go4mobile
Einfach kompetent

Der Einzug des iPads in die Geschäftswelt

Das iPad 2 erschliesst eine Menge neuer Nutzungsszenarien und dringt mit seinen umfangreichen Features ins Geschäftsumfeld ein. go4mobile hat untersucht, welchen Mehrwert Apples Tablet bringt und worauf Unternehmen in Bezug auf Sicherheit achten sollten.

Benutzerfreundlichkeit

Office-Dokumente bearbeiten, E-Mails checken, Mindmaps zeichnen und Visualisierungen erstellen; mit dem iPad steht dem Nutzer ein kompaktes Werkzeug zur Verfügung, welches Mobilität und Nutzerkomfort vereint. Die Grösse des Bildschirms bietet einen praktischen Mehrwert gegenüber dem Smartphone. In Bezug auf das Gewicht und die Akkulaufzeit liegt das Tablet, verglichen mit dem Laptop, deutlich vorne.

Vor allem für Mitarbeiter mit Kundenkontakt erschliessen sich mit dem iPad viele neue Nutzungsszenarien. So kann beispielsweise der Aussendienstmitarbeiter dem potentiellen Kunden Präsentationen in einer angenehmen Grösse vorführen. Auch kann er mit dem iPad vor Ort elektronische Formulare ausfüllen, ohne zwischen sich und dem Kunden eine „Bildschirm-Mauer“ zu errichten. Gleichzeitig hat er jederzeit Zugriff auf die von ihm gewünschten Informationen.

Prozessautomatisierung

Typische Medienbrüche zwischen Papier und Computer können mit dem iPad beseitigt werden. Der Aussendienstmitarbeiter nimmt eine Bestellung bequem über das iPad auf, diese wird direkt zum Verkaufsinnendienst weitergeleitet, die Bestellung ausgeführt und die Rechnung verschickt. So werden Prozessschritte eliminiert, der Kunde schneller beliefert und im genannten Beispiel das Zahlungsziel signifikant verbessert. Die meisten Arbeitsschritte können direkt auf dem iPad umgesetzt werden, so dass Prozesse massgebend verkürzt werden können. Doch bei all den Lobeshymnen auf die Möglichkeiten des Einsatzes von iPads im Geschäftsumfeld, darf die Sicherheit nicht vergessen werden.

Sicherheit

Im mobilen Gebrauch laufen sensible Dokumente und Adressen Gefahr in falsche Hände zu geraten. Ein umfassendes Sicherheitskonzept mit entsprechenden Massnahmen liegt deshalb im Interesse von Unternehmen und Mitarbeitern. Aufgrund der zu bearbeitenden Daten bewegen sich die Sicherheitsszenarien dabei näher am Laptop als am Smartphone.

Die Sicherheitsanforderungen hängen eng mit der Art der Nutzung zusammen. Wird per RAS auf Firmendaten zugegriffen, fällt dieser Zugriff umfassend aus; ein ausgefeiltes Sicherheitskonzept ist zwingend. Auch ein PIM-Sync Zugriff über Exchange ActiveSync auf die Daten ist nicht ungefährlich, obwohl er auf Kalender, Mail, Kontakte und Aufgaben beschränkt ist. Denn auch diese Daten liegen nach der Synchronisation lokal auf dem Gerät, was das potentielle Sicherheitsrisiko erhöht. Die sicherste Art eines Zugriffs auf Firmendaten ist diejenige des View. Dabei werden beispielsweise Kalender, Mail, Kontakte

go4mobile ag
Felsenaustrasse 17
3004 Bern

Telefon: +41 (0) 31 914 18 18
Fax: +41 (0) 31 914 18 19

oder Aufgaben angezeigt, ohne dass diese auf das Gerät geladen werden. Der Nachteil liegt darin, dass die Daten nur zugänglich sind, wenn eine Internetverbindung besteht.

Grundlage für den Schutz mobil genutzter Daten bildet der allgemeine Standard des jeweiligen Unternehmens zum Schutz von Firmendaten. Daraus werden die konkreten Sicherheitsmassnahmen aus den Bereichen Technik, Prozesse und administrative Vorkehrungen abgeleitet und eingeführt. Die am häufigsten eingesetzten technischen Massnahmen sind PIN-Schutz und Remote Wipe. Weiter wächst der Wunsch, Apps kontrollieren zu können. Da aber Apple nicht zulässt, dass selektive Apps gesperrt werden, kann wenigstens ein Monitoring vorgenommen werden, um zu überprüfen, ob verbotene Apps auf einem Gerät installiert sind.

Unter anderem wenn ein Gerät verloren geht oder gestohlen wird, spielen die Betriebsprozesse eine bedeutende Rolle. Der Nutzer muss jederzeit sein Gerät aus der Ferne löschen können. Dazu braucht es beispielsweise einen Helpdesk, der sinnvoll erreichbar ist oder ein Selfservice-Protal, damit der Nutzer das Löschen selber auslösen kann. Nicht zuletzt kommt administrativen Massnahmen eine gewichtige Bedeutung zu. Auf dieser Ebene können beispielsweise durch Schulungen und Verbote die Mitarbeiter auf Probleme aufmerksam gemacht werden, welche auf den vorangehenden Ebenen nicht gelöst werden konnten oder sehr aufwändig zu lösen sind. Verbote können dann mit technischen Mitteln, z.B. Monitoring von Apps, kontrolliert werden.

Schlussendlich liegt es im Ermessen des jeweiligen Unternehmens, wie der Zugriff auf sensible Daten gestaltet werden soll. Dabei sollte jedoch ein ausgeklügeltes Sicherheitssystem aufgesetzt werden, welches den Nutzer nicht oder nur minimal beeinträchtigt. Die gewonnene Effizienz darf auf keinen Fall durch komplizierte Sicherheitsmassenamen wett gemacht werden. Gerne helfen wir von der go4mobile ag Ihnen dabei eine Lösung zu realisieren, die einen deutlichen Mehrwert für Nutzer und IT generiert.

go4mobile ag
Felsenaustrasse 17
3004 Bern

Telefon: +41 (0) 31 914 18 18
Fax: +41 (0) 31 914 18 19