

iPhone im Geschäftsumfeld: Wo liegen die Risiken?

Das ursprünglich für den privaten Einsatz konzipierte Smartphone von Apple dringt zunehmend in die Geschäftswelt und damit in die IT-Infrastruktur der Unternehmen vor. Dies wirft einige Fragen auf – ganz besonders zur Sicherheit.

→ VON RETO HEUTSCHI

Der Anteil an iPhone-Nutzern im Vergleich zur Gesamtbevölkerung ist in der Schweiz höher als in jedem anderen Land. Laut Apfelblog.ch besaßen schon Ende 2009 rund 7,8 Prozent der Schweizer ein iPhone, inzwischen dürften es schon wieder mehr sein. Auf der anderen Seite setzen immer mehr Unternehmen auf mobile Kommunikationslösungen, um Kosten zu reduzieren und die Produktivität zu erhöhen. Dies wirft für die Entscheidungsträger die Frage auf, ob man iPhones ins Unternehmen integrieren soll und welche Risiken damit verbunden sind.

Blickt man in der Evolution der Mobilkommunikation ein paar Jahre zurück, fällt auf, dass das iPhone als eines der ersten Mobiltelefone die Funktionen eines Geschäfts-Handys mit der privaten Nutzung verband. Dazu zählen etwa der Zugriff auf Kalender, Mail oder Kontakte und im privaten Bereich Musik, Videos oder Fotos. Der «Homo Digitalis» rückt damit dem Dogma der Einheit einen Schritt näher. Gleichzeitig steht die Firmen-IT vor der Herausforderung, die private Nutzung nur so viel wie nötig einzuschränken und dennoch die Firmendaten angemessen zu schützen.

Alle drei Teilsysteme einer mobilen Lösung, egal, ob nun auf dem iPhone oder einem anderen Smartphone, sind gewissen Gefahren ausgesetzt; sowohl das Mobiltelefon inkl. Applikationen als auch die Übertragungsstrecke der Daten und die Firmeninfrastruktur sind zu

schützen. Um diesem Umstand gerecht zu werden, ist ein durchgehendes Sicherheits- und Betriebskonzept nötig, das Massnahmen aus technischen Komponenten, Betriebsprozessen und administrativen Vorgaben vereint.

GEFAHR 1: MOBILTELEFON & NUTZER

Geräteverlust oder Gerätediebstahl sind beim iPhone aufgrund seines Prestiges sehr häufig. Es gibt grundsätzlich vier Optionen, um die Sicherung der Daten auf dem Gerät zu gewährleisten: Per Config-File, das mit dem Apple Configuration Tool bereitgestellt wird, mit Policies aus Microsoft Exchange, via Gerätemanagementsystem und mithilfe einer Applikationsverschlüsselung. Diese Varianten weisen gewichtige sicherheitstechnische und betriebliche Unterschiede auf. Mit dem Config-File können etwa der App Store und die Kamera gesperrt werden, doch steht es im Ermessen des Nutzers, ob er dieses installieren will oder nicht. Auf der anderen Seite können die Exchange Policies erzwungen werden, bieten aber nur verhältnismässig wenige Möglichkeiten. Gerätemanagementsysteme werden ab iOS4 unterstützt, sodass sich zum Beispiel Sicherheitseinstellungen auch ohne Exchange durchsetzen lassen. Eine interessante Lösung ist der Schutz von Daten in einer Applikation. Diese Option kommt der parallelen privaten und geschäftlichen Nutzung am ehesten entgegen, bedingt aber eine zusätzliche Software inkl. Server im Backend.

All diese Massnahmen bringen keine hundertprozentige Sicherheit, schaffen aber Zeit für prozesstechnische Massnahmen. Bei einem Geräteverlust müssen sich die Mitarbeiter möglichst schnell melden, damit der Helpdesk einen RemoteWipe auslösen, das ActiveSync-Konto und die SIM-Karte sperren kann. Zu beachten ist die Erreichbarkeit des Helpdesks und eine Ausweichlösung, falls dieser geschlossen ist.

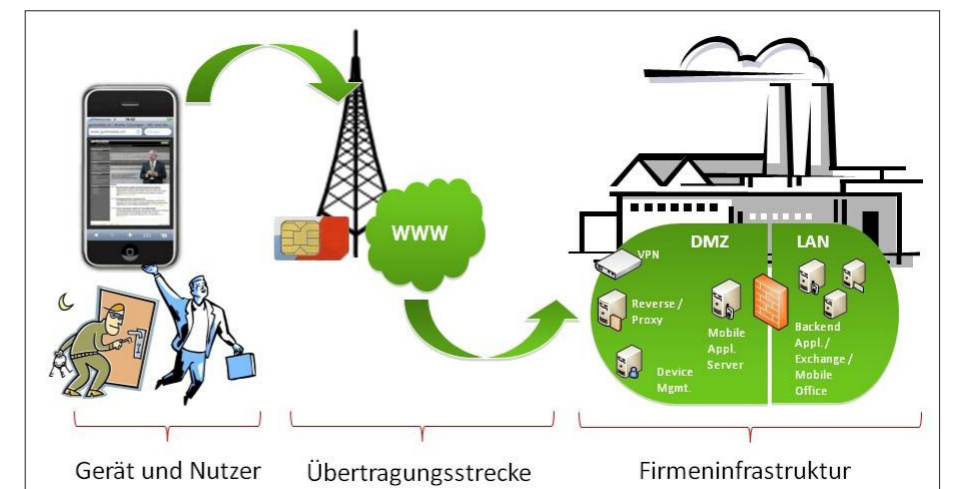
Als drittes Element kommen die administrativen Massnahmen hinzu, die den Nutzer unter anderem anhalten, regelmässig OS-Updates zu machen und keine Jailbreaks auf dem

iPhone durchzuführen. Da durch einen Jailbreak auch Applikationen auf die Geräte gelangen, die nicht von Apple zertifiziert sind, steigt die Gefahr eines Malware-Befalls. Per Jailbreak lassen sich zudem PIN-Schutz und Hardware-Verschlüsselung umgehen. Eine umfassende Information der Nutzer ist nicht nur in dieser Hinsicht wichtig. Wenn die Gefahren verstanden werden, passen die Nutzer auch ihr Verhalten an. Das trägt einerseits zur Sicherheit bei und hilft andererseits, teure Roaming-Rechnungen zu vermeiden.

GEFAHR 2: ÜBERTRAGUNGSSTRECKE

Um ein Mithören im Datentransfer vom oder zum Mobiltelefon zu verhindern, gibt es zwei Optionen. Im ersten Fall wird mit Operator-Produkten dafür gesorgt, dass potenzielle Mithörer gar nicht erst an den Datenstrom kommen. Der Verkehr läuft dabei nicht über das öffentliche Internet, sodass sich ein Angriff sehr aufwendig gestaltet. In der zweiten Variante werden die Daten verschlüsselt, sodass sie für den Angreifer nutzlos sind. Dies kann direkt von einer Applikation wie ActiveSync übernommen werden oder der gesamte Datenverkehr wird über eine Zusatzapplikation getunnelt und am Firmenrouter terminiert.

Eine weitere Bedrohung stellt der unkontrollierte Internetverkehr dar. Sicherheitslücken im Browser, Phishing und das Abhören oder Manipulieren von Kommunikationsinhalten sind nur



Für starke Sicherheit ist ein durchgehendes Konzept zwingend

einige Gefahren, welche im World Wide Web lauern. Die Nutzung von Safari kann unterbunden werden, ist jedoch nicht im Sinne des Nutzers. Die interessantere Lösung ist, den Browserverkehr über die Firmeninfrastruktur zu führen und die gleichen Richtlinien anzuwenden, wie sie für die PC-Nutzung gelten.

GEFAHR 3: FIRMENINFRASTRUKTUR

Beim Schutz der Infrastruktur gilt es, in erster Linie darauf zu achten, dass nur solche Daten und Services zur Verfügung stehen, die wirklich benötigt werden. Des Weiteren sollte für diese

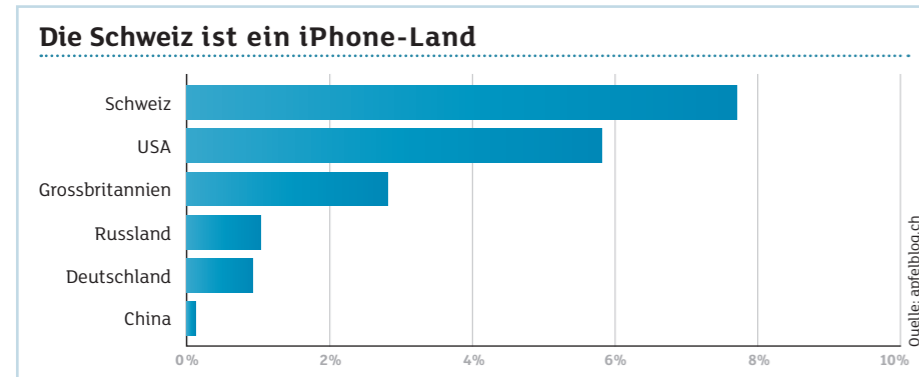
Services nur Verkehr aus dem Mobilnetz zugelassen werden; die Mobile-Anbieter entlassen den IP-Verkehr über ganz wenige Knoten ins Internet. An den Eintrittspunkten der Firma ist der Verkehr gründlich auf Malware zu prüfen, da davon ausgegangen werden muss, dass dieser von nicht geschützten Quellen (iPhones) stammt. Voraussetzung dafür ist, dass es einen definierten Eintrittspunkt gibt. Ein wichtiges Thema sind firmeneigene WLANs. Diese erlauben dem Nutzer, einfach an sehr viele Firmendaten zu gelangen. Oft werden die WLANs auch nicht über einen zentralen Punkt geführt, ein Scannen der Daten ist also schwierig. Diese Gefahr ist auch deshalb gross, weil die Zugangsdaten in der Regel auf den Mobiltelefonen gespeichert werden und so der «Finder» eines Geräts ungehinderten Zugang zu den Firmendaten hat.

Das neue iOS4 zusammen mit entsprechenden Gerätemanagementsystemen und bis zu einem gewissen Grad auch Exchange 2010 sind Werkzeuge, mit denen Inventurdaten der Mobiltelefone, wie Operating System, Gerätetyp etc., ausgelesen werden können. Mit diesen Informationen kann der ActiveSync-Verkehr regelbasiert zugelassen oder gesperrt werden; ein starkes Werkzeug zum Schutz der Infrastruktur.

FAZIT: UNTER VORBEHALT SICHER

Das iPhone ist aus Nutzersicht ein sehr attraktives Gerät, das private und geschäftliche Funktionen vereint. Arbeitgeber können ihren Mitarbeitern einen Gefallen tun und zudem erstmals ohne grossen Widerstand die Mobilflotte vereinheitlichen. Mit diesem Schritt handelt man sich einige Sicherheitsrisiken ein, die allerdings weitgehend für alle Mobiltelefone gelten. Mit einer klaren Sicherheits- und Betriebsstrategie und dem abgestimmten Einsatz von technischen, prozessualen und administrativen Massnahmen kann das iPhone in den meisten Fällen trotzdem mit gutem Gewissen im Geschäftsbereich eingesetzt werden. Verbunden mit den zusätzlichen Features des iOS4 dringt das iPhone damit weiter in die Firmenwelt vor. ←

Reto Heutschi ist Geschäftsleiter der go4mobile ag



Vermuteter Anteil der iPhone-Nutzer an der Gesamtbevölkerung

