

Anwendungslücke schließen

Herausforderungen der mobilen Geschäftskommunikation

Franz Büllingen

Mit dem Ausbau der Mobilfunknetze und der Verbreitung von WLAN-Hotspots für die mobile Datenübertragung sind längst die infrastrukturellen Voraussetzungen für eine breite Marktdurchdringung mobiler Lösungen in die Geschäftsprozesse von Unternehmen und Verwaltungsorganisationen geschaffen. Mit beinahe 130 Mio. aktiven SIM-Karten im Mobilfunk wurde in Deutschland in weniger als zwei Jahrzehnten eine der bedeutendsten Erfolgsgeschichten der Marktpenetration moderner Kommunikationstechnologien geschrieben. Umso erstaunlicher mutet es an, dass ein ähnlicher Erfolg mobiler Kommunikationslösungen in Unternehmen und Verwaltungsorganisationen bislang noch weitgehend aussteht.

Zwar ruhen auf Mobile Business Solutions (MBS), die auf die Steigerung der Effizienz und Produktivität von Organisationen zielen, schon seit einigen Jahren hohe Erwartungen von Endgeräteherstellern, Softwareanbietern, Netzbetreibern sowie Systemintegratoren. Nach heutigem Stand aber wird der Bedarf nach MBS überwiegend noch durch vergleichsweise einfache Massenmarktanwendungen wie Sprachtelefonie, SMS und E-Mail befriedigt. Dabei kommt nach allgemeiner Auffassung von Experten den Innovationen durch MBS eine Art Schlüsselfunktion zu, mit deren Hilfe sich auf allen Ebenen betrieblicher und öffentlicher Wertschöpfungsaktivitäten Prozesse vereinfachen, flexibilisieren und effizienter gestalten lassen.

Hohes Potenzial von Mobile Business Solutions

So lassen sich von unterwegs aus nicht nur Termine koordinieren, E-Mails versenden oder Tickets bestellen, sondern beispielsweise durch den ubiquitären und jederzeitigen Zugriff auf Plandaten (Mobile Enterprise Resource Planning – ERP) die Qualität unternehmerischer Entscheidungen deutlich erhöhen. Durch Mobile Sales Force Automation sowie Mobile Customer Relationship Management wiederum können sowohl die Vermarktung von Produkten und die Kundenbeziehungen nachhaltig verbessert als auch die Flexibilität und der Einsatz der Beschäftigten im Außendienst deutlich erhöht werden (*Bild 1*).

Es bestehen somit berechnete Erwartungen, dass sich durch mobile Geschäftsanwendungen über alle Branchen hinweg sowohl erhebliche Kosten- und Zeitersparnisse als auch beachtliche Produktivitäts- und Qualitätsgewinne bei der Reorganisation der Wertschöpfungsprozesse realisieren lassen.

Durch Optimierung des Personaleinsatzes, Einsparungen in der Logistik und Verbesserung der Datenqualität beim Kunden wird nicht nur die Wettbewerbsfähigkeit von Unternehmen, sondern auch die Effizienz vieler Verwaltungsorganisationen nachhaltig gesteigert. Der Beitrag von Mobile Business Solutions zur Produktivitäts- und Effizienzsteigerung der gesamten Volkswirtschaft kann somit kaum überschätzt werden.

Im Folgenden werden unter Mobile Business Solutions alle Arten von Prozessen, Aktivitäten sowie Applikationen verstanden, die unter Nutzung drahtloser Übertragungstechniken sowie mobiler Endgeräte zur Optimierung von geschäftlichen Vorgängen eingesetzt werden. Hierunter fallen sowohl geschäftliche Transaktionen (M-Commerce, M-Payment) wie auch die Außendienststeuerung, Logistik, Mobile Office, Mobile CRM, Kontroll-, Fernsteuerungs- und Alarmierungssysteme, Mobile Travel Services, Maschine-zu-Maschine-Applikationen sowie die Steuerung des Personaleinsatzes (Job Dispatch).

Herausforderungen bei MBS

Neben dem mikroökonomischen Mehrwert für Unternehmen und Verwaltungen und dem makroökonomischen Mehrwert für die Volkswirtschaft birgt der Markt für MBS allerdings auch eine ganze Reihe von Hemmnissen und zentralen Problemstellungen. Hierbei geht es nicht nur um die aufwendige Rekonfiguration bestehender Wertschöpfungsprozesse, die eine Innovationsstrategie und ein aktives Change Management bei der Mobilisierung von Prozessen verlangen. Es geht auch um die Entwicklung von neuen und tragfähigen Geschäftsmodellen und nicht zuletzt um die Akzeptanz mobiler Lösungen bei den Belegschaften.

Dr. Franz Büllingen ist Abteilungsleiter Kommunikation und Innovation bei der WIK – Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste GmbH in Bad Honnef

Herausforderungen ergeben sich aber vor allem im Bereich der IT-Sicherheit und des Datenschutzes. Die Mobilisierung von Unternehmensanwendungen betrifft primär zunächst Aspekte, wie sie auch äquivalent im Kontext von klassischen Festnetzen anwendbar sind. Im mobilen Kontext sind diese aber wegen der umfangreicheren Schnittstellen der mobilen Endgeräte, des Technologiemix und der damit verbundenen größeren Angriffsfläche der mobilen Endgeräte bedeutend stärker präsent.

Durch die Mobilisierung der Geschäftsanwendungen verlagert sich der Datenverkehr – auch auf der letzten Meile – auf die Mobilfunknetze. Eine adäquate und hinreichende Absicherung der Luftschnittstelle kann nicht bei allen drahtlosen Kommunikationsnetzen als gegeben vorausgesetzt werden. Maßnahmen zur abgesicherten Kommunikation über alle Zwischenknoten und -netze hinweg sind daher notwendig, um die übertragenen Daten unabhängig von den IT-sicherheitstechnischen Eigenschaften des Übertragungsnetzes abzusichern. Die sichere und robuste Integration mobiler Lösungen über potenziell unsichere Netze hinweg in bestehende IT-Backend-Architekturen liegt daher im Fokus bei der Implementierung von MBS.

Der zweite Fokus resultiert aus der Benutzung mobiler Endgeräte, durch deren flächendeckenden Einsatz eine weitere Herausforderung von MBS entsteht. Ohne besondere Schutzmaßnahmen sind dabei Angriffe im mobilen Kontext schneller und einfacher erfolgreich als im Festnetzbereich. Dies ist bedingt durch die Schwächen diverser integrierter Techniken, die anonym zu attackierenden (Luft-)Schnittstellen, die häufig anzutreffende Vermischung von (ungeschützter) privater und geschäftlicher Nutzung der mobilen Geräte und die fehlende Sensibilisierung der Mitarbeiter für Gefahren bei der Nutzung in öffentlichen Netzen.

Die Entwicklung und Integration von IT-Sicherheitslösungen in mobile Geschäftsanwendungen ist ein kritischer Erfolgsfaktor. Nur wenn die Sicherheit aller relevanten Informationen, Daten,

Prozesse usw., die zur Durchführung der unternehmerischen und prozesskritischen Tätigkeiten erforderlich sind, gewährleistet ist, wird MBS der erhoffte flächendeckende Erfolg beschieden sein. Die Entwicklung und Integration von IT-Sicherheit wird somit zum Key-Enabler von MBS. Dies ist umso wichtiger vor dem Hintergrund, dass im Zuge der Globalisierung der Wettbewerbsspyonage auch

Schnittmengen auf. Im Mittelpunkt der Betrachtung der Schutzziele stehen die Vertraulichkeit, Integrität und Verfügbarkeit als Mindestanforderungen beim Einsatz von mobilen Endgeräten im Unternehmensumfeld. Dabei ist Vertraulichkeit gewährleistet, wenn es keine unautorisierte Informationsgewinnung aus der Dienstenutzung gibt. Die Integrität/Datenintegrität ist gewährleistet, wenn es den

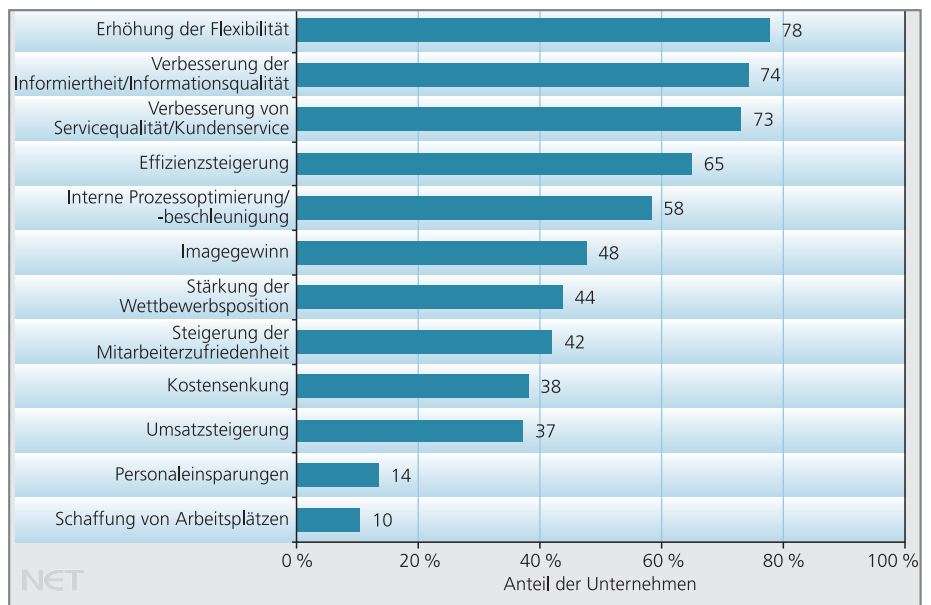


Bild 1: Die Darstellung zeigt eindrucksvoll die Vorteile, die sich aus dem Mobile Business ergeben können; n = 861, Mehrfachnennungen möglich (Quelle: BMWI)

durch ausländische Dienste eine immer größere Bedeutung zukommt und Know-how und wissensintensive Branchen besonders im Fokus ausländischer Interessenten stehen.

Lösungen im Bereich IT-Sicherheit und Datenschutz

Das Bundesministerium für Wirtschaft und Technologie (BMWi) fördert mit dem Programm SimoBIT zwölf ausgewählte Forschungs- und Entwicklungsprojekte zur beschleunigten Entwicklung und breitenwirksamen Nutzung von sicheren, mobil vernetzten Multimediaanwendungen in den Tätigkeitsfeldern von Unternehmen und öffentlichen Verwaltungen (siehe *Textkasten* auf Seite 42). Obwohl die Förderprojekte mit ihren Lösungen sehr heterogene Anwendungsfelder adressieren, weisen ihre Fragestellungen zur IT-Sicherheit und zum Datenschutz zum Teil große gemeinsame

handelnden Nutzern nicht möglich ist, die zu schützenden Dienste oder Daten unbemerkt zu manipulieren. Und schließlich ist die Verfügbarkeit gewährleistet, wenn berechtigte (authentifizierte und autorisierte) Nutzer in der Wahrnehmung ihrer Berechtigungen nicht unautorisiert beeinträchtigt werden können.

Bei der Festlegung von Schutzziele, der Durchführung von Risikoanalysen bzw. der Entwicklung einschlägiger Bedrohungsszenarien wird unter der Annahme bestimmter Use Cases die Feststellung des Schutzbedarfs vorgenommen. Auf dieser Basis werden in jedem Projekt entsprechende Schutzmaßnahmen zur Risikoverminderung abgeleitet. Zu den in allen Projekten behandelten Fragestellungen zählen hierbei die Authentifizierung und Datensicherheit auf mobilen Endgeräten, die Verschlüsselung der Luftschnittstelle, die Entwicklung und Implementierung von Berechtigungs-

und Rollenkonzepten sowie Fragen zum Haftungsrecht.

Datensicherheit auf mobilen Endgeräten

Im Gegensatz zu PCs oder Servern, die sich in der Regel in verschlossenen und nicht selten auch überwachten Räumen befinden, führt der Nutzer mobile Clients auch unterwegs bei sich; sie sind daher generell einem weitaus größeren Risiko des Verlustes oder des Diebstahls ausgesetzt. Verschafft sich ein Angreifer physischen Zugriff auf das mobile Endgerät, so ist gegenwärtig kein vollständiger Schutz der darauf gespeicherten Daten durch technische Maßnahmen möglich. Dennoch kann der Aufwand durch technische Maßnahmen für Angreifer so weit erhöht werden, dass ein erfolgreicher Angriff unwirtschaftlich wird oder weniger erfahrene Angreifer aufgehalten werden. Es ist daher zwingend erforderlich, dass der Zu-

gang zu einem Endgerät durch leicht zu bedienende Authentifizierungsroutinen geschützt und alle Inhalte verschlüsselt werden.

Dazu wird zunächst eine Verschlüsselung zumindest des persistenten Gerätespeichers benötigt, wodurch ein direkter Zugriff auf gespeicherte Daten, an den Schutzmaßnahmen des Gerätes vorbei, verhindert wird. Erstreckt sich die Verschlüsselung auch auf das Betriebssystem des mobilen Endgerätes, wird auch die direkte Manipulation von Schutzfunktionen weiter erschwert.

Durch Maßnahmen zur gegenseitigen Authentifizierung von Benutzer und Endgerät erhält sowohl das Endgerät die Möglichkeit, eine unberechtigte Nutzung zu erschweren, als auch der Nutzer die Möglichkeit, die Echtheit seines Endgerätes zu überprüfen (etwa für den Fall, dass es gegen ein manipuliertes Gerät ausgetauscht wurde, mit dem das Passwort des Nutzers ausgespäht werden soll).

Jedoch erst durch einen Hardware-sicherheitsanker können diese Maßnahmen so weit in das Endgerät integriert werden, dass sie auch für fortgeschrittene Angreifer eine angemessene Hürde darstellen.

Als besonders wichtig erweist sich, dass eine erhöhte Sicherheit nicht die Nutzerfreundlichkeit beeinträchtigen darf, da sonst zu große Anreize bestehen, Sicherheitsmechanismen außer Kraft zu setzen.

Bei der Verwendung der Begrifflichkeit „mobiles Endgerät“ wird übrigens allzu oft vergessen, dass hierzu nicht nur Geräte mit Kommunikationsfunktion wie PDAs oder WLAN-Notebooks zählen, sondern auch externe Festplatten, USB-Token, SD-Karten oder andere Datenträger (*Bild 2*). Vor diesem Hintergrund kommen alle Unternehmen oder Organisationen, die MBS einsetzen wollen, nicht umhin, ein ganzheitliches Mobile Device Management und eine entsprechende Sicherheitspolicy zu implementieren.

Förderinitiative SimoBIT für sichere mobile Informationstechnik

Angesichts der enormen volkswirtschaftlichen und einzelwirtschaftlichen Bedeutung von Mobile Business Solutions und der Tatsache, dass sich die Entwicklung sowie der Einsatz mobiler Geschäftsanwendungen sowie die dazugehörigen IT-Sicherheitslösungen insgesamt noch in einer vorwettbewerblichen Phase befinden, hat das Bundesministerium für Wirtschaft und Technologie (BMWi) 2006 einen Technologiewettbewerb veranstaltet; die Motivation: Sichere Anwendungen der mobilen Informationstechnik zur Wertschöpfungssteigerung in Mittelstand und Verwaltung (SimoBIT) voranzutreiben. Mit einem Förderprogramm von rund 28 Mio. € – die geförderten Projektverbände wenden noch einmal die gleiche Summe auf – wird eine wichtige Grundlage für den breitenwirksamen Transfer des in diesen Projekten generierten Wissens geschaffen.

Das Ziel von SimoBIT besteht darin, durch eine nahtlose Integration von IT-Sicherheit mit mobilen Technologien und Anwendungen die Implementie-

rung von Mobile Business Solutions in bestehende betriebliche und verwaltungsorganisatorische Strukturen zu erleichtern und zu beschleunigen. Die zwölf Projektverbände sind fachlich in vier Kompetenz-Cluster gebündelt:

- Gesundheitswirtschaft (Med-on@ix, VitaBIT, OPAL Health);
- Maschinenbau (SiWear, R2B – Robot to Business, MSW – Mobile Servicewelten);
- Handwerk und kleine Unternehmen (Maremba, ModiFrame, M3V – Mobile Multimediale Multilieferanten-Vertriebsinformationssysteme);
- öffentliche Verwaltung (Mobility@forest, Mobis Pro, simoKIM).

In diesen Projekten werden beispielhaft IT-Sicherheitslösungen erarbeitet und demonstriert, was technisch machbar und erforderlich sowie wirtschaftlich an innovativen Diensten sinnvoll ist. Insgesamt sollen die zwölf Projekte andere Unternehmen und Verwaltungsorganisationen zur Nachahmung anregen.

Um zu sichern, dass die Förderung effizient umgesetzt und ein breiter

Transfer der Ergebnisse in den Markt gewährleistet wird, hat das BMWI 2008 eine wissenschaftliche Begleitforschung eingerichtet. Hierfür wurde speziell zur Evaluation und wissenschaftlichen Begleitung der IT-Sicherheitslösungen neben WIK-Consult Fraunhofer SIT in das Konsortium aufgenommen.

Das Projekt hat eine Laufzeit bis 2011. Durch die Einrichtung von Arbeitsforen werden seit Herbst 2008 Lösungen für Querschnittsfragen erarbeitet. Zum Beispiel bezüglich

- der erfolgreichen Gestaltung von Geschäftsmodellen;
- der Akzeptanzförderung und der Schulung von Mitarbeitern;
- der Prüfung der Kompatibilität mit bestehenden Rechtsnormen;
- der IT-Sicherheit.

Die Arbeitsforen stehen allen interessierten Experten offen. Die Ergebnisse der Arbeit münden in Leitfäden, die gegen Ende der SimoBIT-Laufzeit veröffentlicht werden.

(Informationen und Kontaktmöglichkeiten über www.simobit.de)

Verschlüsselung der Luftschnittstelle

Aufgrund der beim Mobilfunk für die Informationsübertragung genutzten Funkstrecke können Signale anders als im Festnetz nicht physikalisch gegen Mithören und Aufzeichnen abgeschirmt werden. Außerdem werden bei jedem Anmeldevorgang Standortdaten übertragen, die das Erstellen von Bewegungsprofilen ermöglichen und somit zahlreiche Begehrlichkeiten – etwa von Behörden, Privatpersonen, Werbeunternehmen, Location-Based-Service-Anbietern usw. – wecken.

Bezogen auf den Schutz gegen Angriffe auf der Luftschnittstelle können technische Maßnahmen indes umfassend wirken, wenn sie korrekt umgesetzt werden. Eine wesentliche Maßnahme ist eine durch kryptographische Methoden abgesicherte Kommunikation über alle Zwischenknoten hinweg (Ende-zu-Ende-Sicherheit). Je nach eingesetzter Kryptographiestärke wird das Abhören vertraulicher Informationen durch Angreifer dadurch erheblich aufwendiger bzw. bei Berücksichtigung aktueller Methoden für herkömmliche Angreifer vollständig verhindert.

Ein wirksamer Schutz kann daher nur durch eine interoperable, netzübergreifende Ende-zu-Ende-Verschlüsselung hergestellt werden, die bei allen entsprechenden Lösungen zu berücksichtigen ist. Daher sollte bei der Anbindung von Unternehmensdiensten auf unverschlüsselte Kommunikation ganz verzichtet werden und stattdessen durch anerkannte Techniken wie SSL/TLS der Schutz der Online-Inhalte und durch S/MIME oder PGP der Schutz von E-Mails erfolgen. Ist ein vollständiger Zugriff auf das Unternehmensnetz unumgänglich, muss auf die Nutzung von Tunnellösungen (zum Beispiel VPN, SSH) zurückgegriffen werden. Zur Reduzierung des Risikopotenzials sollte dabei jedoch nur ein abgeschotteter, notwendiger Teil des Netzes erreichbar sein.

Da alle Kommunikationsschnittstellen potenzielle Angriffsziele darstellen, besteht eine weitere Maßnahme in der selektiven Aktivierung von Kommunikationsschnittstellen, die nur bei

Bedarf erfolgen und sonst abgeschaltet bleiben sollte (beispielsweise Bluetooth, WLAN).

Berechtigungs- und Rollenkonzepte

Die Realisierung von MBS in einem Unternehmen basiert i.d.R. auf einer technischen Lösung, bei der alle für Geschäftsprozesse relevanten Daten auf einem zentralen Server abgelegt werden. Bei Datenbeständen, die von einem externen Dienstleister gehostet werden, können die Daten unterschiedlicher Eigentümer, je nach Hostingkonzept, auf einem Server sogar



Bild 2: Wenn es um die Datensicherheit mobiler Endgeräte geht, sind auch Komponenten wie USB-Sticks oder mobile Festplatten zu berücksichtigen (Foto: Vodafone)

„nebeneinander“ liegen. Dies bedeutet, dass bei Zugriff verschiedener Nutzer oder Nutzergruppen vorab definiert werden muss, wem der Zugriff auf bestimmte Datenbestände (ganz oder selektiv, nur lesen oder auch schreiben) gestattet wird. Eine solche Festlegung von Zugriffsberechtigungen kann nur in Form eines ausgefeilten Rollenkonzeptes erfolgen. Nur wenn klar definiert, festgelegt und technisch implementiert ist, wer welche Daten lesen, verändern oder löschen darf, sind Vertraulichkeit, Integrität und Authentizität der Daten gesichert.

Jedes Berechtigungs- und Rollenkonzept basiert darauf, dass an zentraler Stelle im Backend ein System für Identity Management eingerichtet wird, mit dessen Hilfe die Identitäten der Nutzer eingerichtet, administriert oder auch gelöscht werden. In jedem Einzelfall sind die Berechtigungen für den Zugriff auch zeitlich und sachlich festzulegen. Dies gilt insbesondere

auch für die Zusammenarbeit verschiedener Personen mit Zugriffsberechtigung untereinander (Orchestrierung). Es zeigt sich hieran, dass die Implementierung von MBS in betriebliche und organisatorische Strukturen ein komplexer Prozess ist, der ohne einen externen Dienstleister kaum umgesetzt werden kann.

IT-Sicherheit, Akzeptanz und Awareness

Umfragen unter geschäftlichen Nutzern zeigen immer wieder, dass auf mobilen Endgeräten vorhandene Sicherheitsfeatures abgeschaltet werden, da sie die Nutzerfreundlichkeit teilweise erheblich beeinträchtigen können. Befürchtungen vor dem Vergessen von Passwörtern, die Bequemlichkeit oder auch die mangelnde Awareness für die Bedeutung und den Wert von Daten führen dazu, dass der IT-Sicherheit und dem Schutz von Daten oft eine zu geringe Aufmerksamkeit zuteil wird. Bei der Implementierung von MBS kommt es demnach nicht nur auf die Einführung einer IT-Sicherheitspolicy an, sondern auch auf eine hinreichende Sensibilisierung und Schulung des im Außendienst befindlichen Personals.

Haftungsrechtliche Fragen

Diensteanbieter im Mobile Business stehen häufig vor der Aufgabe, Kosten von IT-Sicherheitsmaßnahmen gegenüber möglichen Haftungsforderungen abzuwägen. Im Vorfeld der Entwicklung von geschäftlichen MBS-Angeboten geht es daher auch um Fragen der Haftung bei Datenverlust, die Haftung eines Plattformbetreibers gegenüber einem Diensteanbieter sowie Rechtsansprüche von Endnutzern. Auf Basis mobiler Vernetzung entstehen durch „Verschneiden“ vielfach neue Informationen, die dann wiederum andere Abgrenzungen von Verantwortlichkeiten und Nutzungsrechten erfordern. Die veränderten rechtlichen Transparenzerfordernisse schaffen auch die Notwendigkeit neuer Rechte- und Rollenzuweisungen, die nicht allein technisch konzipiert werden können. (we)