

# Plädoyer für Pragmatik

*Die potenziellen Vorteile von Enterprise Mobility sind bekannt. Der Weg dahin weniger. Es scheiden sich die Geister, ob die Security auf die Devices oder ins Netzwerk gepackt werden soll. Höchste Zeit für pragmatische Ansätze.*

MARTIN TRACHSEL

Vom CEO bis zu den Mitarbeitenden an der Verkaufs- oder Servicefront – für alle gilt immer mehr die Maxime, immer und überall Zugriff auf die Daten und Anwendungen des Unternehmens zu haben. Die viel beschworene virtuelle Organisation verspricht ein noch nie da gewesenes Mass an Flexibilität, neue Kooperationsmodelle sowie Effizienz- und Produktivitätssteigerungen. Eine zentrale Rolle spielt dabei der Sammelbegriff «Enterprise Mobility». Er bezeichnet die Mobilität des gesamten Unternehmens mit seinen Mitarbeitenden, Leistungen, Produkten, Prozessen, Informationen und Software. Beim Umsetzen der umfassenden Enterprise-Mobility-Strategien stehen besonders ICT-Integrationsprojekte und die eng damit verknüpfte Frage der Sicherheit im Vordergrund.

## Mega-Trend

Diese Entwicklung ist kein kurzlebiger Hype, sondern ein mit eindrücklichen Zahlen unterlegter Mega-Trend: Allein

in der Schweiz schätzten in einer im laufenden Jahr durchgeführten Umfrage (SECO, 2/2007) 76% der Unternehmen mobile Dienste wie Mobiltelefon, Smartphones oder eine elektronische Agenda (PDA) als wichtig bis sehr wichtig ein. Auch international sprechen die Prognosen eine klare, unüberhörbare Sprache: So rechnet Forrester Research in einer im April 2007 herausgegebenen Studie (Evolution of the Enterprise Mobility Market), dass im Zeitraum 2008–2013 Mobility-Pläne international so richtig zu greifen beginnen werden, wodurch Wireless-Technologien einer grossen Mehrheit der Mitarbeitenden zu Verfügung stehen werden.

Geschäftskritische Mobile-Initiativen werden zur Norm für Unternehmen aller Grössen. Darüber herrscht Einigkeit. Über das Wie hingegen wird in Fachkreisen und in zahllosen Blogs trefflich gestritten. Nichts gegen eine gesunde Debattierkultur, doch die Zeit bzw. der Markt drängt auf Lösungen. Neue, pragmatische, also in der Praxis einfach ein-

setzbare Ansätze sind gefragt. Dies umso mehr, da viele Projekte in der Realität Schiffbruch erleiden.

## Süßer Mobile-Traum trifft bittere Realität

Gemäss Effektivitätsmarktbefragungen wie die der IDC (Convenience, Security and Manageability: How to make mobile workforce programs most effective; 10/2006) heisst es am Ende von nicht wenigen Integrationsprojekten im Bereich mobile ITC-Lösungen: «Willkommen in der Wirklichkeit!». Aus erhofften Wettbewerbsvorteilen werden Mehrkosten. Woran liegt das?

Ein Grund für «gut gemeint, aber dumm gelaufen» ist, dass die Initiative nicht mit einem unternehmensweiten Fokus angegangen, sondern vielmehr auf die heterogenen Bedürfnisse einzelner Benutzergruppen reduziert wird. Das ergibt isolierte Remote-Access-Lösungen, welche die Produktivität kaum verbessern, aber immense Unterhaltskosten verursachen. Und selbst wenn Enterprise Mobili-



Quelle: iStockphoto

biltelefone an. Die meisten Unternehmen tun sich schwer mit dem Management dieser verschiedenen Technologien und Endgeräte und versuchen unter grossen Anstrengungen, Kosten und Sicherheit unter Kontrolle zu halten. Entsprechend hoch sind neben der reibungslosen technischen Integration die Anforderungen an ein durchdachtes Device-Management für die mobilen Endgeräte, das viele Aspekte abdeckt wie Sicherheit, Restriktion einzelner Funktionalitäten, Fähigkeit zur Wiederherstellung des Systems oder Unterstützung für die Synchronisation.

### **Applikationen ursprünglich für PCs gedacht**

Wirklich wertvoll werden Mobile Devices dann, wenn mit ihnen die Geschäftsapplikationen mobil gemacht werden können. Obwohl viele Hersteller und Applikationsentwickler die Fähigkeit propagieren, geschäftskritische Tools auf Handheld und Wireless Devices zu übertragen, machen die heutigen Einschränkungen dieser Plattformen die bestehenden Systeme für viele Unternehmen immer noch unattraktiv. Dem ist unter anderem so, weil Geschäftsapplikationen in erster Linie für PCs innerhalb bestimmter Parameter entwickelt wurden, was sich nicht so einfach auf Handhelds übertragen lässt. Fortschritte sind z.B. im Bereich Logistik erkennbar, doch in anderen Feldern steht noch viel Arbeit an.

In diesem Zusammenhang erstaunt es nicht, wenn – speziell mit Blick auf den Sicherheitsaspekt – empfohlen wird, etwa bei der Einführung von Smartphones, auf die Best Practices zurückzugreifen, die

bei der Migration vom Desktop zum Laptop gemacht wurden.

Gerade beim Stichwort Sicherheit bestehen im Zusammenhang mit Enterprise Mobility Bedenken. Sie sind es, die in der Vergangenheit viele CIOs davon abgehalten haben, «wireless» zu gehen. Das erstaunt nicht weiter, denn die Liste an potenziellen Bedrohungen oder Problemen ist lang. Dazu zählen Hacking, Viren, Würmer, Trojaner, Verlust/Diebstahl, Raub, DoS, Spyware, Überwachung, Sniffing, Defekte und Systemstörungen.

Grundsätzlich gelten die klassischen Bedrohungen auch für mobile Systeme. Jedoch ergibt sich für sie ein erhöhtes Risiko in Form von Verlust/Diebstahl, Überwachung/Sniffing und Raub, da sie sich im Gegensatz zu Desktop- und Serversystemen nicht in einem geschützten bzw. kontrollierten Firmengebäude befinden. Es muss sich noch zeigen, welcher Ansatz praxistauglich ist, um die Faktoren Sicherheit, Vertraulichkeit, Integrität und Verfügbarkeit zu gewährleisten.

### **Netzwerk- oder Device-Security?**

Die potenziell zur Unvernunft neigende Spezies «User» lässt sich wohl weder gänzlich noch auf Dauer kontrollieren – ganz zu schweigen vom organisatorischen und ethisch-moralischen Minenfeld. Technologie hingegen schon. Bei mobilen Systemen stellt sich aber die Frage, wo die Sicherheit eingebaut werden soll. Im Endgerät? Im Netzwerk? Oder in beidem? Wird sich diese Frage zu einem «IT-Glaubenskrieg» entwickeln, oder wird einmal

ty mit dem Anspruch einer ganzheitlichen Betrachtung in Angriff genommen wird, stellen sich noch immer genügend Hürden.

### **Vielfalt als Hürde**

Die wesentliche Herausforderung liegt in der Vielfalt der zu integrierenden Zugangstechnologien und Endgeräte. Zum einen müssen heute von einer Remote-Access-Lösung verschiedenste Zugangstechnologien unterstützt werden: Von zu Hause oder vom Hotel aus wird üblicherweise über Breitband-Internetverbindungen gearbeitet. An Bahnhöfen oder Flugplätzen wird mit Vorliebe drahtlos über WLAN-Hotspots kommuniziert. Wird direkt beim Kunden gearbeitet, wird dessen bestehende Netzwerklösung genutzt. Arbeitet man von unterwegs, müssen GSM- oder UMTS-basierte Mobilfunknetze verwendet werden können. Zum anderen besteht dieselbe Vielfalt bei den verwendeten Endgeräten. Je nach Verwendungszweck bieten sich Notebooks, Tablet-PCs, PDA, Smartphones oder Mo-



Quelle: SonyEricsson

*Smartphones werden immer intelligenter. In Sachen Sicherheit bilden sie hingegen noch eines der schwächeren Glieder.*

Überall und jederzeit Zugriff auf die Firmendaten und -anwendungen: der Mega-Trend.



Quelle: SonyEricsson

mehr der Weg der praktischen Machbarkeit obsiegen?

### Pragmatisch kombiniert

Es gibt sie bereits, die so dringend nötigen pragmatischen Lösungsansätze als Ergebnis konkreter Erfahrungen. Zum

Beispiel jener Ansatz, der minimalen Device-Schutz mit State-of-the-Art Security auf Netzwerkebene kombiniert. Grob skizziert heisst das:

Ein Minimalschutz ist heute gut umsetzbar, also Personal Firewall und Virenschutz auf jedem mobilen Gerät. Alles

andere kann gegenwärtig weggelassen werden, weil die Kosten im Vergleich zum Nutzen schlicht zu hoch sind. Der springende Punkt dabei: Sobald ein solches Mobilgerät eine Datenverbindung ins vertraute Unternehmensnetz (LAN) herstellen will, muss das Gerät vorgängig geprüft werden. Der sichere Zugang erfolgt über VPN (Virtual Private Network), die Überprüfung mit Network Access Control. Beim Verbindungsaufbau erfolgt die Access Control, und anhand der gültigen Sicherheits-Policies wird entschieden, ob ein Gerät Zugang ins Netz erhält oder in einen Quarantänenbereich weitergeleitet wird. In der Quarantäne stehen minimale und nicht sicherheitskritische Dienste zur Verfügung. Reichen diese Dienste dem Benutzer nicht aus, so muss er zuerst sein Gerät wieder in Stand stellen. Der Benutzer wird so zusätzlich sensibilisiert. Dieser Ansatz hat in dieser oder abgeänderter Form grosses Potenzial, realisiert zu werden, denn die entsprechenden Technologien bzw. Produkte und Dienstleistungen stehen schon zur Verfügung. Einer Zukunft, welche die Enterprise-Mobility-Versprechen von Wettbewerbsvorteilen und Produktivitätsgewinnen mit cleverem Mobile-Device-Management sowie einem pragmatischen Optimum an Sicherheit kombiniert, steht grundsätzlich nichts im Weg.



Remote Access Services von United Security Providern ermöglichen sicheren Fernzugriff auf das Unternehmensnetz, unabhängig von Endgeräten oder Zugangstechnologien.

Der Autor: Martin Trachsel ist verantwortlich für den Bereich Enterprise Network Services von United Security Providern.