

# Gratwanderung: Informations-High/Sicherheits-Low

Mobiles Business beschränkt sich bisher vor allem auf Geschäfts-E-Mail von unterwegs. Die Entwicklung hin zu weit gewinnbringenderen Anwendungen läuft – vor allem auch in der Finanzbranche. Parallel zur Entwicklung wachsen auch die Sicherheitsrisiken. *Hans Fischer*



**Hans Fischer**

ist bei Rolotec AG, Biel, in den Bereichen Business Development, Marketing und Kommunikation mit Fokus auf Knowledge Management, Beratung und Börseninformation tätig.  
fi@rolotec.ch

Die 2-Milliarden-Schwelle sei überschritten, verkündete Wireless Intelligence jüngst den Rekordwert an weltweiten Mobiltelefon-Benutzern. Erstaunlich, denn prognostiziert war die Erreichung dieses Wertes erst auf Ende 2010. Sicher ist: Die Nachfrage ist äusserst nachhaltig. Weit weniger zügig als die mobile Telefonie etabliert sich das Mobile Business. Die Universität Köln kommt zwar zum Schluss, dass die Unternehmen im deutschsprachigen Raum zusätzliche Wertschöpfung durch Mobile Business erwarten würden und auch gewillt seien, diese für sich zu nutzen. Zeitlicher Umsetzungsdruck scheint aber nicht gegeben. Das Fachmagazin CIO schreibt denn auch von einem Hype, der nicht von der Realität gedeckt sei. Und das, weil es an Strategien und Know-how für Mobile Business fehle.

Als einziger Wachstumstreiber hat sich bisher der mobile Zugang zu den Geschäfts-E-Mails erwiesen. Als innovativ kann das aber keinesfalls bezeichnet werden. Noch keine Spur von der viel beschriebenen Ausnutzung der Hauptvorteile Prozessbeschleunigung, Qualitätsverbesserung und Kostenreduzierung. Und von der Vision der Uni Köln, wonach uns die Gerätegenerationen der Zukunft bei alltäglichen Vorgängen und Handlungen unterstützen, ohne bewusst von uns wahrgenommen zu werden, sind wir bei realistischer Betrachtung noch viele Jahre entfernt.

## Innovationstreiber Finanzbranche

Manchmal brauchen Technologiefortschritte etwas länger. Besonders empfänglich zeigt sich aber einmal mehr die Finanzbranche. Während sich viele Branchen – und konsequenterweise vor allem deren Management-Gilden – schwer tun mit dem Entwerfen von Einsatzmöglichkeiten mobiler Lösungen, übernehmen die Finanter eine wichtige Vorreiterrolle. Wie bereits zu Internet-Pionierzeiten treiben sie innovative Lösungen voran

und testen sie im Markt. So haben insbesondere die bedeutenden Finanzinformationsspezialisten ihre bisherigen SMS- und WAP-Dienste für Börsenkurs- und Newsabfragen auf technologisch ansprechendes und modernes Niveau angehoben.

Mit von der Partie ist auch die Schweizer Telekurs Financial mit der von ihrer Bieler Tochterunternehmung Rolotec AG realisierten Desktoplösung «Telekurs iD mobile». Die Architektur von Telekurs iD erlaubt es, das Börsengeschehen ähnlich einer Profilösung am Computer-Bildschirm auf dem Mobilgerät anzuzeigen. Dank ausgeklügelter XML-Technik können etwa die aktuellen Börsenkurse mit den Veränderungswerten laufend angezeigt werden. Das mobile Endgerät wird zum Streaming-Empfänger. Dazu kommen Nachrichten der Newslieferanten Dow Jones Newswires und AWP, Charts, individuelle Listenverwaltung sowie Gesellschaftsdaten wie Aktiensplitts oder Dividendenauszahlungen. «Telekurs iD mobile», das derzeit nur im Package mit der Desktoplösung «Telekurs iD Intelligent Display» angeboten wird, läuft auf dem BlackBerry-Geräte der kanadischen RIM (Research in Motion). Geplant ist zudem die Einführung der Lösung auf andere Endgeräten wie etwa den Treo 650 von Palm.

## Mobile Virenseuche

Trotz faszinierender Technik und enormem Markterfolg haben diese den vermeintlichen Nachteil, dass sämtliche Datenströme von den BlackBerry-Enterprise-Servern zwingend via VPN zum BlackBerry-Internet-Gateway-Server in London getunnelt werden. Selbstredend, dass «iD mobile» mit den exakt gleich hoch stehenden Sicherheitsmassnahmen ausgestattet ist wie die stationären iD-Lösungen für die Finanzprofis. Ein Restrisiko mag bei Telekurs und Rolotec niemand abstreiten. Deshalb gibt es durchaus Unternehmen, die aus diesem Grund den Einsatz von BlackBerrys kategorisch ausschliessen.



**Erhöhtes Sicherheitsrisiko: Beim Mobile-Banking können hochsensible Unternehmensdaten nicht mehr so einfach unter Verschluss gehalten werden**

Laut Sicherheitsexperten sind missbräuchliche Situationen theoretisch denkbar. Die Gefahr ist allerdings äusserst gering. Zudem betreffen diese keinesfalls die Anwendungen an sich, sondern die Verwendung von BlackBerry-Geräten.

Grundsätzlich stellen sämtliche mobilen Endgeräte ein Sicherheitsrisiko dar. Dass diese Aussage begründet ist, kann leicht nachgeprüft werden. Man gebe die entsprechenden Stichworte in eine Suchmaschine ein und staune ob der Vielfalt an themenaffinen Studien, Umfragen, Artikeln und Weblogbeiträgen. Kurz zusammengefasst,

werden vorab mobile Viren als ernste Bedrohung angesehen. Gemäss Sicherheitspezialisten können sich Viren, Trojaner und Würmer auf mobilen Plattformen immer besser ausbreiten. Unangenehm, da sich gleichzeitig der Nachrichtenverkehr in mobilen Netzen ausdehnt.

#### Unsicherheitsfaktor Mitarbeiter

Die Zahl der Malware ist letzter Zeit dramatisch angestiegen. Das Bewusstsein für die Gefahren hat sich trotzdem noch nicht etabliert. Der Virenschutz für mobile Geräte beispielsweise ist in vielen Unternehmen überhaupt kein Thema. Gemäss Gartner Group ist das noch nicht mal allzu gravierend. Die Gefahr, dass sich ein Virus oder Wurm auf mehr als 30 Prozent aller mobilen Endgeräte verbreiten könnte, wird von den Gartner-Analysten konstant klein beschrieben – zumindest für die nächsten beiden Jahre. Anschliessend werde das Risiko massiv zunehmen, weil die Gefahr einer sich rasch verbreitenden Virusattacke mit der Verbreitung von Smartphones steige – für 2007 sagt Gartner einen Smartphone-Marktanteil von bereits fünfzehn Prozent voraus. Kommt dazu, dass eine Konsolidierung der derzeit noch sehr vielfältigen Betriebssysteme stattfinden dürfte. Selbstredend, dass damit die Verbreitung von schädlicher Software begünstigt wird.

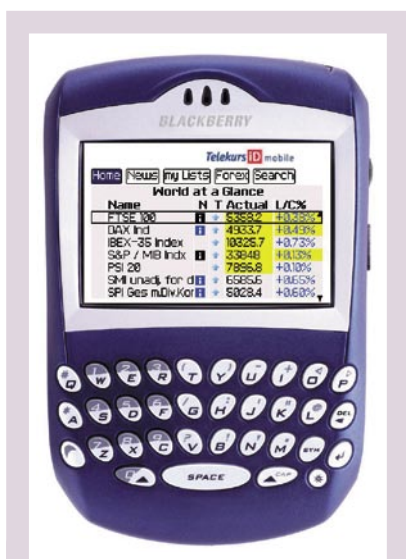
Die Verwundbarkeit der Unternehmensnetze wird vielfach nicht nur durch effizientere Viren, sondern vor allem auch durch mangelnde Restriktionen erhöht. Ein stattdessen Anteil von Sicherheitsverantwortlichen weiss nicht, wie viele und welche privaten

Mobilgeräte an das Firmennetz angeschlossen sind. Viele User spiegeln ihre Daten – und auch diejenigen des Unternehmens – zudem ohne Wissen des Arbeitgebers auf «öffentlichen» Servern, um jederzeit und von jedem Rechner aus Zugriff zu haben. Die Chance, dass solche Server – und damit sensible Daten – gehackt werden, ist gross.

Die Gefahren rund um die Parallelnutzung von beruflichen und privaten Inhalten haben sich auch im jüngsten Bericht des Bundesamtes für Sicherheit und Informationstechnik zur Lage der IT-Sicherheit in Deutschland niedergeschlagen: «Beruflich eingesetzte mobile Endgeräte befinden sich zudem oft ausserhalb der Sicherheitsgrenzen des Unternehmensnetzes. Verfügen sie über einen Netzzugang, können sie für den Einbruch in die IT-Systeme eines Unternehmens missbraucht werden. Schutzmassnahmen wie Virens Scanner oder Firewalls werden zwar mittlerweile auch für eine Reihe mobiler Endgeräte angeboten, sind jedoch noch kaum verbreitet.»

Oft wird auch vergessen, dass Geräte schlicht verloren gehen oder gestohlen werden können. Der Verlust von sensiblen Unternehmens- und Kundendaten hat mitunter schwerwiegende, teilweise auch juristische Folgen.

Konsequente Vorgaben betreffend Handhabung von Unternehmensdaten sind genauso unumgänglich wie effiziente Sicherungs- und Überwachungsmaßnahmen. Wer das bereits heute als selbstverständlich empfindet, wird die Freuden und Vorteile der mobilen Zukunft unbeschwert nutzen können. ■



**Hat sich trotz Sicherheitsbedenken als Endgerät durchgesetzt: BlackBerry von RIM**