Franz Büllingen, Annette Hillebrand, Martin Oczko, Matthias Ritscher

IT-Sicherheit als kritischer Erfolgsfaktor mobiler Geschäftsanwendungen

Zielsetzungen der BMWI-Förderinitiative SimoBIT

Die Entwicklung und Integration von IT-Sicherheitslösungen in mobile Geschäftsanwendungen ist ein kritischer Erfolgsfaktor für die flächendeckende Verbreitung innovativer Lösungen. Wichtige Herausforderungen bestehen nicht nur bei der Entwicklung geeigneter Sicherheitsarchitekturen und ihrer korrekten Implementierung, sondern auch bei der Integration neuer mobiler Dienste und Anwendungen in bestehende betriebliche und administrative Prozesse, der Beantwortung rechtlicher Fragen sowie der Schulung und der Akzeptanz der Anwender.

Dr. Franz Büllingen

Abteilungsleiter Kommunikation und Innovation, Leiter der SimoBIT-Begleitforschung, WIK-Consult, Bad Honnef
E-Mail: f.buellingen@wik-consult.com

Annette Hillebrand

Senior Consultant SimoBIT-Begleitforschung, Arbeitsforum IT-Sicherheit, WIK-Consult, Bad Honnef
E-Mail: A.hillebrand@wik-consult.com

Martin Oczko

System Engineer HSM
Leiter SimoBIT-Arbeitsforum IT-Sicherheit, Utimaco Safeware AG – A member of the Sophos Group
E-Mail: Martin.Oczko@aachen.utimaco.de

Einleitung

Mit beinahe 130 Mio. aktiven SIM-Cards 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 solchen, auf die Steigerung der Effizienz und Produktivität von Organisationen zielenden Mobile Business-Solutions (MBS)[1] seit einigen Jahren bereits die hohen Erwartungen von Endgeräte-Herstellern, 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.

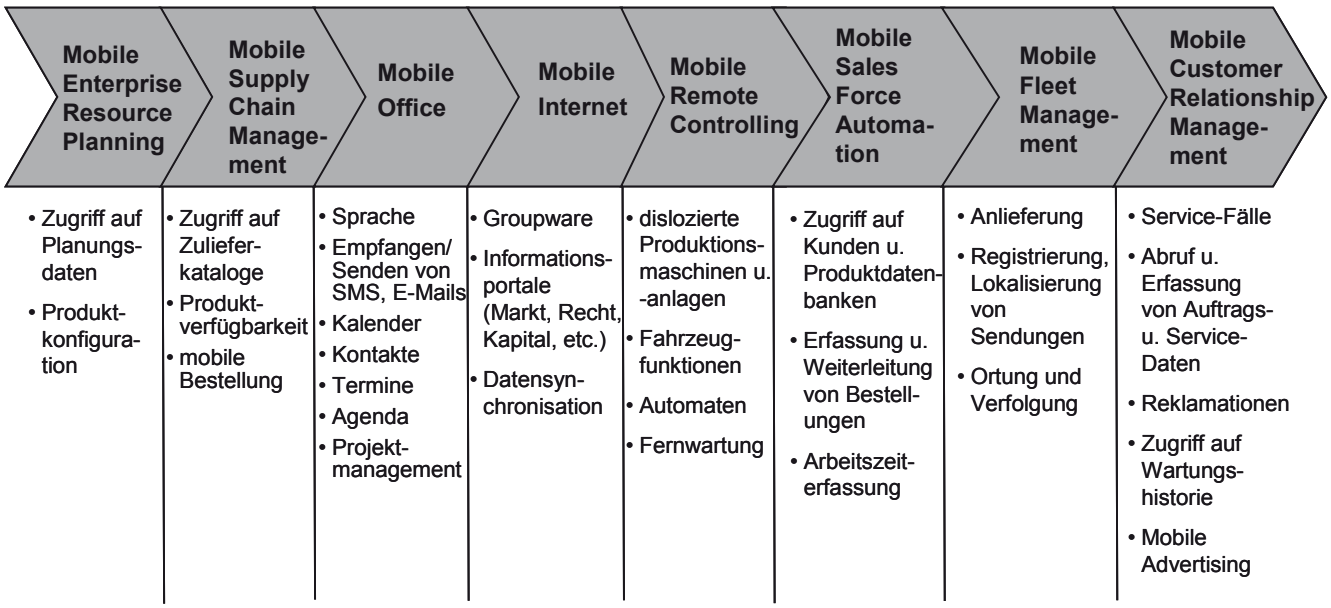
Dabei wurden angebotsseitig mit dem in den letzten Jahren erfolgten Ausbau der GSM/EDGE- und UMTS/HSPA-Netze sowie der Verbreitung Tausender WLAN-Hotspots längst die infrastrukturellen Voraussetzungen für eine breite Marktdurchdringung mobiler Lösungen in die Geschäftsprozesse von Unternehmen und Verwaltungsorganisationen geschaffen. Im Rahmen eines intensivierten Dienstewettbewerbs der Mobilfunkanbieter können geschäftliche Anwender bei sinkenden Kosten und kostenkontrollierenden Preismodellen (Flatrates) zudem auf immer größere Bandbreiten und leistungsfähigere Endgeräte (Smart Phones, Blackberries, Subnotes) zurückgreifen, die sich sowohl für private als auch geschäftliche Anwendungen nutzen lassen.

1 Im Folgenden werden unter Mobile Business-Solutions jede Art von Prozessen, Aktivitäten sowie Applikationen verstanden werden, die unter Nutzung drahtloser Übertragungstechnologien 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).

Matthias Ritscher

Fraunhofer-Institut für Sichere Informationstechnologie (SIT) Forschungsbereich "Sichere mobile Systeme", SimoBIT-Begleitforschung/Evaluationspartner IT-Sicherheit
E-Mail: matthias.ritscher@sit.fraunhofer.de

Abbildung 1 | Prozessinnovationen durch Mobile Business… auf allen Stufen der Wertschöpfung



1 Volkswirtschaftliche Bedeutung von Mobile Business-Solutions

Nach allgemeiner Auffassung von Experten kommen 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. 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) die Qualität unternehmerischer Entscheidungen deutlich erhöhen. Durch Mobile Sales Force Automation sowie Mobile Customer Relationship Management können sowohl die Vermarktung von Produkten und die Kundenbeziehung nachhaltig verbessert als auch die Flexibilität und der Einsatz der Beschäftigten im Außendienst deutlich erhöht werden [1].

Es bestehen somit berechtigte 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 die Optimierung des Personaleinsatzes, Einsparungen in der Logistik und die Verbesserung der Datenqualität beim Kunden vor Ort 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 [2].

2 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 nicht nur um die aufwändige Rekonfiguration bestehender Wertschöpfungsprozesse, die eine durchdachte 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.

Herausforderungen ergeben sich aber vor allem im Bereich der IT-Sicherheit und des Datenschutzes. Die Mobilisierung von Unternehmensanwendungen betreffen 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, dem Technologie-Mix und der damit verbundenen größeren Angriffsfläche der mobilen Endgeräte bedeutend stärker präsent. Durch die Mobilisierung der Geschäftsanwendungen verlagert sich der Datenverkehr (auf der letzten Meile) zunehmend 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 potentiell unsichere Netze hinweg in bestehende IT-Backend-Architekturen bildet daher einen zentralen Fokus bei der Implementierung von MBS.

Der zweite Fokus resultiert aus dem Einsatz mobiler Endgeräte, durch den eine weitere Herausforderung bei 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 Technologien, den anonym zu attackierenden (Luft-)Schnittstellen, der häufig anzutreffenden Vermischung von (ungeschützter) privater und geschäftlicher Nutzung der mobilen Geräte und der fehlenden Sensibilisierung der Mitarbeiter für Gefahren bei der Nutzung in öffentlichen Netzen.

Die Entwicklung und Integration von IT-Sicherheitslösungen in mobile Geschäftsanwendungen ist somit ein kritischer Erfolgsfaktor. Nur wenn die Sicherheit aller relevanten Informationen, Daten, Prozesse etc., die zur Durchführung der unternehmerischen und prozesskritischen Tätigkeiten erforderlich sind, gegeben 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 Rahmen der Globalisierung Wettbewerbsspionage durch ausländische Dienste eine immer größere Gefahr darstellt und Know-how- und wissensintensive Branchen besonders im Fokus ausländischer Interessenten stehen [3].

3 Die Förderinitiative SimoBIT

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 dazu gehörigen IT-Sicherheitslösungen insgesamt noch in einer vorwettbewerblichen Phase befinden, hat das Bundesministerium für Wirtschaft und Technologie (BMWI) 2006 die Förderinitiative SimoBIT ins Leben gerufen. SimoBIT steht für „Sichere Anwendungen der mobilen Informationstechnik zur Wertschöpfungssteigerung in Mittelstand und Verwaltung“.[2] Mit einem Förderprogramm von rund 28 Mio. Euro – die geförderten Projektverbünde wenden noch einmal die gleiche Summe auf – wird eine wichtige Grundlage für den breitenwirksamen Transfer des in diesen Projekten generierten Wissens geschaffen.

Die Zielsetzung von SimoBIT besteht darin, durch eine nahtlose Integration von IT-Sicherheit mit mobilen Technologien und Anwendungen die Implementierung von MBS in bestehende betriebliche und verwaltungsorganisatorische Strukturen zu erleichtern und zu beschleunigen. Die zwölf Projektverbünde sind in vier Kompetenzcluster gebündelt [4]:

1. Gesundheitswirtschaft (Med-on-@ix, VitaBIT, OPAL Health),
2. Maschinenbau (SiWear, R2B – Robot to Business, MSW – Mobile Servicewelten),
3. Handwerk und kleine Unternehmen (MAREMBA, ModiFrame, M3V – Mobile Multimediale Multiliferanten-Vertriebsinformationsysteme),
4. öffentliche Verwaltung (Mobility@forest, Mobis Pro, simoKIM).

Im Rahmen dieser Projekte werden beispielhaft IT-Sicherheitslösungen erarbeitet und demonstriert, was technisch machbar und erforderlich sowie wirtschaftlich an innovativen Diensten sinnvoll ist. Insgesamt sollen die 12 Projekte andere Unternehmen und Verwaltungsorganisationen zur Nachahmung anregen. Damit die effiziente Umsetzung der Förderung gesichert und ein breiter Transfer der Ergebnisse in den Markt gewährleistet wird, hat das BMWi 2008 zum Förderschwerpunkt SimoBIT aus Gründen der Qualitätssicherung und zum Transfer der Ergebnisse eine wissenschaftliche Begleitforschung[3] eingerichtet. Das Projekt hat eine Laufzeit bis 2011. Durch die Einrichtung von Arbeitsforen werden seit Herbst 2008 Lösungen für Querschnittfragen z. B. bezüglich

- der erfolgreichen Gestaltung von Geschäftsmodellen,
- der Akzeptanzförderung und der Schulung von Mitarbeitern,
- der Prüfung der Kompatibilität mit bestehenden Rechtsnormen,
- und nicht zuletzt der IT-Sicherheit

erarbeitet. Die Arbeitsforen stehen allen interessierten Experten offen. Die Ergebnisse dieser Arbeit münden in die Erstellung von Leitfäden, die gegen Ende der SimoBIT-Laufzeit veröffentlicht werden.[4]

4 Herausforderungen im Bereich IT-Sicherheit und Datenschutz

Obwohl die 12 Förderprojekte mit ihren Lösungen sehr heterogene Anwendungsfelder adressieren, weisen ihre Fragestellungen zur IT-Sicherheit und zum Datenschutz z. T. große gemeinsame Schnittmengen auf. Im Mittelpunkt der Betrachtung der Schutzziele stehen die Vertraulichkeit, Integrität und Verfügbarkeit als Mindestanforderungen beim Einsatz von mobilen Endgeräten im Unternehmensumfeld oder bei Verwaltungen.

- Dabei ist Vertraulichkeit gewährleistet, wenn es keine unautorisierte Informationsgewinnung aus der Dienstenutzung gibt.
- Die Integrität/Datenintegrität ist gewährleistet, wenn es den handelnden Nutzern nicht möglich ist, die zu schützenden Dienste oder Daten unbemerkt zu manipulieren.
- Die Verfügbarkeit ist gewährleistet, wenn berechtigte (authentifizierte und autorisierte) Nutzer in der Wahrnehmung ihrer Berechtigungen nicht unautorisiert beeinträchtigt werden können.

Im Rahmen der Festlegung von Schutzzielen, der Durchführung von Risikoanalysen bzw. der Entwicklung einschlägiger Bedrohungsszenarien wird unter der Annahme bestimmter Use Cases die Feststellung des Schutzbedarfes vorgenommen. Auf dieser Basis werden in jedem Projekt entsprechende Schutzmaßnahmen zur Risikoverminderung abgeleitet. Zu den in allen Projekten behandelten Fragestellungen zählen hierbei die Authentisierung und Datensicherheit auf mobilen Endgeräten, die Verschlüsselung der Luftschnittstelle, die Entwicklung und Implementierung von Berechtigungs- und Rollenkonzepten sowie die Klärung der Fragen zum Haftungsrecht.

4.1 IT-Sicherheit im Kontext von Geschäfts- und Fachprozessen

Im Hintergrund vieler mobiler Anwendungen stehen Geschäfts- oder Fachprozesse, die in den Applikationen abgebildet werden. Es ist wesentlich, dass Sicherheitsmechanismen nicht nur Bestandteil der entsprechenden Applikationen sind, sondern in die Prozesse an sich integriert werden. Dieses Vorgehen bringt mehrere Vorteile mit sich.

Zum einen verbessert sich durch Integration von technischen, zum Beispiel kryptographischen Sicherheitsmechanismen in die Prozesse die Auditierbarkeit der gesamten Anwendung. Durch Anwendung moderner Prozessbeschreibungs- und Ausführungssprachen wie BPMN

2 Weitergehende Informationen zur Förderinitiative SimoBIT finden sich unter: www.simobit.de.

3 Speziell zur Evaluation und wissenschaftlichen Begleitung der IT-Sicherheitslösungen wurde neben WIK-Consult Fraunhofer SIT in das Konsortium der Begleitforschung aufgenommen.

4 Eine Kontaktaufnahme zum Arbeitsforum IT-Sicherheit kann einfach erfolgen über die SimoBIT-Homepage: www.simobit.de.

oder BPEL lassen sich Prozesse graphisch darstellen und beschreiben, was die Übersichtlichkeit von komplexen Prozessen deutlich verbessert.

Zum anderen lassen sich auf der Prozessebene technische Sicherheitsmechanismen mit organisatorischen einfach kombinieren. Als Beispiel kann hier das Vier-Augen-Prinzip genannt werden, welches einerseits eine organisatorische Sicherheitsmaßnahme darstellt, andererseits aber auch durch kryptographische Mechanismen hinterlegt werden kann.

4.2 Authentisierung und Datensicherheit auf mobilen Endgeräten

Im Gegensatz zu Personal Computern oder Servern, die sich in der Regel in verschlossenen und nicht selten auch überwachten Räumen befinden, werden mobile Clients stets mit herum geführt und 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 soweit erhöht werden, so dass ein erfolgreicher Angriff unwirtschaftlich wird oder weniger erfahrene Angreifer aufgehalten werden.

Es ist daher zwingend erforderlich, dass der Zugang zu einem Endgerät durch leicht zu bedienende Authentisierungsroutinen geschützt und alle Inhalte verschlüsselt werden [5].[5]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 Endgeräts, wird auch die direkte Manipulation von Schutzfunktionen weiter erschwert.

Durch Maßnahmen zur gegenseitigen Authentisierung von Benutzer und Endgerät erhält sowohl das Endgerät die Möglichkeit, eine unberechtigte Nutzung zu erschweren, als auch der Nutzer die Chance, die Echtheit seines Endgeräts zu überprüfen (etwa für den Fall, dass es gegen ein manipuliertes ausgetauscht wurde, mit dem das Passwort des Nutzers ausgespäht werden soll). Jedoch erst durch einen Hardwaresicherheitsanker können diese Maßnahmen so weit in das Endgerät integriert werden, dass sie auch für fortgeschrittene Angreifer eine angemessene Hürde darstellen [6].

Je nach Art der Anwendung hält das mobile Endgerät eine Verbindung zu einer online Applikation. Hier ist es wichtig, dass sich nicht nur der Benutzer und das mobile Endgerät gegenüber der Anwendung authentifizieren sondern auch die Anwendung gegenüber dem Anwender. Nur so kann verhindert werden, dass ein Angreifer die online Applikation simuliert und auf diesem Wege vertrauliche Informationen abgreift, dem Anwender manipulierte Informationen übermittelt oder sogar das Endgerät manipuliert [7, 8].

Bei der Verwendung der Begrifflichkeit „mobiles Endgerät" wird leicht vergessen, dass hierzu nicht nur Geräte mit Kommunikationsfunktion zählen, sondern auch externe Festplatten, USB Token, SDCards oder andere Datenträger. 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. Dies ist besonders wichtig vor dem Hintergrund, dass mobile Endgeräte häufig sporadisch und unsystematisch beschafft werden, nicht zuletzt auch, um mit den schnellen Lebenszyklen Schritt halten zu können [9].

4.3 Verschlüsselung der Luftschnittstelle

Durch die beim Mobilfunk für die Informationsübertragung genutzte 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 (Behörden, Privatpersonen, Werbeunternehmen, Location Based Service-Anbieter) 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 kryptografische Methoden abgesicherte Kommunikation über alle Zwischenknoten hinweg (Ende-zu-Ende-Sicherheit). Je nach eingesetzter Kryptographiestärke wird das Abhören vertraulicher Informationen durch Angreifer dadurch erheblich aufwändiger 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 Technologien wie SSL/TLS der Schutz der Online-Inhalte und S/MIME oder PGP der Schutz von E-Mails erfolgen. Ist ein vollständiger Zugriff auf das Unternehmensnetzwerk unumgänglich, muss auf die Nutzung von Tunnel-Lösungen (VPN, SSH) zurückgegriffen werden. Zur Reduzierung des Risikopotenzials sollte dabei jedoch nur ein abgeschotteter, notwendiger Teil des Netzwerks erreichbar sein.

Da alle Kommunikationsschnittstellen potentielle Angriffsziele darstellen, besteht eine weitere Maßnahme in der selektiven Aktivierung von Kommunikationsschnittstellen, die nur bei Bedarf erfolgen und sonst abgeschaltet bleiben sollten (bspw. Bluetooth, WLAN). Ein Paradigma welches durchgehenden Ende-zu-Ende Schutz der Daten bei der Speicherung und während der Kommunikation bietet, ist der Ansatz der datenzentrischen Sicherheit. Der Gedanke dahinter ist, die Sicherheitsmechanismen nicht an die verwendete Speichereinheit oder das Übertragungsprotokoll zu binden, sondern an das Datenobjekt selbst.

Dies kann zum Beispiel durch Verschlüsseln der Datenobjekte erfolgen, bei dem zusätzliche Information über den verwendeten Schlüssel an das Datenobjekt angehängt werden. Solche Datenobjekte können dann gefahrlos auf beliebigen Datenträgern gespeichert und über unverschlüsselte Medien übertragen werden. Ein Beispiel für die Anwendung dieses Paradigmas ist ERM oder DRM (Enterprise bzw. Digital Rights Management).

5 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.

4.4 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, liegen die Daten unterschiedlicher Eigentümer auf einem Server sogar „nebeneinander". 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 die Vertraulichkeit, Integrität, 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 (ggf. auch örtlich) festzulegen. Dies gilt insbesondere auch für die Zusammenarbeit verschiedener Personen mit Zugriffsberechtigung untereinander (Orchestrierung).

Hieran zeigt sich, dass die Implementierung von MBS in betriebliche und organisatorische Strukturen ein komplexer Prozess ist, der ohne externe Dienstleister kaum umgesetzt werden kann.

4.5 IT-Sicherheit, Akzeptanz und Awareness

Umfragen unter geschäftlichen Nutzer zeigen immer wieder, dass auf mobilen Endgeräten vorhandene Sicherheitsfeatures abgeschaltet werden, da sie die Nutzerfreundlichkeit z. T. erheblich beeinträchtigen können. Befürchtungen, ein Passwort zu vergessen, die Bequemlichkeit oder auch die mangelnde Awareness für die Bedeutung und den Wert von Daten führen dazu, dass IT-Sicherheit 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 insbesondere auch auf eine hinreichende Sensibilisierung und Schulung des im Außendienst befindlichen Personals.

4.6 Haftungsrechtliche Fragen

Diensteanbieter im Mobile Business stehen häufig vor der Aufgabe, Kosten von IT-Sicherheitsmaßnahmen gegenüber möglichen Haftungsforderungen oder Imageverlusten abzuwägen. Im Vorfeld der Entwicklung von geschäftlichen MBS-Angeboten geht es daher auch ganz entscheidend um Fragen der Haftung bei Datenverlusten, 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. Antworten für diese rechtlich oft sehr komplexen Fragestellungen stehen i. d. R. bislang noch aus und müssen von den Akteuren gemeinsam erarbeitet werden.

5 Zusammenfassung

Bei der Sicherheit von MBS gibt es bereits technische und organisatorische Ansätze, die in erheblichem Umfang dazu beitragen können, Vertrauen in den Einsatz mobiler Endgeräte in Geschäftsumfeld und in Verwaltungsprozesse zu schaffen. Dennoch bestehen eine Reihe von Herausforderungen aufgrund fehlender vertrauenswürdiger mobiler Hardware und der Dynamik beim Zusammenwachsen von Netzen.

Zudem bestehen für die Sicherheit weitere Fragestellungen bei der Umsetzung des aktuellen Trends zur Organisation von Diensten in unternehmensfremden „Clouds", wo sie orchestriert und dem Nutzer zur Verfügung gestellt werden. Das Sicherheitsbewusstsein ist sowohl bei den Unternehmen als auch bei den privaten Nutzern in den vergangenen Jahren gestiegen, wodurch die Bereitschaft vorhanden ist, einerseits auf Seiten der Unternehmen in die Sicherheit zu investieren und andererseits bei den privaten Nutzern, etwas für sichere Dienstleistungen zu bezahlen. Sicherheit, Schutz der Privatsphäre und Etablierung neuer Vertrauensmodelle werden daher in den kommenden Jahren, beispielsweise auf Basis der SimoBIT-Projekte, stärker adressiert werden, um Akzeptanz bei den Unternehmen – vor allem bei KMU – zu schaffen, mobile Endgeräte bei der Optimierung ihrer Geschäftsprozesse einzusetzen.

Literatur

[1] Franz Büllingen (2006): *Mobile Enterprise-Solutions – Stand und Perspektiven mobiler Kommunikationslösungen in kleinen und mittleren Unternehmen*, Bad Honnef

[2] Arnold Picot, Martin S. Schmid (2009): *Mobilisierung von Wertschöpfungsprozessen durch innovative und sichere Informationstechnologie*, Institut für Information, Organisation und Management (IOM) der Ludwig-Maximilians-Universität München, Studie im Auftrag des BMWi im Rahmen von SimoBIT

[3] Bundesamt für Sicherheit in der Informationstechnik (2006): *Drahtlose Kommunikationssysteme und ihre Sicherheitsaspekte*, Bonn

[3] Bundesamt für Sicherheit in der Informationstechnik (2006): *Mobile Endgeräte und mobile Applikationen: Sicherheitsgefährdungen und Schutzmaßnahmen*, Bonn

[4] Bundesministerium für Wirtschaft und Technologie (2009): *SimoBIT. Sichere Anwendung der mobilen Informationstechnik (IT) zur Wertschöpfungssteigerung in Mittelstand und Verwaltung*, Berlin

[5] Frank Kölmel (2007): *Mobile User sicher authentifizieren*, in: kes Die Zeitschrift für Informationssicherheit, Sonderausgabe Juli, SecuMedia Verlags-GmbH, Ingelheim

[6] Peter Schill (2007): *Mobile Identitätsprüfung*, in: kes Die Zeitschrift für Informationssicherheit, Sonderausgabe Juli, SecuMedia Verlags-GmbH, Ingelheim

[7] Harald Duelli (2007): *Mobile Endgeräte: Nutzung und Schutz*, in: kes Die Zeitschrift für Informationssicherheit, Sonderausgabe Juli, SecuMedia Verlags-GmbH, Ingelheim

[8] Christian Koch, Oliver v. Feldegg (2007): *Schutz für mobile Clients*, in: kes Die Zeitschrift für Informationssicherheit, Sonderausgabe Juli, SecuMedia Verlags-GmbH, Ingelheim

[9] Daniel Liebisch (2007): *Security durch Zentralisierung*, in: kes Die Zeitschrift für Informationssicherheit, Sonderausgabe Juli, SecuMedia Verlags-GmbH, Ingelheim