensibilisieren.
- Das Gerät sollte immer unter Kontrolle der Anwender sein.
- Die Passwörter bzw. PIN's sollten regelmäßig geändert werden.
- Die Datenspeicherung im generellen und im speziellen auf Wechselmedien sollte grundsätzlich nur verschlüsselt erfolgen.
- Wiederaufgefundene abgängige mobile Endgeräte sollten einen gründlichen Check bezüglich ihrer Unversehrtheit im Bezug auf die Hardware, das Betriebssystem und der installierten Applikationen unterzogen werden, bevor sie wieder mit privaten oder Unternehmens-PC's synchronisiert und eingesetzt werden.
- Ungesicherte, offene Kommunikationsverbindungen sind grundsätzlich nicht empfehlenswert und sollten unterbunden werden.



- Es sollte regelmäßig geprüft werden, ob die Standardsicherheitsmechanismen um Zusatzsoftware ergänzt werden können. Dies betrifft zum Beispiel die Authentifizierungs- und Kryptofunktionalitäten.
- Der Einsatz spezieller Viren-Scanner für diese mobilen Endgeräte (soweit verfügbar) ist absolut empfehlenswert.
- Begleitend sind die Nutzung und die Integration mobiler Endgeräte in die Unternehmensprozesse und in die Sicherheitsrichtlinien aufzunehmen und sind in einer Betriebsvereinbarung zu regeln. Darin sind beispielsweise Verantwortlichkeiten bei Schadensfällen und der Einsatz von unternehmenseigenen und eventuellen privaten Software-Lizenzen zu klären.

Fazit: Mobile Endgeräte haben aus Anwendersicht eine Vielzahl von Vorteilen und sind aus diesem Grund sehr beliebt. Wenn die entsprechenden Gegenmaßnahmen beachtet und umgesetzt werden, dann können die beschriebenen Risiken auf ein Minimum reduziert werden. Ob dieses Restrisiko akzeptabel ist, muss jeder Anwender bzw. jedes Unternehmen für sich selbst entscheiden. Diese Entscheidung ist im Besonderen auch von den speziellen Einsatzszenarien und den auf den mobilen Endgeräten gespeicherten Daten abhängig.

4.2. Spezielle Risiken und Gegenmaßnahmen

Um die speziellen Risiken erkennen und entsprechende Gegenmaßnahmen umsetzen zu können, ist es notwendig zwischen der Herkunft und der Nutzung des mobilen Gerätes zu unterscheiden.

Einsatz Mobiles Endgerät	PRIVAT	DIENSTLICH
PRIVAT	Wird nicht betrachtet	Subtil, keine oder kaum Kontrolle
DIENSTLICH	Eingeschränkte Kontrolle	Beste Kontrolle

Abbildung 2: Schematische Einteilung Eigentum vs. Einsatzzweck mobiles Endgerät

4.2.1. Privates mobiles Endgerät bei ausschließlich privater Nutzung

Dieses Szenario, bei dem z.B. der private PDA mit dem privaten PC synchronisiert wird, wird nicht beleuchtet, denn hier ist die Gefahreinschätzung auf den Privatmann beschränkt. Die sich ergebenden



Gefahren und Gegenmaßnahmen können aus den folgenden speziellen Szenarien und der allgemeinen Risikobeschreibung abgeleitet werden.

4.2.2. Privates mobiles Endgerät bei dienstlicher Nutzung

In Unternehmen, in denen noch kein eigenes Sortiment an mobilen Endgeräten existiert, lässt sich ein kritischer Trend identifizieren: Viele Mitarbeiterinnen und Mitarbeiter haben längst den Nutzen mobiler Endgeräte als jederzeit verfügbaren Datenspeicher und Kommunikations-Tausendsassa erkannt. Ohne Sorge vertrauen sie zunehmend vertrauliche Informationen ihrer Kundenbeziehungen, interne Geschäftsprozesse und Unternehmensgeheimnisse ihren privaten zumeist ungesicherten Geräten an. Sollten Sie dies in Ihrem Unternehmen beobachten, besteht sofortiger Handlungsbedarf!

Die dienstliche Nutzung privater mobiler Endgeräte birgt gleich mehrere hohe Gefahrenpotentiale und Risiken für das Unternehmen:

- Die Geräte entziehen sich weitgehend der expliziten Kontrolle durch die IT-Administratoren des Unternehmens.
- Schadsoftware wird am Arbeitsplatz unbemerkt von jeglicher Firewall in das interne Unternehmensnetz eingeschleust, wodurch vertrauliche Daten kompromittiert werden können und Schaden an der Unternehmens-IT entstehen kann.
- Durch die nicht vorhersehbare Heterogenität und Fluktuation an mobilen Endgeräten entsteht zudem ein erhöhter Integrations- und Verwaltungsaufwand.
- Die Zertifizierung nach BS7799, BASEL II und weiteren nicht nur für die Reputation entscheidenden Kriterienkatalogen wird im Zweifel abgelehnt oder wieder aberkannt.

Ohne Zweifel: Mittelfristig gilt es aufgrund des hohen Bedarfs, eine unternehmensweite Strategie zur Einführung dienstlich genutzter mobiler Endgeräte umzusetzen, auf die wir im Abschnitt „Dienstliche Endgeräte im dienstlichen Einsatz“ näher eingehen. Kurzfristig lassen sich darüber hinaus zum Schutz der Unternehmensinfrastruktur und vertraulicher Daten einige Sofortmaßnahmen ableiten und gezielt einsetzen:

- Private Endgeräte sollten so bald wie möglich und in regelmäßigen Abständen Sicherheitschecks unterzogen werden.
- Ein mittelfristiger Umstieg auf unternehmenseigene mobile Endgeräte für die dienstliche Nutzung sowie eine zentrale Administration ist aus unserer Sicht mehr als empfehlenswert.

Fazit: Die Duldung der dienstlichen Nutzung privater Endgeräte bringt für Unternehmen lediglich kurzfristige Kostenvorteile. Mittelfristig lohnt sich jedoch für alle Beteiligten sowohl aus organisatorischer als auch aus sicherheitstechnischer Sicht die Einführung von dienstlichen mobilen Endgeräten zur (ausschließlich) dienstlichen Nutzung. Diese Konstellation behandelt ausführlich der entsprechende Abschnitt.



4.2.3. Dienstliches mobiles Endgerät bei privater Nutzung

Ein wesentlicher Beweggrund für die Einführung von mobilen Endgeräten in Organisationen besteht in der besseren Koordination der geschäftlichen Termine der Mitarbeiter und der Bereitstellung von Adress- und Kontaktdaten für den Außendienst. Ziel ist die Synchronisation der geschäftlichen Termini der Mitarbeiter mit einem zentralen Terminkalender um somit einen Überblick über die Verfügbarkeit der Mitarbeiter und die durchgeführte und anberaumten Geschäftstermine zu gewährleisten. Weiterhin werden auch die Adressdaten zwischen der zentralen Adressdatenbank der Organisation und den mobilen Endgeräten synchronisiert, umso schneller Änderungen von Adressdaten bzw. Ansprechpartnern in der Organisationszentrale zu erhalten.

Anwender, die von den Vorteilen eines mobilen Endgeräts insbesondere von den Annehmlichkeiten des Terminkalenders und der schnellen Verfügbarkeit von Adressdaten überzeugt sind, kommen früher oder später auf die Idee, das dienstliche mobile Endgerät auch mit dem auf dem privaten PC gepflegten Terminkalender bzw. der dort gespeicherten Adressen und Kontakte zu synchronisieren. Diese Idee wird noch beschleunigt, wenn der Nutzer bereits mehrfach Konflikte mit privaten Terminen aufgrund der Nichtverfügbarkeit des privaten Terminplaners bei Terminvereinbarungen mit Kunden lösen musste. Das für die Datenverbindung zwischen dem dienstlichen mobilen Endgerät und dem privaten PC benötigte Equipment (z.B. Kabel) ist über den einschlägigen Fachhandel oder über das Internet problemlos beziehbar. Weiterhin werden eine Vielzahl von Softwareprodukten für die Synchronisation von Adressbüchern, Terminkalendern und des Posteingangs im Internet als Freeware, Shareware oder kommerzielle Software zum Download angeboten. Oftmals muss diese Software nicht nur auf dem privaten PC installiert werden, sondern erfordert für den vollen Funktionsumfang eine zusätzliche Softwareinstallation auf dem mobilen Endgerät.

Die private Nutzung dienstlicher mobiler Endgeräte birgt Gefahrenpotentiale und Risiken für das Unternehmen:

- Datenspeicherung
 - Durch die Synchronisation der Termin- und Adressdaten des Unternehmens auf dem privaten PC entziehen sich diese der expliziten Kontrolle durch die IT-Administratoren des Unternehmens.
- Applikation
 - Durch die Datenverbindung zwischen privaten PC und mobilen Endgerät kann das mobile Endgerät mit Schadsoftware infiziert werden..
 - Durch die Synchronisation privater E-Mails vom privaten PC auf das mobile Endgerät und von dort auf den dienstlichen PC kann der dienstliche PC bzw. das gesamte Netzwerk mit Schadsoftware infiziert werden. Alle zentralen Viren- und Contentscanner des Unternehmens werden in diesem Falle umgangen und haben keine Zugriffsmöglichkeiten



auf diese übertragenen Daten. Schadsoftware kann somit am Arbeitsplatz unbemerkt von jeglicher Firewall in das interne Unternehmensnetz eingeschleust, wodurch vertrauliche Daten kompromittiert werden können und Schaden an der Unternehmens-IT entstehen kann.

Die private Nutzung dienstlicher mobiler Endgeräte birgt nicht nur hohe Gefahrenpotentiale und Risiken für das Unternehmen sondern auch für den Anwender:

- Datenspeicherung
 - Durch die Synchronisation der dienstlichen und privaten Termin- und Adresdaten mit dem dienstlichen PC entziehen sich diese der expliziten Kontrolle durch den Anwender.
 - Da in der Regel keine Rechteverwaltung auf den derzeitigen mobilen Endgeräten implementiert ist, können alle Dateien vom mobilen Endgerät auf ein anderes Gerät, wie zum Beispiel den dienstlichen PC kopiert werden. Dies entspricht einem Komplettbackup aller mobilen Endgeräte Daten und somit erlangt das Unternehmen die privaten Adresdaten, selbst wenn die Daten als privat und nicht synchronisierbar gekennzeichnet sind.

An den Vorteilen und der Sinnhaftigkeit des Einsatzes dienstlicher mobiler Endgeräte aus Organisations-sicht bestehen keine Zweifel. Begleitend zur Einführung und im Betrieb mobiler Endgeräte sind zum Schutz der Unternehmensinfrastruktur und der vertraulichen Daten begleitende Maßnahmen zu definieren und umzusetzen:

- Dienstliche mobile Endgeräte sollten in regelmäßigen Abständen Sicherheitschecks unterzogen werden.
- Das Verbot der privaten Nutzung mobile Endgeräte sowie eine zentrale Administration ist aus unserer Sicht absolut empfehlenswert.

Fazit: Die Duldung der privaten Nutzung dienstlicher Endgeräte birgt für das Unternehmen hohe Risiken. Unbestritten lohnt sich jedoch für alle Beteiligten sowohl aus organisatorischer als auch aus sicherheitstechnischer Sicht die Einführung von dienstlichen mobilen Endgeräten zur ausschließlich dienstlichen Nutzung. Die private Nutzung dienstlicher mobiler Endgeräte ist aus Organisationssicht sowohl organisatorisch (z.B. per Policies / Richtlinien / Arbeitsanweisungen) und technisch (z.B. Überwachung der installierten Software auf dem mobilen Endgerät) zu untersagen.

4.2.4. Dienstliches mobiles Endgerät bei dienstlicher Nutzung

Werden mobile Geräte den Mitarbeitern durch die jeweiligen Organisationen gestellt, so können diese in die Sicherheitspolicy und Sicherheitsrichtlinien der jeweiligen Organisation eingebunden werden. Im Gegensatz zu privaten Geräten, die dienstlich genutzt werden, kann den Mitarbeitern der Einsatz und der Umgang mit den mobilen Endgeräten vorgeschrieben werden.



Die Existenz und Entwicklung von Organisationen ist immer häufiger an die Qualität, Verfügbarkeit und Vertraulichkeit ihrer Daten gekoppelt. Sind Daten nicht mehr existent, vertraulich oder intakt, dann kann eine Organisation innerhalb kürzester Zeit in finanzielle Schwierigkeiten geraten. Dies wird immer häufiger auch dem Management bewusst. Das Bewusstsein muss allerdings noch weiter geschärft werden, da nicht nur die organisationsinternen Daten sondern auch die Daten von Außendienstmitarbeitern einer organisationskritischen Relevanz unterliegen. Dies wird meist erst dann erkannt, wenn die mobil gespeicherten Daten verloren, d.h. z.B. gelöscht oder im noch schlimmeren Fall Unbefugten in die Hände gelangt sind

Auch der ausschließliche dienstliche Einsatz von mobilen Endgeräten birgt Gefahrenpotentiale und Risiken für das Unternehmen, die zum Verlust, Missbrauch und Manipulation von Daten führen können.



- Datenspeicherung
 - Da in der Regel keine Rechteverwaltung auf den derzeitigen mobilen Endgeräten implementiert ist, können alle Dateien vom mobilen Endgerät auf ein anderes Gerät, wie zum Beispiel einen privaten PC kopiert werden, wenn das mobile Endgerät + Passwort oder die Zugriffs-PIN in die Hände unbefugter Dritter gelangt sind.

An den Vorteilen und der Sinnhaftigkeit des ausschließlich dienstlichen Einsatzes mobiler Endgeräte aus Organisationssicht bestehen keine Zweifel. Begleitend zur Einführung und im Betrieb mobiler Endgeräte sind zum Schutz der Unternehmensinfrastruktur und der vertraulichen Daten begleitende Maßnahmen zu definieren und umzusetzen:

- Dienstliche mobile Endgeräte sollten in regelmäßigen Abständen Sicherheitschecks unterzogen werden.
- Das Verbot der privaten Nutzung mobile Endgeräte sowie eine zentrale Administration ist absolut empfehlenswert.

Fazit: Auch der ausschließliche dienstliche Einsatz mobiler Endgeräte birgt für die Organisationen Risiken. Unbestritten lohnt sich jedoch für alle Beteiligten sowohl aus organisatorischer als auch aus sicherheitstechnischer Betrachtung die Einführung mobiler Endgeräte zur ausschließlich dienstlichen Nutzung. Bei der ausschließlich dienstlichen Nutzung mobiler Endgeräte sind sowohl organisatorische (z.B. per Policies / Richtlinien / Arbeitsanweisungen) als auch technische (z.B. Überwachung der installierten Software auf dem mobilen Endgerät, eindeutige Festlegung der zu synchronisierenden Daten je Anwender und/oder Endgerät) Vorgaben zu definieren und umzusetzen.

4.3. Checkliste der Sicherheitsmaßnahmen

Zusammenfassend sind Bedrohungs-Szenarien und die damit verbundenen Maßnahmen in Form einer Checkliste zusammengefasst die, es erlaubt sich sehr schnelle bei geplantem oder auch schon bestehendem Einsatz von Mobilien Endgeräten im Unternehmen ein erstes Bild über den Sicherheitsstand zu erarbeiten. Es ist immer darauf zu achten das der Bezug für die geplanten Anwendungen hergestellt ist, und die in Kapitel 4 beschreibenden Einsatz-Szenarien einbezogen werden.

Somit sind die Bedrohungen und die daraus resultierenden Bewertungen immer im Kontext der Anwendung zu sehen. Folgende Bewertungs-Maßstäbe sind definiert:



Bewertung: hoch

Diese Bedrohung ist in meinem spezifischen Anwendungsfall unternehmenskritisch und ist als hoch einzustufen. Ich muss schon im aktuellen Status des Projektes umgehend prüfen ob hier hinreichende Sicherheitsmaßnahmen getroffen wurden.

Bewertung: mittel

Diese Bedrohung ist in meinem spezifischen Anwendungsfall erst im Rahmen der Umsetzung als kritisch einzustufen. Ich muss bei der geplanten Einführung von Mobilien Endgeräten darauf achten das für diese Bedrohung hinreichend Sicherheitsmaßnahmen umgesetzt werden. Ansonsten ist hier einem Sicherheitsrisiko zu erwarten.

Bewertung: niedrig

Diese Bedrohung ist in meinem spezifischen Anwendungsfall als nicht kritisch einzustufen. Sie sind weder unternehmenskritisch, noch müssen Sofortmaßnahmen getroffen werden. Bei der Planung der Einführung von Mobilien Endgeräten ist diese Art von Bedrohungen zu beachten, wird aber nur mit niedriger Priorität verfolgt.



Bereich	Bedrohung	Technische Maßnahmen	Bewertung der Bedrohung (hoch / mittel / niedrig)
Betriebssysteme	Sniffer und Trojaner die das Betriebssystem angreifen	Einführung von Virens Scanner und Personals Firewalls	
Hardware	Verlust oder Diebstahl ermöglichen potentiellen Angreifen das Auslesen von sensitiven Daten	Verschlüsselung der Daten oder des Speichers	
Authentifizierung	Ausspähen von Passwörtern oder Einsatz von unzureichenden Authentifizierungsmaßnahmen	Sensibilisierung der Endbenutzer, Einsatz von Zusatzsoftware für starke Authentifizierungs-Verfahren	
Applikation	Ausnutzung von Bugs in der Applikation	Regelmäßige Updates durch die interne IT	
	Passwortanalyse aus dem Filesystem	Einsatz von Zusatzsoftware zur Verschlüsselung des Dateisystems oder des Datenspeichers	
Netzwerke (öffentliche)	Abhören der Verbindungen mit dem Zweck an die Nutzdaten wie Kennwörter oder Daten zu gelangen	Einsatz von Firewalls, VPN (zertifikatsbasiert) und durch Portkontrolle auf dem Client	
Netzwerke (Intranet)	Einsatz von nicht befugten Endgeräten im Intranet; Gefährdung von Firmen internen Daten und Netzwerke	Einsatz von Firewalls, VPN Systemen	

Tabelle 1: Checkliste für den Einsatz mobiler Endgerät

5. Zusammenfassung

Es gibt einen sehr breiten Einsatzbereich für mobile Endgeräte in Organisationen mit einem sehr hohen Einspar- und Optimierungspotential, vorausgesetzt die organisatorischen und technischen Rahmenbedingungen für den Einsatz wurden entsprechend analysiert und angepasst. Der schleichende Einsatz privater mobiler Endgeräte sollte genauso unterbunden werden, wie die private Mitbenutzung dienstlicher mobiler Endgeräte. Das Risikopotential ist nicht unbeträchtlich und kann teilweise nicht abgeschätzt werden, da es auch von der individuellen Einsatzumgebung der mobilen Endgeräte abhängig ist und diese



umfasst auch die privaten Arbeitsplätze der Anwender. Diese privaten Arbeitsplätze sind aus Organisations-sicht unkontrollierbar und somit als unsichere Umgebung einzustufen.

Auch der ausschließliche dienstliche Einsatz mobiler Endgeräte birgt gewisse Gefahren und Risiken für die Organisationen. Jedoch bei einem gut geplanten und überlegten Einsatz mobiler Endgeräte lassen sich eine Vielzahl der unkalkulierbaren Risiken auf ein akzeptables, kalkulierbares Minimum reduzieren. Dies setzt jedoch voraus, dass umfangreiche organisatorische und technische Maßnahmen definiert und umgesetzt werden. Dies umfasst im technischen Bereich unter anderem den Einsatz von Viren-Scannern, zentrale Administration, usw. und im organisatorischen Bereich die Schulung der Mitarbeiter, regelmäßige Sicherheitsüberprüfungen. Definition von Policies und Richtlinien, usw.. Die erforderlichen Maßnahmen sind im starken Maße von der individuellen Einsatzumgebung der mobilen Endgeräte und der darauf gespeicherten und zu verarbeitenden Daten abhängig.

Im Zweifelsfall ist es ratsam externe Spezialisten hinzuzuziehen und die Funktionalitäten der auf dem mobilen Endgerät installierten Applikationen und Betriebssysteme mit spezieller Zusatzsoftware zu ergänzen.

Der ausschließlich dienstliche Einsatz mobiler Endgeräte unter Beachtung der angeführten technischen und organisatorischen Maßnahmen einschließlich einer Risikoabschätzung ist aus unserer Sicht bereits heute sehr gut möglich und empfehlenswert.

6. Glossar

Anwendungen	Computerprogramm, mit dem der Anwender seine Aufgaben erledigt.
Applikationen	Siehe Anwendungen
Audit	Siehe Sicherheitschecks
Backup	Siehe Datensicherung
BASEL II	Mit dem Stichwort "Basel II" wird die Diskussion um die Neugestaltung der Eigenkapitalvorschriften der Kreditinstitute bezeichnet (Initiative des Basler Ausschuss für Bankenaufsicht im Juni 1999 eröffnet). Ziel von "Basel II" ist es, die Stabilität des internationalen Finanzsystems zu erhöhen. Dazu sollen die Risiken im Kreditgeschäft besser erfasst und die Eigenkapitalvorsorge der Kreditinstitute risikogerechter ausgestaltet werden. Das bedeutet im Kern, dass die Kreditinstitute zukünftig umso mehr Eigenkapital vorhalten sollen, je höher das Risiko des Kreditnehmers ist, an den sie einen Kredit vergeben.
Betriebssystem	Computerprogramm, das die grundlegende Verwaltung anderer Programme übernimmt und die dabei notwendigen Routinen zur Verfügung stellt.
Bluetooth	Drahtlose Kommunikation auf kurzen Entfernungen. Dient vorrangig als Kabelersatz bei der Einbindung unterschiedlicher Geräte. Der Datendurchsatz ist geringer als bei WLAN. Es bietet jedoch ausgefeilte Sicherheitsmechanismen sofern diese implementiert und verwendet werden.



BS 7799, ISO17799	BS7799 ist der Britische Standard für die Implementierung und Wartung eines Information Security Management Systems, aus dem die ISO 17799 abgeleitet wurde. Der Ansatz ist, die größten Risiko- Faktoren, denen Ihre Organisation ausgesetzt ist, zuerst zu adressieren. Das Ziel besteht darin, Management und Investoren transparent machen zu können, dass die Security Budgets sinnvoll verwendet werden.
Datensicherung	Verfahren zur langfristigen Speicherung von Daten und deren Wiederherstellung nach dem Datenverlust.
GSM, UMTS	Mobilfunknetz, ursprünglich für Telefongespräche konzipiert, ist Echtzeitfähig und bietet große Reichweite bei gleichzeitig nahtloser Übergabe der Kommunikation. Der Durchsatz ist gegenüber WLAN um ein Vielfaches geringer.
Malware	(Quelle BSI: http://www.bsi.bund.de/literat/faltbl/F19Kurzviren.htm) Alle Arten von Programmen, die verdeckte Funktionen enthalten und damit durch Löschen, Überschreiben oder sonstige Veränderungen unkontrollierbare Schäden an Programmen und Daten bewirken und somit zusätzliche Arbeit und Kosten verursachen oder Vertraulichkeit und Verfügbarkeit von Daten oder Programmen negativ beeinflussen.
Mobile Geräte	Zusammenfassung von Smartphones, PDAs und Notebooks unter diesem Begriff.
Notebook	Tragbarer Computer, der zur Ausführung von Anwendungen dient. Im Vergleich zum PDA um ein vielfaches größer und schwerer, dafür aber leistungsfähiger und mit Tastatur ausgestattet.
Operating System (OS)	Siehe Betriebssystem
PDA	Steht für "Personal Digital Assistent" - und bezeichnet einen handlichen, flachen Computer den man in der Hand halten kann, daher auch Handheld genannt. Dieser bietet die Möglichkeit lokale Anwendungen auszuführen.
Sicherheitschecks	Durch unabhängige Personen oder Organisationen regelmäßig durchgeführte Prüfungen von IT-Infrastrukturen oder Teilen davon. Ziel ist die Einhaltung einer vorgegebenen Sicherheitspolicy beziehungsweise die Aufdeckung von Verstößen gegen diese.
Sicherheitspolicy	Organisationsweit gültige Vorgabe, wie mit Daten, Programmen und Infrastrukturen umzugehen ist. Dabei werden die notwendigen Prozesse und technischen Vorgaben festgelegt, die Mitarbeiter einzuhalten haben. Die Kontrolle ob dies zutrifft, erfolgt über Sicherheitschecks/Audits.
Smartphone	Vereinigung des Leistungsumfangs eines PDA mit einem Mobiltelefon. Smartphones haben bieten die Fähigkeit, im Mobilfunknetz zu telefonieren (wie ein Mobiltelefon), andererseits haben sie auch die Fähigkeit, als kleiner Computer Anwendungen auszuführen, wie bei einem PDA.
Synchronisation	Technischer Prozess um zwei Objekten die gleiche Datenbasis zur Verfügung zu stellen.
Trojaner, Trojanische Pferde	(Quelle BSI: http://www.bsi.bund.de/literat/faltbl/F19Kurzviren.htm) Selbständiges Programm mit einer verdeckten Schadensfunktion, ohne Selbstreproduktion.



Verschlüsselung	Technisches Verfahren, die einzelnen Daten werden dabei so durcheinander gebracht, dass sie nur vom Eigentümer mit dem persönlichen Schlüssel wieder in den Ausgangszustand gebracht werden können.
Viren:	(Quelle BSI: http://www.bsi.bund.de/literat/faltbl/F19Kurzviren.htm) Ein Computer-Virus ist eine nicht selbstständige Programmroutine, die sich selbst reproduziert und dadurch vom Anwender nicht kontrollierbare Manipulationen in Systembereichen, an anderen Programmen oder deren Umgebung vornimmt. <i>Eine nicht selbstständige Programmroutine bedeutet, dass der Virus ein Wirtsprogramm benötigt. Diese Eigenschaft und seine Befähigung zur Reproduktion führte in Analogie zum biologischen Vorbild zu der Bezeichnung "Virus".</i>
WLAN/Wireless Lan (IEEE 802.11 (a/b/g))	Drahtloses Netzwerk mit hohem Durchsatz, bei geringer Reichweite (max. 1-2 km, meist 100-300 m). Echtzeitfähigkeit und nahtlose Übergabe der Kommunikation zwischen den Sendestationen sind implementiert.
Wurm:	(Quelle BSI: http://www.bsi.bund.de/literat/faltbl/F19Kurzviren.htm) Selbstständiges, selbst reproduzierendes Programm, das sich in einem System (vor allem in Netzen) ausbreitet.

7. Über TeleTrust Deutschland e.V.

TeleTrust Deutschland e.V. wurde 1989 gegründet und ist heute ein Kompetenzverbund für angewandte Kryptographie und Biometrie aus über 90 institutionellen Mitgliedern.

Sein Ziel ist die Unterstützung von Entwicklung und Verbreitung vertrauenswürdiger Informations- und Kommunikationstechnik, sie nutzender Applikationen sowie Dienste zu deren Unterstützung. Durch diese Förderung sollen Geschäftsprozesse in Wirtschaft und Verwaltung mit unterschiedlichsten Sicherheitsanforderungen individuell vertraulich, fälschungssicher, nachprüfbar und beweiskräftig auf der Basis elektronischer Kommunikation, Datenverarbeitung und Datenarchivierung betrieben werden können. Hierbei ist die Zusammenarbeit mit Institutionen aus anderen Ländern eine wichtiges Anliegen, um Ziele und Standards in der Europäischen Union zu harmonisieren.

Die inhaltliche Arbeit wird von Experten der Mitgliedsunternehmen in derzeit 7 Arbeits- und 2 Themengruppen, 2 Services und 2 Projekten geleistet. Deren Ergebnisse werden der Öffentlichkeit zugänglich gemacht und darüber hinaus der Dialog zwischen technischen und juristischen Disziplinen, dem Daten- und Verbraucherschutz sowie der Politik zur Notwendigkeit einer umfassenden Anwendung von geeigneten Kryptoverfahren für Informations- und Kommunikationssicherheit wirksam gefördert.



8. Unterstützende Unternehmen

Fraunhofer-Institut für Sichere Informationstechnologie SIT

Bei der Nutzung der Informationstechnologie wird IT-Sicherheit immer stärker zum entscheidenden Erfolgsfaktor. Bei der zukunftsfähigen Gestaltung von Diensten, Prozessen und Infrastrukturen gilt es deshalb stets, Sicherheitsinteressen von Kunden und Geschäftspartnern zu berücksichtigen. Diese marktgerechte, skalierbare IT-Sicherheit steht im Zentrum der Arbeit am Fraunhofer-Institut für Sichere Informationstechnologie SIT.

Ziel des Instituts ist die Ausrichtung der IT-Sicherheit an den tatsächlichen Bedürfnissen der Partner. Erst durch diese ganzheitliche Herangehensweise ergeben sich innovative, nachhaltige Lösungen. Solche IT-Sicherheit kann sich sogar oft als befördernder Faktor erweisen, der Unternehmen neue Anwendungsfelder erschließt und Marktanteile dauerhaft sichert. Dabei gilt: Je früher IT-Sicherheit in die Prozesse integriert wird, desto zukunftsfähiger und effizienter sind die entsprechenden Systeme. So wird Sicherheit zum klaren Marktvorteil.

Eine besondere Stärke des Instituts stellt die Kompetenz in der Sicherheit mobiler Systeme und Endgeräte dar. Die unmittelbare Beteiligung des Instituts an der aktuellen Forschung verschafft seinen Partnern hierbei einen großen Wissensvorsprung, zum Beispiel in der Gestaltung sicherer Funk- und Mobilfunk-Netze sowie entsprechender Schnittstellen und sicherer mobiler Arbeitsumgebungen.

NetSys.IT Information & Communication GbR

Die NetSys.IT Information & Communication GbR als innovative IT-Dienstleistungsagentur entwickelt individuelle Informations- und Kommunikationslösungen und erbringt dazu qualifizierte IT-Dienstleistungen mit einer starken Ausrichtung auf Internet- und Security-Technologien.

Unser Ziel ist es, zusammen mit unseren Kunden, durch professionelle Produkte und Dienstleistungen Informations- und Kommunikationssysteme effizienter und sicherer zu gestalten. Zu unserem Dienstleistungsangebot im IT-Security-Umfeld gehört neben der Beratung, Konzeption und Neuentwicklung von individuellen Lösungen zum Einsatz von Kryptografie (Verschlüsselung, Signatur) insbesondere die Integration kryptografischer Methoden in bestehende Geschäftsprozesse und deren unterstützende Anwendungssysteme. Zu den durch uns eingesetzten technischen Konzepten und Lösungen gehören dazu unter anderem: Dateisystemverschlüsselung, E-Mail-Verschlüsselung/-signatur, VPN, SSL/TLS, Sign On (SO), Single Sign On (SSO), Keyrecovery, Backuprecovery,, Biometrische Lösungen, Bridge-CA Konzepte zum Aufbau vertrauenswürdiger Kommunikation zwischen Unternehmen und Verwaltungen, Crosszertifizierung.



noventum consulting GmbH

Die noventum consulting GmbH ist ein vielseitiges Beratungsunternehmen im bundesweiten und internationalen Markt für Groß- und gehobene mittelständische Unternehmen. Betriebswirtschaftliche Organisationslösungen von der Konzeption bis zur Realisierung sowie die Planung und Einführung effizienter und sicherer Informationssysteme sind unsere Stärke.

Neben der Entwicklung von Individualkonzepten für sichere e-Business Lösungen, beraten und schulen wir unsere Kunden zu den Themen Security Prozesse, (Single) Sign On Lösungen, sicherer organisationsübergreifender Datenaustausch, Secure Messaging, elektronische Signaturen, bei der Sicherung der Infrastruktur und der Integration von mobilen Systemen.

Weiterhin sind wir sehr aktiv auf dem Gebiet der Forschung und Entwicklung und sind somit auch bei nationalen und internationalen Gremien (z.B. TeleTrust e.V. und The Open Group) und diversen Sicherheitskonferenzen präsent.

Teleca Systems GmbH

Mit mehr als 3000 Mitarbeitern in 15 Ländern ist Teleca eine internationale Unternehmensgruppe, die neueste Technologien in den Marktsegmenten Mobile Communication, Mobile Devices, Automotive und Life Science entwickelt und anwendet. Teleca Systems GmbH in Nürnberg ist die erste deutsche Niederlassung der Teleca Gruppe. Das Angebot unseres Unternehmens reicht von der Technologie-Beratung bis zur Durchführung von vollständigen Entwicklungsprojekten für Hochtechnologie-Anwender. Unsere derzeitigen Aufgabenschwerpunkte liegen in den Bereichen Mobilkommunikation, automatische Spracherkennung und Sicherheitsanwendungen.

Utimaco Safeware AG

Utimaco Safeware AG ist der führende Hersteller von professionellen Lösungen für die IT-Sicherheit. Die von Utimaco entwickelten Sicherheitstechnologien und -lösungen schützen die elektronischen Werte von Unternehmen und Behörden vor unberechtigtem Zugriff und gewährleisten die Verbindlichkeit und Vertraulichkeit von Geschäftsprozessen und Verwaltungsabläufen in der elektronischen Welt.

Der Geschäftsbereich Personal Device Security liefert Technologien und Lösungen zur Gewährleistung von mobiler Sicherheit in den Bereichen starke Authentisierung inkl. biometrischer Verfahren, Verschlüsselung und Integritätskontrolle. Die Produkte und Lösungen sichern Daten in Terminal Server- und Citrix-Umgebungen, auf PCs, Laptops und PDAs am



Arbeitsplatz und beim mobilen Einsatz.

Der Geschäftsbereich Transaction Security der Utimaco ist spezialisiert auf Sicherheitslösungen für E-Business-, E-Government- und E-Payment auf Basis eigener Technologien (Telekommunikations-Managementsysteme, Hardware-Sicherheitsmodule, Gateways für E-Mail-Sicherheit, Authentisierung und digitale Signaturen, Public Key Infrastructure und PKI-basierte Anwendungen).