iPad® im Business

Kompendium zur Integration von iOS Geräten

Konzeptionierung | Netzwerkanbindung | Management | Sicherheit

Eine Publikation der brainworks computer technologie GmbH | 3. Auflage € 5,90

„Wir liefern schon heute tragfähige Lösungen für die mobile Kommunikationswelt der Zukunft“, lautet der Leitspruch des Münchner Value Added Distributors brainworks, aus dessen Reihen sich die drei Autoren rekrutieren. brainworks bietet seit 1989 Kunden und Handelspartnern innovative Technologien, fundierte Marktkenntnis und Expertise. Für das Kompendium iPad® im Business haben die Spezialisten aus den Fachbereichen Hochleistungs-WLAN, Netzwerkanalyse und Clientmanagement Ihr Wissen zusammengetragen, um einen ganzheitlichen und langfristig erfolgreichen Best Practice Ansatz zu entwickeln.

Christian Rattmann verantwortet seit 2007 das Kundensegment Clientmanagement und heterogene Netzwerke. Zu seinen Kernkompetenzen gehören die Konzeptionierung und Begleitung von Mittelstand- und Enterprise-Projekten zur Clientintegration. Aus seiner bisherigen Laufbahn bringt er tiefgehendes Spezial Know How auf dem Gebiet Qualitäts- und Prozessmanagement und Praxiserfahrung aus rund 10 Jahren als selbständiger Unternehmer mit. Zudem ist er Sprecher der Enterprise Desktop Alliance und Initiator der Xing Gruppe „Apple/Mac und Enterprise“.

Christian Rattmann: 089 326764-37 | rattmann@brainworks.de

Aurel Takacs ist seit 2008 Sales Engineer für Public Internet Access und WLAN. Von der operativen Planung bis zum Going Live ist er der zentrale Ansprechpartner für anspruchsvolle Gästeinternet Projekte in Enterprise Umgebungen, gehobener Hotellerie als auch Messe- und Konferenzzentren. Zahlreiche Referenzinstallationen profitieren von seiner langjährigen Netzwerkerfahrung und Spezial Know How auf dem Gebiet Hochleistungs WiFi und AAA-Lösungen.

Aurel Takacs: 089 326764-23 | takacs@brainworks.de

Stefan Haberland ist seit 2003 als NGN Technologie Spezialist der Experte, wenn es um Performance und Hochverfügbarkeit von Netzwerken geht. Mit 10 Jahren Praxiserfahrung, umfassendem Netzwerk Know How und großer Beratungskompetenz sorgt er für den Erfolg bei der Konzeptionierung und Realisierung großflächiger Hochleistungs WiFi Projekte bis zur Highspeed-Netzwerkanalyse in komplexen Rechenzentrumsstrukturen.

Stefan Haberland: 089 326764-19 | haberland@brainworks.de

Sehr geehrter Interessent,

laut Wikipedia ist das iPad® ein Tablet Computer des amerikanischen Herstellers Apple Inc., der sich durch einen berührungsempfindlichen Bildschirm bedienen lässt.

Den Absatzzahlen und der Präsenz in den Medien nach zu schließen ist es mehr: Anwender und Unternehmen empfinden es als neue Geräteklasse oder gar als Retter ganzer Wirtschaftszweige. Die Folge ist, dass sich Administratoren konzeptionell und technisch damit auseinander setzen und Lösungen zum Thema Integration, Administration und Sicherheit finden müssen.

Mit diesem Kompendium wollen wir Ihnen einen Leitfaden an die Hand geben, der alle relevanten Schritte beleuchtet von der Konzeption über Netzwerkanbindung und Management bis hin zu Sicherheitsaspekten...damit mit dem iPad® nicht Frust, sondern Freude aufkommt – sowohl beim Administrator und nicht zuletzt beim User.

Herzliche Grüße

Christian Rattmann, Aurel Takacs & Stefan Haberland

Anwendergruppen und Konzeptionierung 5

Empowering Employee
Hardwareklassen und Anwendungen

Mobile Security der Zukunft 7

Starke Authentisierung
One-Time-Passwörter (OTP): Flexibel und sicher
Richtlinien langfristig durchsetzen – lässt sich Sicherheit automatisieren?
Kontrollierte Contentfreigabe nur für autorisierte Devices
iOS Backup

Netzwerkanbindung 12

Grenzerfahrung 3G
Site Survey. Planungssicherheit statt Kostenfalle
Funkzellenplanung
5 GHz ist die Zukunft
Die Alternative: WiFi-Array
Sicheres WLAN - heute und in Zukunft
Intelligente Verteilung der WLAN Clients

Management 18

Architektur
Möglichkeiten der Konfiguration
App/Softwareverteilung
Weitere Funtionen von MDM Server Produkten

Virtualisierungsansatz 25

Quick Views 27

WLAN Planung
Mobile Security
Mobile Device Management Planung

Empowering Employee

Die IT Strategie gerade großer Unternehmen war bis vor kurzem noch vom Begriff der Standardisierung geprägt. Galt es vor ein paar Jahren noch als Ziel, die Mitarbeiter mit gleichen Rechnern, gleichen Desktops und gleichen Images auszustatten, startet seit kurzem eine komplett gegensätzliche Entwicklung unter dem Oberbegiff „Empowering Employees", bedeutet: Dem User soweit wie möglich alle Freiheiten im Bezug auf Hard- und Software zu bieten. Im Zuge dessen wird auch immer wieder der Begriff Self Service Konzept verwendet, der ausdrückt, dass z.B. Software nicht mehr von der IT Abteilung standardmäßig vorinstalliert wird, sondern der Benutzer diese bei Bedarf selbst installiert. Individualisierung ist das neue Stichwort und IT Abteilungen haben oft nur die Auswahl zwischen zuschauen oder einer aktiven Steuerung der Entwicklung.

Eine der wichtigsten Vorraussetzungen, um das Konzept der Freiheit zu unterstützen ist die clientunabhängige Organisation von Unternehmensanwendungen und IT Infrastruktur, z.B. durch browserbasierende Anwendungen.

Anwendergruppen und Konzeptionierung

Mehr als zwei Drittel der Tätigkeiten im Arbeitsalltag lassen sich in der ein oder anderen Form auf das Erfassen und Verwalten von Daten oder das Ausfüllen von Formularen reduzieren - ideal, um mit Clients wie dem iPad® erledigt zu werden. Dies betrifft nicht nur Mitarbeiter im Büro mit festen Arbeitsplatz, sondern auch Berufsbilder mit überwiegender Aussendienst-Tätigkeit. Kurz gesagt - mobile Mitarbeiter. Für das Erfassen von Gesprächsnotizen werden weder ein großer Bildschirm noch ein vollwertiger PC oder Mac benötigt. Notwendig ist nur eine Anbindung an zentrale Datenbanken und Anwendungen wie CRM - also eher performancearme Applikationen wie einen Browser.

Das ist weiter nichts Neues und wird in Großunternehmen schon seit Jahren mit sog. Thin oder Zero Clients praktiziert. Das Besondere an der Geräteklasse „Tablet" oder iPad® ist die emotionale Bindung des Anwenders an das Endgerät: Es ist chic, wird gerne in die Hand genommen, verbindet die private Ebene mit dem Geschäft. Gerade bei jüngeren Anwendern oder sog. Digital Natives mit ihrem Userverhalten ist die Akzeptanz und Affinität sehr hoch (http://community.citrix.com/pages/viewpage.action?pageId=158574140). Es wird als Belohnung empfunden, wenn vom Arbeitgeber solche Geräte bereitgestellt werden. Das geht soweit, dass sich viele Anwender die Geräte auf eigene Kosten beschaffen. Teilweise wird dies auch von Unternehmen in sogenannten „Bring your own PC" (BYOPC) oder „Bring your own Device" (BYOD) Programmen gefördert.

Die Auswirkungen auf die Supportkosten der Unternehmen kann durchaus positiv sein. Denn...beschafft sich der Anwender die Hardware selbst, werden auch Hardware Supportfälle auf den Anwender übertragen. Die Unternehmen unterstützen nur noch die Softwareprobleme, die durch unternehmensrelevante Lösungen entstehen. Klingt auf Anhieb gut. Kann aber dazu führen, dass sich andererseits die Software Supportfälle spürbar erhöhen. Schließlich hat der User mehr Rechte, verglichen zu Strukturen mit zentral kontrollierten Endgeräten.

Die Verbindung von „Privat“ und „Geschäft“ auf einem Device hat aber noch weitere Auswirkungen auf die Konzeptionierung beim Unternehmenseinsatz von iOS Geräten, z.B. private Apps vs. Business Apps, gewünschte Apps vs. unerwünschte Apps.

Nach heutigem Stand ist es keinem Hersteller von iOS Management Software - trotz eventueller gegenteiliger oder suggestiver Darstellung - möglich, den Download bestimmter Apps im Einzelnen und gezielt einzuschränken. Es besteht nur die Möglichkeit, die Installation von Programmen/Apps und/oder den Kauf von Apps aus dem Apple AppStore generell zu erlauben oder zu verbieten. Näheres entnehmen Sie bitte dem Abschnitt „Management“.

Bei iPads®, die z.B. nur bei Messen oder in der Produktion genutzt werden, ist eine komplette Einschränkung bezüglich der Installation von Apps umsetzbar und sinnvoll. In anderen Einsatzbereichen wirkt sich ein solches Vorgehen sehr negativ auf die Akzeptanz der Devices aus, insbesondere wenn die iPhones® und iPads® vom Mitarbeiter selbst angeschafft wurden. Insofern ist es sehr ratsam, sich mit diesen Aspekten der Consumerization bei der Konzeptionierung des iOS Einsatzes zu befassen.

Um die iPads® effizient zu nutzen, sollten Unternehmen Anforderungen und Tätigkeiten der Mitarbeiter im Vorfeld untersuchen, analysieren und bewerten. Auch unter dem Aspekt, welche Unternehmenssoftware genutzt oder auf welche Systeme vom Mitarbeiter zugegriffen werden muss, ob dies möglich ist, und wenn nicht, welcher Entwicklungsaufwand nötig ist. Nur so lässt sich vermeiden, dass das falsche Gerät für deren Alltag zur Verfügung gestellt wird und even-tuell diesen eher behindert als fördert.

Hardwareklassen und Anwendungen

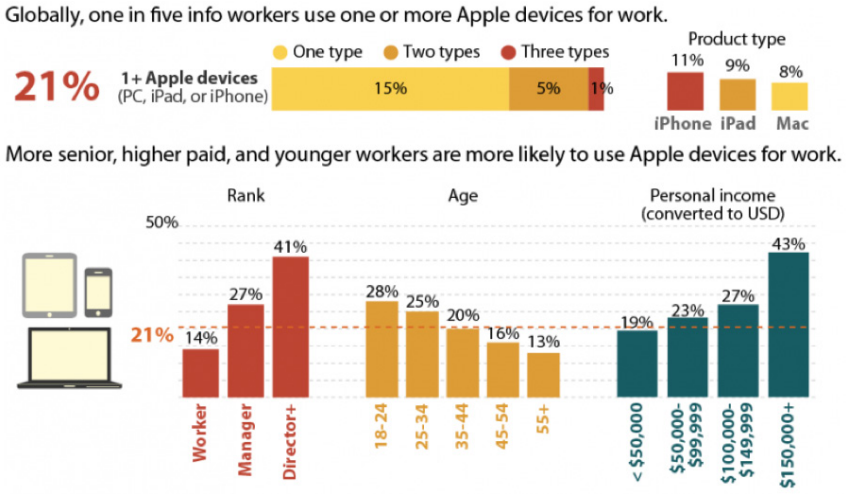
iPhone®/Smartphone: Jederzeit Zugriff
Fokus/Schlagwörter: Konsumieren, Sammeln und Verteilen von Informationen, Ergänzung zum PC oder Mac, Erreichbarkeit
Berufe oder Tätigkeiten: Groupware, E-Mail, Surfen

iPad®/Tablet: Informationsverarbeitung
Fokus/Schlagwörter: Abändern, Ausfüllen, Erfassen, Verwalten, Präsentieren, 80% der Tätigkeiten im Arbeitsmarkt
Berufe oder Tätigkeiten: Außendienstmitarbeiter, Verkäufer, Schüler, Studenten, Kassierer, Ärzte, Lehrer, Monteure, Dienstleister

PC und Mac: Informationserstellung
Fokus/Schlagwörter: Erstellen, kreatives Arbeiten, Produzieren
Berufe oder Tätigkeiten: Rechenintensive Anwendungen, Anwendungen, die einen großen Bildschirm benötigen

Mobile Security der Zukunft: Content statt Hardware sichern

21% der Information Worker nutzen lt. einer jüngsten Forrester Studie Apple Rechner, davon ein erheblicher Anteil iPhones® und iPads®. Und der Trend wird sich in Zukunft noch verstärken, immer öfter flankiert durch gewollte oder geduldete Bring-your-own-Device (BYOD) Generationen. Die Folge: Kontrollverlust bezüglich der Endgeräte, wenn Nutzer zum Beispiel private Geräte anbinden und Kontrollverlust bezüglich des Abflusses von Inhalten wie z.B. Dokumente. Security Konzepte der Zukunft sollten sich deshalb verabschieden vom traditionellen Bestreben, hauptsächlich die Hardware zu sichern. Fokus und Herausforderung liegen darin, den Content zu sichern mit Hilfe von plattformunabhängigen Schutz- und Steuerungskonzepten. Hierbei stehen den Administratoren und Sicherheitsbeauftragten wirksame Stellschrauben zur Verfügung.



Quelle: Forrester Report „Apple Infiltrates The Enterprise" von Frank E. Gillet, Januar 2012

Das iPhone® bietet mittlerweile viele grundlegende Verbesserungen beim Thema Sicherheit, das bislang eher einen Hinderungsgrund für einen Unternehmenseinsatz darstellte.

Die Sicherheitsaspekte können aufgeteilt werden in:

Gerät: Passwortschutz und Methoden gegen unbefugte Nutzung
Daten: Schutz und Verschlüsselung gespeicherter Daten
Netzwerk: Netzwerkprotokolle und Verschlüsselung der Datenübertragung
Programme: „Sandbox" Verfahren und sicheres Framework

Ein sehr umfassendes Apple-eigenes Dokument mit dem Titel „iPhone® in Unternehmen - Sicherheitsaspekte“ erhalten Sie unter diesem Link:

http://images.apple.com/de/iphone/business/docs/iPhone_Security.pdf

Die darin aufgeführten Einstellungen und Einschränkungen, z.B. bezüglich WLAN und VPN, müssen nicht zwingend am jeweiligen Client festgelegt werden. Mit Hilfe von iOS Managementtools können diese auch zentral, drahtlos und aus der Ferne übertragen werden. Bitte achten Sie bei einer entsprechenden Toolauswahl auf die Möglichkeiten der Lösung.

Angesichts der zunehmenden Heterogenität der (mobilen) Gerätelandschaften in den Unternehmen ist bei allen Sicherheitsüberlegungen und nicht zuletzt bei der Wahl geeigneter Security Strategien auf eine ganzheitliche Sichtweise zu achten. Flexibilität und Plattformunabhängigkeit sind dann entscheidende Parameter, um parallele Sicherheitskonzepte zu vermeiden. Diese sind nicht nur kosten- und pflegeintensiv – sie hinterlassen schlimmstenfalls gefährliche Sicherheitsschlupflöcher.

Starke Authentisierung

Grundsätzlich lässt sich jedes Active Sync-fähige Gerät beliebig allein durch Benutzername und Passwort anbinden. Angesichts der Tatsache, dass die mobilen Geräte lediglich das Übertragungsmedium für Unternehmensinformtionen und –daten sind, ist es wichtig, wirksame Sicherheitsmaßnahmen beim eigentlichen Ziel anzulegen. Tatsächlicher Endpunkt in diesem Kommunikationsprozess ist nämlich der Benutzer selbst und nicht die Hardware. Unternehmen müssen jederzeit darauf vertrauen können, dass nur berechtigte Benutzer Zugang zu Unternehmensinformationen bekommen. Dabei gilt es sowohl den Loginvorgang als auch die Zugriffsprotokolle gegen Mißbrauch abzusichern. Diese Anforderung kann mit Hilfe einer 2-Faktor-Authentisierung (2FA) gelöst werden. Dabei lassen sich drei Arten von Faktoren nutzen:

- Etwas, das man weiß, z.B. Passwort oder eine vertrauliche Information
- Etwas, das man hat, z.B. Hardware Token, Handy
- Etwas, das man ist, z.B. biometrische Eigenschaften wie Auge, Fingerabdruck

Mit dem Wissen seiner persönlichen Zugangsdaten bestehend aus Name und persönliches Kennwort kann also die erste Authentisierungshürde genommen werden. Um die Zugangsberechtigung zu verifizieren, haben sich One-Time-Passwörter (OTP) bewährt, die über sog. Token bei Bedarf bereitgestellt werden, sprich in den Besitz des Users gelangen. Diese können mit kleinen handlichen Geräten generiert oder auch einfach via SMS direkt auf das iPhone® übermittelt werden. Für die Wahl der Identifizierungsmerkmale als auch Verteilwege gibt es keine eindeutige Empfehlung. Das optimale Sicherheitskonzept wird maßgeblich vom Einsatzszenario bestimmt. Hier spielen Nutzerverhalten und Gerätelandschaft ebenso eine Rolle wie die IT-Infrastruktur, in die sie eingebettet sind.

Wie stark oder schwach ein Faktor ist, hängt von unterschiedlichsten Aspekten ab. Beispielsweise ist ein kurzes, einfaches Passwort schwächer als ein langes, komplexes. Die Wirksamkeit ist aber wie so oft sehr an das Benutzerverhalten gebunden. Ein Hardware Token z.B. hat nicht annähernd den persönlichen Wert wie das eigene Smartphone. Letzteres wird man weniger leichtfertig verleihen und der Verlust wird auch deutlich schneller auffallen. Andererseits ist der Hardware Token aus technischer Sicht sicherer. Seine singuläre Ausrichtung auf die Bereitstellung eines One-Time-Passworts bietet weniger Angriffspunkte als z.B. SMS-basierte Smartphone Token, die letztlich das GSM Netzwerk passieren.

One-Time-Passwörter (OTP): Flexibel und sicher

OTP Lösungen gewinnen im Zuge des Mobilisierungstrends und steigender Heterogenität der IT Landschaft zunehmend an Bedeutung, weil sie per se Device-unabhängig sind. OTPs können auf JEDEM Gerät – ob stationär oder mobil genutzt werden. Im Gegenteil: Die mobilen Devices selbst werden mehr und mehr als Hardware Token eingesetzt. Smartphones können OTPs sowohl via SMS empfangen oder mittels installiertem Software Token selbst generieren und somit als Hardware Token fungieren. Die SMS Variante ist vor allem aus administratorischer Sicht sehr attraktiv. Existiert die Mobilnummer bereits im Active Directory des Unternehmens geht der Verwaltungsaufwand gegen Null. Software Token haben dafür den Vorteil, dass sie keinerlei SMS Kosten produzieren und auch unterwegs – unabhängig von der Funkabdeckung – jederzeit OTPs generieren können. Eher selten lässt sich aber durchsetzen, dass externe Benutzer einen Software Token installieren.

Risiko Multi-Device-User: Immer öfter wird mal im Büro mit PC, unterwegs per Smartphone als auch mit dem heimischen Tablet auf die Unternehmensdaten zugegriffen. Problematisch dabei ist, wenn OTP und Datenzugriff über ein und dasselbe Gerät erfolgen. In dem Fall rücken Hardware Token wieder mehr ins Rampenlicht, die OTPs generieren unabhängig vom Gerät, über das der eigentliche Zugriff auf die Unternehmensinformationen erfolgt.

Richtlinien langfristig durchsetzen – lässt sich Sicherheit automatisieren?

Die technische Anbindung und eine wasserdichte Authentisierung der mobilen Nutzer ist ein erster Schritt. Langfristig gilt es aber die Einhaltung der mobilen Sicherheitsstrategie möglichst zu automatisieren, soll die BYOD Idee nicht zum Administrationsmonster mutieren. Gerade die iOS Welt bietet dem sog. “empowered user” zahlreiche Schlupflöcher: Beachtenswert ist z.B., dass bei iOS Geräten der Nutzer Administrationsrechte besitzt und sich somit dem Managementsystem durch Löschen der Anbindung entziehen kann. Auch Jailbreak, Diebstahl oder Verlust sind typische ungewollte Eingriffe in das Netzwerk, die durch automatisierte Restriktionen bzgl. Zugriff oder im worst case Löschen von Dokumenten vom mobilen Gerät abgefedert werden müssen.

Ein hilfreicher Ansatz ist, beim Mobile Device Management (MDM) mit dynamischen Gruppen und daraus folgenden Handlungen zu arbeiten. Bedeutet: Entzieht sich ein Nutzer dem System oder begeht eine sicherheitskritische Handlung, werden zeitgleich und automatisiert alle Zugänge zu Firmensystemen entzogen und vorhandene Firmendokumente und Anwendungen unwiederbringlich

gelöscht. Dieser Ansatz wird Carrot&Stick oder Zuckerbrot und Peitsche genannt. Im Gegensatz zu früher muss man den Nutzer heute motivieren – Erzwingen ist bei privaten Geräten schon rechtlich nicht mehr durchsetzbar.

Ein Beispiel: Der Administrator verlangt von Smartphone Nutzern ein komplexes Passwort mit 10 Stellen und 2 Sonderzeichen. Die Vorgabe wird für wenig Begeisterung sorgen, jedoch akzeptiert werden, wenn nur damit bequemer Zugriff zu den gewünschten Dokumenten und hilfreicher Software erlangt werden kann. Setzt der Nutzer die Passwörter außer Kraft, findet er sich in einer Gruppe wieder, die keinerlei firmenbezogene Zugänge, Dokumente oder Software erhält und das mitgebrachte Device somit nicht nutzbar ist.

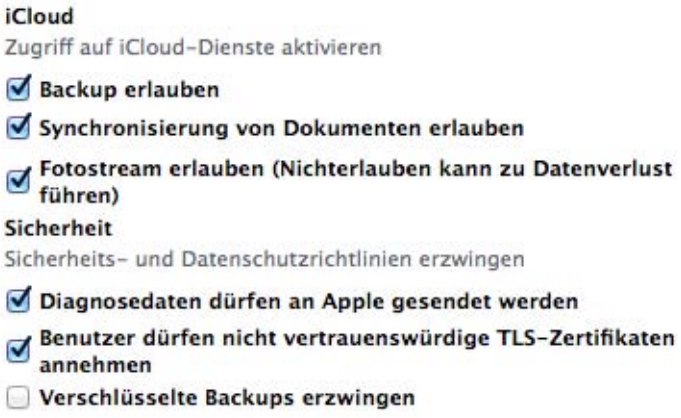
Ein weiterer sicherheitsrelevanter Knackpunkt bei der Nutzung mobiler Devices ist die konsequente Trennung privater und geschäftlicher Nutzung. Insbesondere in BYOD Umgebungen gilt es effiziente Methoden zu etablieren, um eine sicherheitskritische Vermischung zu vermeiden. MDM Lösungen bieten dazu zeitgesteuerte Profile an, die sicherstellen, dass z.B. der Zugriff auf E-Mail, WLAN und Dokumente nur während der üblichen Geschäftszeiten möglich ist. Solche zeitgesteuerten Profile sind zudem hilfreich, um beispielsweise die Gültigkeit von Preislisten durchzusetzen.

Kontrollierte Contentfreigabe nur für autorisierte Devices

Bei aller Wahlfreiheit und mobilen Zugriffsmöglichkeiten hat sich das Microsoft Exchange Active Sync Protokoll als Standard etabliert, wenn es um die Synchronisation von E-Mails, Kontakten, Kalendern, Aufgaben over-the-air geht. BYOD-freundlich, kompatibel mit allen gängigen mobilen Geräten und vor allem ohne Client-Installation auf dem Gerät. Im Falle von Verlust oder Diebstahl der Hardware besteht bei klassischen Active Sync Anbindungen die Gefahr des Auslesens von Active Directory Benutzername und Passwort. Dies eröffnet potenziellen Angreifern Tür und Tor zum kompletten Unternehmensnetzwerk. Für die Authentisierung bietet sich also neben Benutzername/ Passwort (unsicher) und Softzertifikat (kostenintensiv) ein Secure Active Sync Gateway an. Damit lässt sich nicht nur verhindern, dass sich Nutzer mit unsicheren oder unkontrollierten Devices ans System anbinden, sondern gleichzeitig eine konsistente und granulare Content Kontrolle für den Zugriff mobiler Nutzer durchsetzen. Für die Benutzer Authentisierung werden nur starke Merkmale akzeptiert. Hierfür kann das Domain Passwort oder Pin-Code / Passwort aus der OTP Lösung an das jeweilige Device respektive die Device ID gekoppelt werden. Diese ist ein eindeutiges in jedem Device durch den Hersteller hinterlegtes Merkmal. Durch die eindeutige User-Device-Verknüpfung ist auch im Fall eines Diebstahls der Zugangscodes ein missbräuchlicher Zugriff unmöglich. Damit nicht bei jedem Zugriff ein neues OTP eingegeben werden muss, kann zusätzlich ein Gültigkeitszeitfenster definiert werden. Der Administrator hat somit jederzeit aktive Kontrolle über seine abgesicherten Systeme und den Content.

iOS Backup

Durch iCloud ist es nun möglich, Backups in der Cloud von Apple zu hinterlegen. Allerdings handelt es sich dabei nur um eine 1zu1 Verbindung zwischen dem Nutzer und Apple. Das Bedeutet: Administratoren haben keinen Einfluss darauf, dass, wann und auch wo gesichert wird, denn der Ort ist unabänderlich festgelegt. Was allerdings konfiguriert werden kann, ist eine zwingende Verschlüsselung und ob Dokumente und Fotos eingeschlossen werden dürfen. Gerade Letzteres ist wichtig, um einen unkontrollierten Datenabfluss von Firmendokumenten zu verhindern.



Netzwerkanbindung

Meist ist es das Management der Geräte, das im Vordergrund der Überlegungen steht. Viel früher stellt sich aber die Frage nach einer hochperformanten und tragfähigen Anbindung der Geräte. Es gilt zum einen, das Vielfache an mobilen Usern zu bewältigen, hochwertige Performance für bandbreitenhungrige Business-Applikationen und v.a. auch Ausfallsicherheit gerade innerhalb industrieller Einsatzszenarien zu gewährleisten. Mit WLAN als primären Netzzugang bei iPhone® und iPad® gilt der Konzeption der drahtlosen Infrastruktur ein besonderes Augenmerk. CIOs und IT Administratoren sollten dabei einige Aspekte beachten, um langfristig optimale Bedingungen zu schaffen.

Grenzerfahrung 3G

Einige iPad® Modelle verfügen neben der WLAN Schnittstelle über eine 3G Verbindung, um Daten abrufen und versenden zu können. Das „Überall-Internet" stößt jedoch dort auf seine Grenzen, wo die UMTS Abdeckung schlecht bis nicht vorhanden ist. So zum Beispiel in Gebäuden mit verspiegelten/mit Metall bedampften Glasfronten, in Kellergeschossen u.ä.. Große Programm-Downloads via „AppStore" werden bereits durch das iOS unterbunden, wenn keine breitbandige WLAN Verbindung zur Verfügung steht.

Eine weitere Limitierung in Bezug auf Geschwindigkeit bei 3G Verbindungen stellt VPN dar. Aus sicherheitstechnischer Sicht setzen viele Firmen auf die Verwendung von VPN Zugängen für externe Mitarbeiter. iPads®, die per UMTS ins Firmennetz wollen, stellen einen solchen „externen Client" dar, egal wo er sich gerade befindet. Anders ausgedrückt: Die Verwendung des UMTS Netzes zur Kommunikation mit Firmenservern macht aus performance-technischer Sicht nur dann Sinn, wenn keine WLAN Verbindung zur Verfügung steht.

Site Survey. Planungssicherheit statt Kostenfalle

In den meisten Fällen ist also die einzige Netzwerkschnittstelle von Mobilgeräten ein WLAN-Adapter - eine neue Herausforderung für das bestehende Netzwerk. Da jeder Benutzer heute schon im Schnitt 2-3 WLAN-fähige Devices hat, wird die Anzahl der im WLAN aktiven Geräte pro Quadratmeter in den nächsten Jahren drastisch zunehmen. Grundvoraussetzung für eine lückenlose WLAN-Abdeckung ist die gewissenhafte Ausleuchtung des Firmengeländes.

Ein sog. Predictive Site Survey liefert ein erstes Mengengerüst, das zur Budgetierung des Projekts und als Grundstock für weitere Schritte dient. Anhand der Gebäudepläne wird die theoretisch mögliche Ausleuchtung und Anzahl der benötigten Access Points simuliert.

Eine verlässliche Aussage über die zu erwartende Leistungsfähigkeit des zukünftigen WLANs liefert nur eine aktive Messung vor Ort, zweckmäßigerweise mit dem für das Projekt vorgesehenem Access Point Typ. Als Ergebnis erhält man ein Dokument, welches die exakte Anzahl der benötigten Geräte und die Installationspunkte definiert – im Idealfall mit einer Abdeckungsgarantie, um nicht von unerwarteten Kosten während des laufenden Projekts überrascht zu werden.

Diese Messung identifiziert auch „versteckte“ Hindernisse, die dämpfend auf WLAN Signale wirken, wie z.B. Wasserleitungen, Kabelschächte oder Metallkonstruktionen in Trockenbauwänden. Je nach Einsatzszenario ist eine gewisse Mindestsignalstärke sicherzustellen. In Bereichen mit großer Benutzerdichte sollte mindestens eine Signalstärke von -72dBm erreicht werden. Für den Einsatz von Voice over WLAN Telefonen müssen es sogar -67 dBm bis -65 dBm sein. Selbst wenn aktuell (noch) keine 5 GHz-fähigen Clients zum Einsatz kommen, sollte der Survey mit Blick auf Investitionssicherheit von Anfang an auf beide Frequenzbänder – 2,4 und 5 GHz - ausgelegt sein.

Site Survey Best Practice:

DOs	DON'Ts
• Messung für 5GHz und 2.4GHz • Messungen wärend der normalen Betriebszeiten • Türen geschlossen halten • Messung genau dort, wo der Benutzer später arbeitet (z.B. Schreibtisch) • „Durchdringung“ von Decken/Böden beachten • Post-Survey nach der Installation durchführen	• Benutzen Sie kein Predictive Survey für die Umsetzung des Projekts • Nicht nur für 802.11 b/g/n messen • Falls Unterstützung für 802.11 a/b/g gewünscht ist, nicht mit 802.11 n Adapter messen • Maximale Länge für Ethernetsegmente nicht vergessen

Funkzellenplanung

Für wirklich reibungslosen Betrieb ist jedoch auch die optimale Frequenzverteilung Pflicht, genauso wie eine gründliche Planung der Funkzellen, also des Bereichs, der von einem Access Point abgedeckt wird.

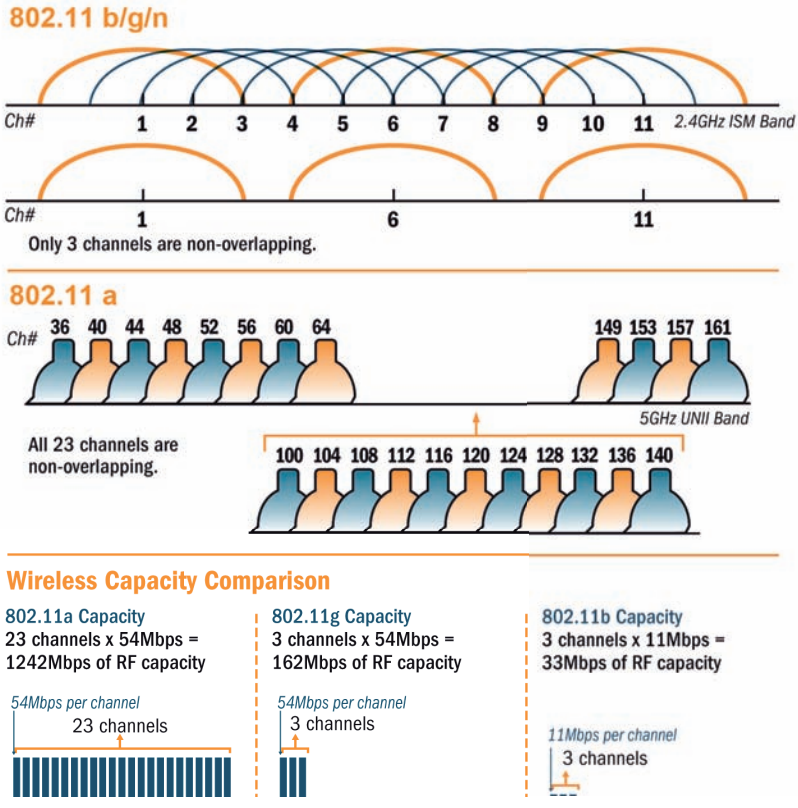
Pro Funkzelle geben die meisten Hersteller eine maximale Anzahl von 64 Benutzern an. In der Praxis macht es jedoch nur selten Sinn, mehr als 40 Geräte gleichzeitig in einer Funkzelle zu betreiben - in einem Großraumbüro, der Kantine oder den Besprechungsräumen ist diese Zahl schnell erreicht. Soll Telefonie über WLAN erfolgen, sollte die Anzahl der Telefone pro Funkzelle sogar unter 15 liegen. Die Folge ist, dass bei der WLAN-Planung nicht nur die abzudeckende Fläche, sondern vor allem die Benutzerdichte und Art der über WLAN benötigten Dienste (Internet, Mail, Voice, Videostreaming) zum bestimmenden Faktor wird.

Da besonders im 2,4 GHz-Bereich die Anzahl der störungsfrei nebeneinander arbeitenden Funkzellen sehr eingeschränkt ist (2,4 GHz: 3 unabhängige Kanäle, 5 GHz: 16 unabhängige Kanäle), muss immer darauf geachtet werden, dass zwei benachbarte Funkzellen nicht den selben Kanal verwenden. An jeder Stelle, an der sich zwei Funkzellen mit dem gleichen Kanal überlappen, käme es zu einem massiven Einbruch der Verbindungsqualität und -geschwindigkeit durch gegenseitige Störung (Crosstalk). Solche Bereiche sind daher dringend zu vermeiden. In einem reinen 2,4 GHz-Netzwerk sind derartige Überlappungen auch mit höchsten Anstrengungen kaum zu vermeiden.

5 GHz ist die Zukunft - 5x mehr Bandbreite als im 2,4 GHz Band

Das iPad® macht es vor, viele ziehen jetzt schon nach: Mobile Devices sind auf den 5 GHz-Bereich angewiesen, damit eine vernünftige Netzwerkplanung möglich wird. Wenngleich die Kanalplanung im 5 GHz-Bereich deutlich unkritischer ist, sollte diese dennoch gründlich durchdacht werden. Der neue Standard 802.11n funktioniert in beiden Frequenzbereichen - 2,4 und 5 GHz. Die Endgeräte, die nach diesem Standard zertifiziert sind, können jedoch nicht zwingend im 5 GHz-Bereich funken.

Die hohe theoretische Datenrate von 300 Mbit/s wird u.a. durch Channel Bonding erreicht: Dabei werden zwei benachbarte, unabhängige WLAN-Kanäle (z.B. Kanal 1 und Kanal 6) gemeinsam für eine Funkzelle verwendet. Das bedeutet, dass sich die Anzahl der freien Kanäle noch weiter verringert: Im 2,4 GHz-Bereich bleiben gerade einmal 2 Kanäle übrig, davon einer mit 300 Mbit/s und einer mit 150 Mbit/s. Im 5 GHz-Bereich wiederum verbleiben 8 Kanäle mit 300 Mbit/s. Die gesamte theoretische Bandbreite des 2,4GHz-Bandes beträgt also gerade einmal 450 Mbit/s, verglichen mit den 2.400 Mbit/s, die theoretisch im 5 GHz-Band möglich sind.



Die Betrachtung der gesamten theoretischen Bandbreite ist im Übrigen nicht nur für große Dateitransfers interessant - dadurch, dass innerhalb einer Funkzelle alle Clients sich das Medium teilen, kann immer nur ein Device „sprechen" und die anderen müssen abwarten. Je schneller also jede einzelne Datenübertragung beendet ist, desto kürzer sind die Wartezeiten der anderen Clients. Insgesamt sorgt das für ein spürbar leistungsfähigeres Netzwerk und ein reibungsloses Zusammenspiel aller Komponenten.

Bei der bereits angesprochenen zu erwartenden explosionsartigen Zunahme von Devices und den angesprochenen Limitierungen pro Funkzelle, scheint zunächst der einzige Weg darin zu bestehen, die Sendeleistung der WLAN Access Points zu reduzieren und auf diese Art kleinere Funkzellen zu realisieren. Der Vorteil liegt auf der Hand: Es gibt insgesamt weniger Crosstalk zwischen den benachbarten Funkzellen und die Dichte der Access Points kann gesteigert werden. Allerdings wird dieser Vorteil erkauft durch eine deutliche Zunahme des Planungs-, Geräte- und Installationsaufwands.

Je kleiner die Funkzellen, desto größer ist der Anteil an Grenzflächen zwischen den einzelnen Funkzellen, was die Kanalplanung weiter erschwert: Konnte vorher ein Großraumbüro mit 2 Access Points versorgt werden, sind nun mitunter 4-6 nötig, die alle auf einer eigenen Frequenz betrieben werden müssen. Eine flächendeckende 2,4 GHz-Abdeckung ist mit diesem Konzept nur mit deutlichen Kompromissen in der Leistungsfähigkeit des Netzwerks zu realisieren. Die Verdoppelung bis Verdreifachung des Geräteaufwands schlägt sich zudem 1:1 im Budget nieder, zum Einen was Anschaffungskosten für WLAN-Hardware angeht, zum Anderen hinsichtlich Verkabelung, Switchports, Installation/ Konfiguration und Stromverbrauch (TCO)

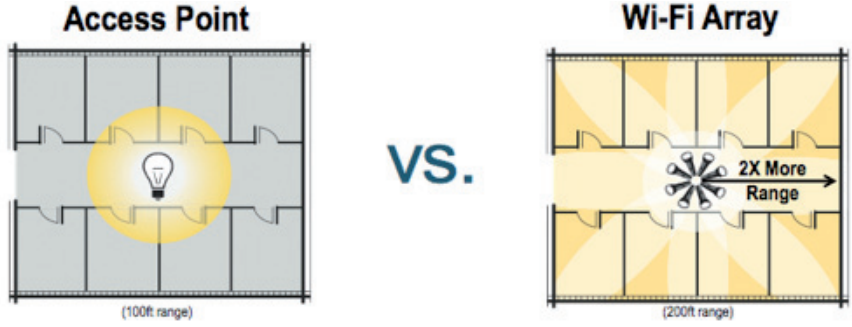
Beispielrechnung (zur Abdeckung Vorlesungssaal Seite 16):

Traditionelles WiFi		**WiFi Arrays**
17	Geräte	3
1.500	Verkabelung	300m
17	Switchports	3
17 Stunden	Installationsaufwand	3 Stunden
4100 kWh	Stromverbrauch p.a.	1700 kWh
?	Lebensdauer	72.000 Std. (8 Jahre)

Die Ursache für diesen Zielkonflikt liegt unter anderem in der Tatsache begründet, dass die meisten Access Points rundstrahlende oder omnidirektionale Antennen verwenden. Es wird also ähnlich einer Glühbirne die Funkleistung in alle Richtungen gleichmäßig verteilt.

Die Alternative: WiFi-Array

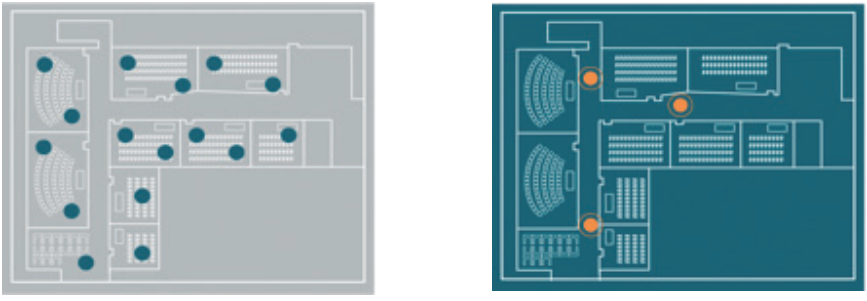
Teilweise kann man die oben geschilderten Konflikte umgehen, indem man auf ein anderes WLAN-Konzept setzt. Im Gegensatz zu traditionellen Access Points verwendet ein sogenanntes WiFi-Array Sektorantennen, wie sie z.B. auch im Mobilfunkbereich verwendet werden. Durch die Unterteilung des auszuleuchtenden Gebiets in klar definierte „Tortenstücke" können wesentlich einfacher mehrere Funkzellen auf eine bestimmte Fläche ausgebracht werden.



Quelle: Xirrus Inc. High Performance WiFi

Da die Sendeleistung auf einen bestimmten Bereich konzentriert wird, anstatt sich kugelförmig im Raum zu verteilen, erhöht sich die Reichweite der Funkzelle in der Praxis oft auf das Doppelte, während gleichzeitig die oben beschriebenen Probleme bzgl. Crosstalk deutlich verringert werden. Damit einher geht eine Verringerung der Gerätedichte anstelle einer Erhöhung.

Beispiel der Access Point Verteilung für ein Vorlesungsgebäude
Traditionelle Access Points vs. WiFi Arrays



Quelle: Xirrus Inc. High Performance WiFi

Sicheres WLAN - heute und in Zukunft

WLAN kann immer nur so sicher sein wie der verwendete Verschlüsselungsalgorithmus und -schlüssel. WPA2-Personal stellt hier das Minimum dar, besser noch WPA2-Enterprise. Wer auf WPA2-Personal setzt, sollte ein Passwort mit mindestens 20 Zeichen, bestehend aus großen und kleinen Buchstaben, Sonderzeichen und Zahlen verwenden. Idealerweise wird dieses Passwort alle 3-4 Wochen geändert. Der damit verbundene Administrationsaufwand lässt sich durch die Verwendung eines entsprechenden Management Tools relativ gering halten. Derzeit am sichersten ist der Einsatz von WPA2-Enterprise: Hier wird zwar der selbe Verschlüsselungsalgorithmus wie bei WPA2-Personal verwendet, jedoch wird jedem WLAN Client ein individueller, temporärer Verschlüsselungskey durch einen RADIUS Server zugewiesen.

Übrigens: Wer die volle Datenrate des 802.11n Standards nutzen möchte, muss bei der Verschlüsselung auf AES setzen. WEP und WPA-TKIP verschlüsselter Datenverkehr wird automatisch auf 54Mbit/s limitiert!

Welche Verschlüsselungsstandards in Zukunft zum Einsatz kommen ist derzeit noch nicht absehbar. Idealerweise setzt man heute schon auf WLAN Hardware, bei der zukünftige Sicherheitsstandards nachträglich eingebunden werden können - Stichwort: Investitionssicherheit. Ein Wi-Fi Array setzt hier beispielsweise auf den Einsatz von FPGAs. Diese integrierten Schaltkreise können entsprechend programmiert werden und sind in der Lage Daten nahezu in Echtzeit zu verarbeiten.

Intelligente Verteilung der WLAN Clients erhöht die Gesamtperformance

Je mehr Clients mit einem Access Point oder einer Funkzelle verbunden sind, desto träger wird das Gesamtsystem. Da immer nur ein einzelner Client seine Daten in der gemeinsam genutzten Funkzelle senden kann, erhöht sich die Wartezeit der übrigen Clients proportional mit der Zunahme der Sendestationen. Zudem produziert jeder angemeldete WLAN Client Last auf dem Access Point, was zudem schnell zu Problemen führen kann. Beides zusammen genommen äußert sich in schlechter Performance und damit in einem „negativen" WLAN-Erlebnis.

Intelligente WLAN Systeme bieten mit „Client Load Balancing" auf der Wireless Seite einen adäquaten Lösungsansatz. Befindet sich beispielsweise ein WLAN Client im Abdeckungsbereich zweier Access Points, wird anhand der bereits angemeldeten WLAN Teilnehmer auf dem jeweiligen Access Point entschieden, welcher Access Point den neu hinzukommenden Client annehmen soll.

Vereinfacht gesagt: Der Access Point, der weniger zu tun hat, bekommt den neuen Client zugewiesen. Damit dieser Mechanismus funktioniert, müssen die Access Points untereinander diverse Informationen austauschen. Dies geschieht entweder über einen Controller als zentrale Instanz, die im Netzwerkbackbone angeordnet ist oder über intelligente verteilte WLAN Systeme, die direkt an der LAN/WLAN Schnittstelle Entscheidungen treffen. Bei Systemen, die auf eine zentrale Instanz bei der Client Verwaltung und Steuerung setzen, sollte die Zunahme der Netzwerklast durch den laufenden Datenaustausch zwischen Access Point und Controller nicht außer Acht gelassen werden.

Management

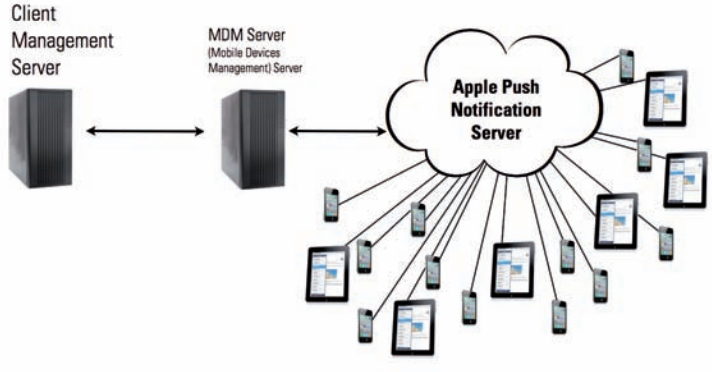
Bis zur neuesten Betriebssystemversion iOS war eine Konfiguration nur über Skripte, die per E-Mail übertragen wurden, oder das kostenfreie iPhone® Konfigurationstool möglich. Letzteres setzte allerdings die physische Verbindung der Endgeräte via Kabel voraus, um Konfigurationen zu übertragen. Für das Management mehrerer Geräte eine äußerst unkomfortable Vorgehensweise. Der User wurde deshalb gerne auf das sog. „Self Service Konzept" verwiesen oder anders gesagt sich selbst überlassen - mit entsprechenden Auswirkung auf Sicherheit und andere Problemstellen. Mit dem Erscheinen von iOS stellt Apple eine Schnittstelle zur Verfügung, die als Beginn von professionellem iOS Device Management gesehen werden darf.

Architektur

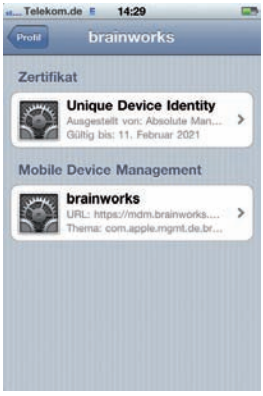
Clientmanagement von iOS Geräten unterscheidet sich von „normalem" Clientmanagement. Am auffälligsten ist ein zentraler Punkt: Apple erlaubt den Herstellern von Managementlösungen keinen eigenen Client auf den Geräten, sondern gibt eine Schnittstelle frei, um externe/eigene Mobile Device Management Server anzubinden. Der Anbindungsprozess an zentrale Clientmanagementlösungen erfolgt also nicht - wie vielleicht gewohnt - über einen eigenen Agent/Client. Ebenso gibt es keine direkte Kommunikation zwischen Mobile Device Management Server und Client. Als Mittler fungiert der Apple Push Notification Server. Dieser triggert die Devices an (Push), teilt mit, dass etwas Neues für sie da ist und sie sich bei ihrem zugewiesenen Mobile Device Management Server (MDM) melden sollen. Um den Service in Anspruch nehmen zu können, ist ein Zertifikat nötig, das eine Apple ID voraussetzt. Eine genauere Beschreibung finden Sie unter: www.apple.com/iphone/business/integration/mdm/

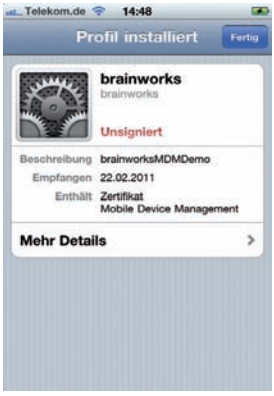
Dieses Zertifikat deckt aber „nur" die Standardmöglichkeiten ab. Wenn firmeneigene App-Stores oder andere ergänzende Funktionen genutzt werden sollen, kann es sein, dass Sie ein Zertifikat benötigen, welches Sie nur im Apple Enterprise Developer Account erhalten.

(http://developer.apple. com/programs/ios/enterprise/).



Dieses Zertifikat muss in einem Profil an das iOS Device übertragen und installiert werden. Konkret gesprochen erhält das Gerät eine E-Mail, einen E-Mail Anhang oder eine SMS mit einem Link auf eine sog. Enrollment Page, auf der das Konfigurationsprofil heruntergeladen und installiert werden kann. Die Enrollment Page ist eine kleine Website, die mit Zugangsdaten (Benutzername und Passwort) geschützt werden kann und meist selbständig von den MDM Lösungen erstellt wird. Die Installation des Anbindungsprofils geschieht „Silent". Folgende Konfigurationsprofile, z.B. VPN Zugänge, können in den meisten MDM Lösungen entweder dem User in einem Katalog angeboten oder auch direkt und Silent installiert werden. Zu sehen sind die installierten Profile unter:
Einstellungen>Allgemein>Profile.





Apple will „empowered" User und sichert deren Adminrechte mit entsprechenden technischen Restriktionen: So kann das initiale Anbindungsprofil an die eigene Clientmanagementsoftware bzw. an den eigenen MDM Server nicht mit Passwort gegen ein Löschen geschützt werden - mit all seinen Konsequenzen. Wird diese gelöscht, gehen auch vorhandene Konfigurationsprofile, z.B. bezüglich WLAN oder VPN verloren. Das Löschen des Profils, was einem Entziehen aus dem Managementsystem gleich kommt, kann vom Administrator mit dem Löschen von firmenrelevanten Apps verbunden werden. Dies stellt eine erhebliche Verbesserung bei der Absicherung firmenrelevanter Daten und Zugänge dar.

Nach dem Anbinden der Devices ist das Verhalten der iOS Devices vergleichbar mit anderen mobilen oder stationären Clients und man kann die verschiedenen Schritte eines Clientmanagements beginnen.

1. Inventarisierung: Administratoren erhalten mittlerweile knapp 70 verschiedene Informationen bezüglich Hard- und Software. Besonders nützlich sind z.B. Garantieinformationen, da gerade hier manchmal Diskrepanzen auftauchen. Diese Abfragemöglichkeiten eignen sich neben der reinen Information auch zur Erstellung dynamischer Gruppen. Beispielsweise können mehrere tausend iPads® sortiert und diesen Gruppen Administratoren oder Aufgaben/Rechte von Administratoren zugewiesen werden.

Einschränkung: Es ist nicht möglich, die Verwendung von Applikationen abzufragen.

2. Konfigurationen: Hersteller von Softwarelösungen zu MDM bieten für iOS Devices die Möglichkeit, verschiedene Konfigurationsprofile von zentraler Stelle aus per Push an die Devices zu verteilen. Wichtig: Wie schon im Abschnitt Architektur beschrieben, werde keine Konfigurationen über den Apple Push Notification Service verteilt. Dieser kontaktiert nur die iOS Devices und fordert sie auf, sich bei Ihrem MDM Server zu melden, da etwas Neues für sie vorhanden ist. Gerade im Hinblick auf Zugangsdaten, für z.B. E-Mail-Konten oder VPN Zugänge ist dies ein wichtiger Punkt. Bei manchen Produkten erfolgt die Erstellung der Konfigurationen innerhalb der Lösung über eine integrierte Benutzeroberfläche. Andere verwenden das Apple iPhone Configuration Utility. Vorteil hier: Man kann jederzeit alle aktuellen Möglichkeiten und Entwicklungen nutzen, die Apple bereitstellt. Proprietäre Lösungen müssen diese Neuerungen i.d.R. mit Zeitverzug nachentwickeln.

Tipp: Es ist möglich, verschiedene Konfigurationen, z.B. WLAN und VPN, in ein Profil aufzunehmen. Dabei ist abzuwägen, ob es günstiger ist, den Weg eines Profils mit allen Einstellungen zu wählen oder z.B. für verschiedene Zugänge separate Konfigurationen zu erstellen und einzeln zu übertragen.

Die erstellten Dateien sind im XML Format und können mittels Passwort gegen eine Deinstallation geschützt werden - im Gegensatz zum initialen Profil, welches die Anbindung des Devices an das MDM System sicherstellt.

Die Installation der generierten Konfigurationen (XML Dateien) geschieht entweder direkt und „Silent". In die neueste Generation von MDM Lösungen können diese Konfigurationen dem Benutzer auch in einem firmeneigenen AppStore zur Installation angeboten werden. Manche MDM Softwarehersteller unterstützen die Nutzung von Variablen, was zu einer signifikanten Vereinfachung umfangreicher Verteilprozesse führt. Sollen z.B. an 500 iOS Devices E-Mail Konfigurationen verteilt werden, müssen nur einmal entsprechende Variablen statt 500 Mal Benutzername und Passwort hinterlegt werden. Gerade Unternehmen mit einer größeren Anzahl von iOS Devices sollten auf diese Möglichkeit achten - idealerweise mit einer unbegrenzten Anzahl an Funktionsvariablen.

Möglichkeiten der Konfiguration:

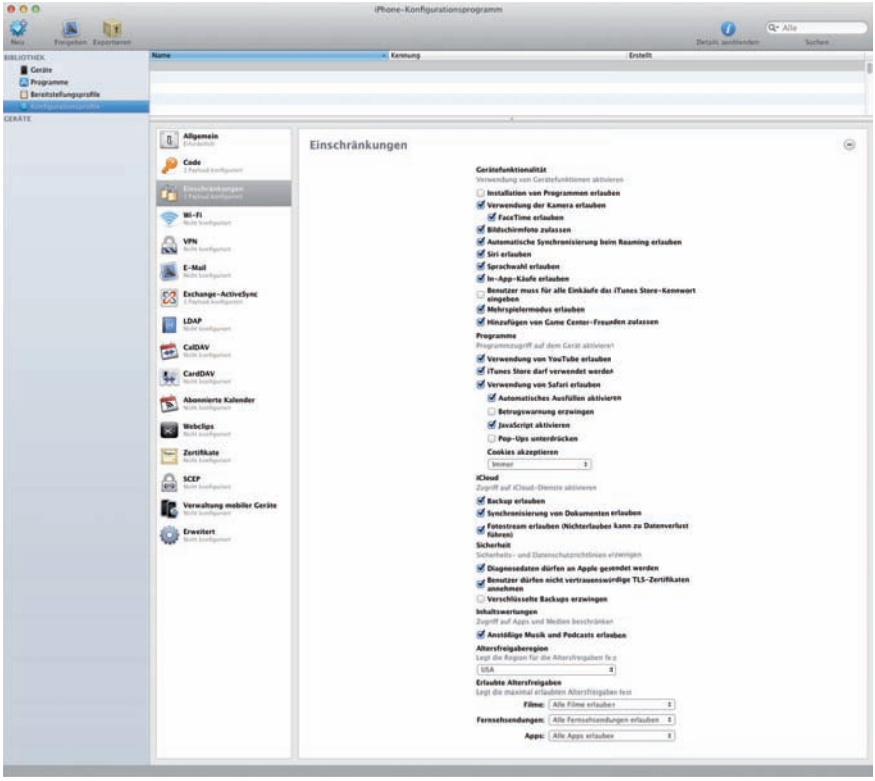
Accounts:
- Exchange ActiveSync
- IMAP/POP-E-Mail
- VPN
- Wi-Fi
- LDAP
- CalDAV
- CardDAV
- Abonnierte Kalender

Richtlinien:
- Code anfordern
- Einfachen Wert zulassen
- Alphanumerischen Wert anfordern
- Codelänge
- Anzahl komplexer Zeichen
- Maximale Geltungsdauer des Codes
- Zeit bis zur automatischen Sperrung
- Anzahl eindeutiger Codes vor der Wiederverwendung
- Frist für Gerätesperre
- Anzahl fehlgeschlagener Versuche vor dem Löschen
- Entfernen des Konfigurationsprofils durch den Benutzer steuern

Einschränkungen:
- App Installation
- Kamera
- Bildschirmfoto
- Automatische Synchronisierung von E-Mail Accounts beim Roaming
- Sprachwahl bei Sperrung
- In-App-Käufe
- Verschlüsselte iTunes Sicherungen anfordern
- Musik und Podcasts in iTunes mit anstößigen Inhalten
- Bewertungen zulässiger Inhalte für Filme, Fernsehsendungen, Apps
- Safari Sicherheitseinstellungen
- YouTube
- iTunes Store
- App Store
- Safari

Weitere Einstellungen:
- Zertifikate und Identitäten
- Weblinks
- APN-Einstellungen

Quelle: Apple, Stand 03/2011



App/Softwareverteilung

Wie einleitend schon beschrieben, unterscheidet sich die Softwareverteilung bei iOS Geräten etwas von anderen Systemen. Die meisten MDM Lösungen bieten Unternehmen die Möglichkeit, Ihren eigenen AppStore zu generieren und dem User neben (selbstentwickelten) In-House Apps auch Apps aus dem Apple AppStore anzubieten. Idealerweise direkt auf dem Device ohne Umweg über eine verlinkte Website. Dieser firmeneigene AppStore hat den großen Vorteil, dass dieser in der Firmeneigenen CI gestaltet werden kann und neben Applikationen auch Benutzerkonfigurationen zur Auswahl anbietet.

Mit iOS5 ist neben dem reinen „Anbieten" auch eine „Fast-Silent" Installation möglich bei der der Nutzer der Installation nur noch zustimmen muss. Bei Apps aus dem Apple AppStore ist weiterhin eine Apple ID nötig.

Bei der Software und Applikationsverteilung sind einige Einschränkungen zu beachten.

Die auffälligsten Punkte sind:

• App Verteilung von Apps aus dem Apple AppStore
Für Apps aus dem AppStore bestehen derzeit zwei Möglichkeiten. Erstens kann die App dem Nutzer angeboten werden, er wird dann in den AppStore weitergeleitet und installiert sich die App nach der Authentifizierung (Apple ID). Die zweite Möglichkeit ist eine „Fast-Push" Installation. Das bedeutet: Der Administrator weist dem Nutzer eine App zu und dieser wird gefragt, ob der Server die Applikation installieren darf. Im Anschluss folgt die Authentifizierung am Apple AppStore (Apple ID). Wichtig dabei ist, dass von dieser Apple ID dann die Kosten für kostenpflichtige Apps abgezogen werden.

Tipp: Für eine Verteilung einer größeren Anzahl eines App Store Apps lohnt es sich, die gewünschte App direkt über den Entwickler der Applikation zu beziehen und diese dann zentral auszurollen. Apple hat begonnen, ein sogenanntes Voucher Purchase Programm zu entwickeln, welches im Moment im Bildungsbereich in den USA schon zur Verfügung steht. Dieses macht einen zentralen Einkauf für Unternehmen möglich, die die Apps praktisch „vorbezahlen". Es ist aber immer noch ein iTunes Account notwendig, um diese Applikation dann herunterzuladen.

Das Verhindern der Installation unerwünschter einzelner Applikationen aus dem AppStore (Black- oder Whitelisting) ist nicht vorgesehen. Es besteht nur die Möglichkeit einer generellen Einschränkung oder Erlaubnis Apps zu installieren. Hilfe bieten hier manche iOS Management Softwarehersteller. Die Lösungen erlauben z.T. eine sog. „Überwachung", d.h. man erstellt eine Liste von nicht erwünschten Applikationen. Sobald der User eine dieser Apps installiert, erkennt die Managementsoftware dies und der Administrator kann entsprechende Schritte einleiten, wie z.B. Löschen/Deaktivieren des Firmen E-Mail-Accounts etc.

• Es können keine Updates für Programme aus dem Apple AppStore verteilt werden
Die Updateverteilung für Apps aus dem AppStore erfolgt über den AppStore und wird über diesen angestoßen, wobei der Benutzer zustimmen muss. Bitte beachten Sie, dass auch hierfür ein iTunes Account notwendig ist. Updates von selbstentwickelten Apps können zentral zur Verfügung gestellt werden.

• Es können keine neuen Betriebssysteme oder Updates zentral verteilt werden.
iOS Updates werden entweder über iTunes, mit Kabel, oder kabellos auf das Device übertragen. Es ist jedoch nicht möglich als Administrator Einfluss darauf zu nehmen z.B. in Form von einem Anstoßen oder Verbieten. Dies bleibt dem Nutzer überlassen.

Weitere Funktionen von MDM Server-Produkten

Remote Zugriff: Neben den oben beschriebenen Funktionen bieten die meisten MDM Server Lösungen die Möglichkeit, iOS Devices aus der Ferne zu sperren (Remote Lock), zu löschen (Remote Wipe) bzw. in den Auslieferungszustand zurückzusetzen.

Jailbroken Devices: Mit der Betriebssystemversion 4.2.1 entzog Apple die Möglichkeit, sog. Jailbroken Devices zu identifizieren. Einige Hersteller traten mit Eigenentwicklungen die Flucht nach vorne an, die die „geknackten" Devices ausfindig machen. Gerade im Hinblick auf Compliance ist dies ein wichtiger Fortschritt, da diese Geräte offen für jegliche ungeprüfte Installationen sind. Somit haben Administratoren wieder die Möglichkeit jegliche unternehmensrelevanten Zugänge und Konfigurationen automatisiert zu entziehen und bei Bedarf wieder zuzuweisen.

Geolokation: Für manche Anwendungsfälle ist es interessant, den Standort/die Position von iOS Devices herauszufinden. Einige Hersteller verwenden hierfür die Apple-eigene Lokalisierungsfunktion aus Mobile Me, welche einen entsprechenden Account voraussetzt. Die jüngste Generation von MDM Produkten benötigt diesen Zugang nicht mehr und Administratoren können sich die Position einfach in Google Maps oder Bing anzeigen lassen. Spätestens hier tritt der Betriebsrat auf den Plan und kann beruhigt werden: Die Anwender unterliegen nicht willkürlicher Kontrolle - die Funktion kann nur mit einem Passwort genutzt werden, welches der User selbst auf seinem Device generiert hat.

Benachrichtigungen: Damit Administratoren mit den Benutzern direkt in Kontakt treten können, lassen die Hersteller von MDM Lösungen einfach Nachrichten versenden. Hier gibt es zwei Wege: Ein Teil der Hersteller wählte den technisch trivialen Weg, ein SMS Gateway anzubinden. Auf den ersten Blick ein guter Ansatz. Leider können iPads® aber keine SMS Nachrichten empfangen. Zudem ist dies bei einer entsprechenden Anzahl ein durchaus ernstzunehmender Kostenträger. Der andere Teil nutzt wieder den sog. firmeneigenen Appstore, an den Nachrichten kostenfrei und direkt per Push versendet werden. Die Nachricht erscheint vom „Alarmverhalten" wie eine SMS und ist in der Zeichenzahl nicht limitiert.

Sichere Dokumentenverteilung: Eine interessante Neuerung ist bei vielen MDM-Lösungen der neuesten Generation ein zentraler Dokumenten-Mediaserver. Dieser ist ein zentraler und abgesicherter Verteilungspunkt für Medien, Dokumente und Inhalte. Administratoren können z.B. Dokumente verteilen, mit einem Passwort sichern oder gegen eine Vervielfältigung schützen.

Zeitlich befristete Nutzung: Es setzt sich gerade im Businessumfeld eine neue Funktion durch, die es Administratoren erlaubt, Konfigurationen, Apps, und Dokumente mit einem Zeitfenster zu versehen. Damit ist es ein Leichtes zum Beispiel E-Mail-Zugänge, Preislisten, CRM Systeme nur zu Geschäftszeiten zu ermöglichen. Dies ist ein erheblicher Fortschritt hinsichtlich der Absicherung von Daten und Systemen und erleichtert eine Trennung von privater und geschäftlicher Nutzung signifikant.

Virtualisierungsansatz

Mit der Idee der Virtualisierung auf iOS Devices treten manche Unternehmen den entstehenden Problemen durch die Verquickung privater und geschäftlicher Verwendung der iOS Devices entgegen. Denn seit einiger Zeit ist es möglich, komplett virtualisierte Windowsarbeitsplätze inklusive Applikationen auf iOS Devices abzubilden.

Gerade in schon bestehenden Virtualisierungsumgebungen ist eine Anbindung extrem einfach. Citrix bietet z.B. das benötigte App - ein sog. Receiver - kostenfrei an. Und auch der zweite große Virtualisierer VMware hat seit März 2011 eine entsprechende Lösung im Programm.

In der Praxis bedeutet das: Der Anwender lädt sich die App kostenfrei aus dem App Store herunter, gibt Anmeldedaten und Serverdaten an, startet die App und erhält einen kompletten Zugriff auf seine z.B. virtualisierte Windows 7 Umgebung inklusive aller Anwendungen, Desktops und Dokumente etc.

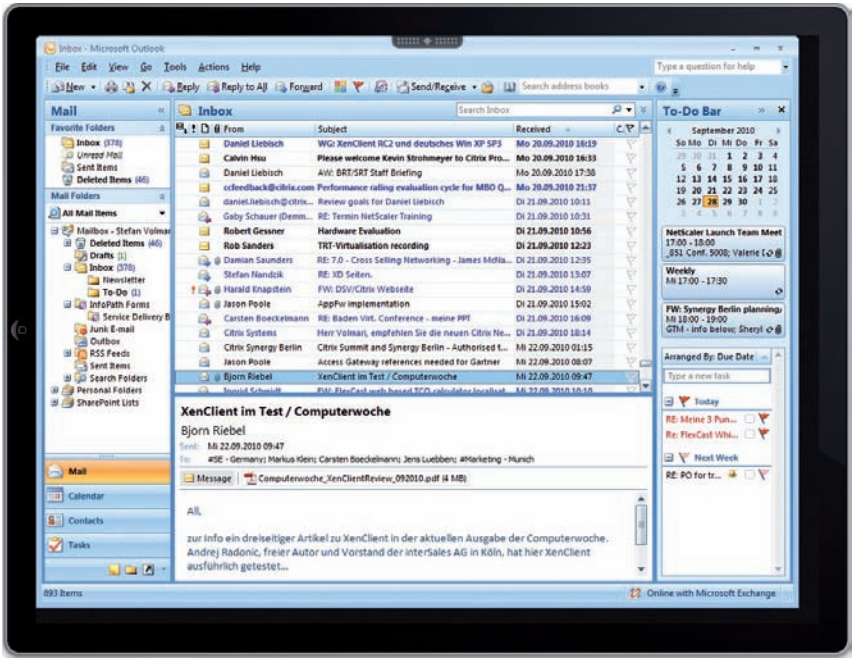
http://www.citrix.com/v/#videos/2781

Interessant ist, dass gerade rechenintensive Anwendungen, komplexe Datenbank- und professionelle 3D-Anwendungen auf dem Device geöffnet werden können, denn die Prozesse laufen schließlich nicht auf dem iOS Gerät ab. Der Flaschenhals ist somit nicht mehr die Rechenperformance der Endgeräte, sondern verschiebt sich auf den Datentransfer zwischen Serverfarm und iOS Device.

Große Vorteile sind:

- Eine klare Abgrenzung von privatem und geschäftlichem Bereich auf dem iPad®
- Datensicherheit bei Verlust
- Vermeidung von Inkompatibilitätsproblemen, z.B. MS Office
- Einfache Softwareverteilung und -kontrolle
- Flash Integration
- Kompletter Java Support

Es mag für den Einen oder Anderen eine schmerzvolle Vorstellung und Erfahrung sein, auf seinem iOS Gerät, Windows 7 zu starten und mit Outlook zu arbeiten. Aber abseits von ideologischen Ansichten kann dies eine optimale Ergänzung und Einbindung von iOS Devices darstellen und einige konzeptionelle Probleme lösen.



Zu bedenken ist jedoch: Für Unternehmen, die den Weg der Anwendungsvirtualisierung bisher nicht eingeschlagen haben, stellt eine Umstellung einen grundsätzlichen Strategiewechsel zu der bisherigen IT Architektur dar. Und der ist auch nicht von heute auf morgen zu stemmen.

Vielleicht erleichtert diese Möglichkeit aber auch für das ein oder andere Unternehmen den Einstieg, sich mit dem Thema Anwendungs-virtualisierung und Umsetzung im eigenen Unternehmen zu befassen.

Quick Views - für den schnellen Überblick

Ob als Schnelleinstieg in das Thema, als Checkliste oder Leitfaden bei Ihrem iOS Projekt, die Quick Views führen Sie ohne Umwege zu den zentralen Aussagen. Die thematisch abgegrenzten Kurzprofile sollen Ihnen helfen, schon in der Planungsphase gefährliche Stolperfallen zu erkennen und zielführende Konzepte auf den Punkt zu bringen.

Welche Besonderheiten gibt es zu beachten, was sollte man unbedingt vermeiden, wie geht man am besten vor - auf den folgenden Seiten bekommen Sie ein kompaktes Infopaket zu diesen Themen:

1. WLAN Planung
2. Mobile Security
3. MDM Planung

Quick View – WLAN Planung

Anders als bei kabelgebundenen Ethernet Installationen, wo sich die Anzahl der benötigten Switch-Ports einfach aus der Zahl der einzubindenden Clients ableiten lässt, ist bei der WLAN-Planung eine ganze Reihe von Determinanten zu berücksichtigen:

1. Welche Bereiche des Gebäudes müssen funktechnisch abgedeckt sein?
2. Wie ist die Beschaffenheit des Gebäudes (Ziegel, Stahlbeton oder Trockenbauweise)?
3. Welche Clients kommen zum Einsatz (Smartphones, Laptops oder Tablet-PCs)?
4. Wie stark steigt der Anteil mobiler Devices mit WLAN als primärer Netzzugang? -> Dominanz der WLAN Clients bei der Netzwerkplanung berücksichtigen
5. Wieviele 5 GHz-fähigen Devices sind bereits im Einsatz oder können zukünftig etabliert werden? -> Hochperformante Gerätelandschaft durch leistungsstarke IT Infrastruktur unterstützen
6. Wie wird sich die Benutzerverteilung voraussichtlich darstellen (Einzelbüros, Konferenzräume etc.)?
7. Welche Dienste (Web-Browsing, E-Mail, Datenbanken, Voice und/oder Video) werden über das WLAN angeboten, und welche Mindestbandbreite soll den einzelnen Clients zur Verfügung stehen?

DOs	DON'Ts
WPA/WPA2 in der „Enterprise Variante" (802.1x-Authentifizierung) verwenden Jeder Client erhält individuellen Session basierten Verschlüsselungskey	Keine WEP Verschlüsselung wählen -> kann binnen Sekunden mit Hilfe kostenloser Tools geknackt werden
802.1x Clientkonfiguration absichern Server-Zertifikat Validierung aktivieren	„SSID verstecken" ist relativ nutzlos -> kann mit WLAN Sniffer trotzdem ausgelesen werden -> erschwert den Verbindungsaufbau für manche WLAN Clients
WLAN IDS/IPS installieren Erkennen von Rogue APs und anderen Gefahren	MAC Adressfilter sind wirkungslos MAC Adressen lassen sich fälschen
SSIDs auf den Clients einschränken Windows bietet z.B Möglichkeiten, die auswählbaren SSIDs zu limitieren	
Physikalische Absicherung der WLAN Hardware durch abschließbare Gehäuse	

Quick View – Mobile Security

Der „mobile Flohzirkus" muss nicht nur in die IT, sondern auch in die Security Konzepte integriert werden. Alles andere ist nicht nur kosten- und zeitintensiv, sondern vor allem auch gefährlich. Gefragt sind ganzheitliche Lösungen, die

1. unerwünschte und/oder risikobehaftete Geräte „aussperren"
2. kontrollierten Zugriff auf Unternehmensressourcen gewährleisten
3. plattformunabhängig einsetzbar sind
4. flexible Konzepte für unterschiedliche Zugriffsoptionen bereitstellen
5. Benutzerfreundlichkeit und Sicherheitsbestreben in Einklang bringen

Bei der Planung und Umsetzung sind folgende Überlegungen zu berücksichtigen:

- Risikoverständnis schärfen:
  - Welche generischen Bedrohungen bestehen für die mobilen Endgeräte?
  - Welche plattformspezifischen Besonderheiten gilt es zu beachten, z.B. Administrationsrechte für iOS Nutzer

- Was kann man technisch, was muss man organisatorisch regeln?
- Welche Anforderungen werden durch das jeweilige Einsatzszenario definiert? Bereits vorhandene IT Infrastruktur, mobile Gerätelandschaft, Nutzerverhalten?
- Welche Bordmittel bieten die jeweiligen Gerätetypen /Betriebssysteme und (wie) lassen sich diese integrieren?
- Wahl sicherer Authentisierungsmethoden (2-Faktor-Authentisierung) in Abhängigkeit und Abwägung von Benutzerverhalten, Sicherheitslevel, lfd. Sekundärkosten, z.B. durch SMS Authentisierung, Effizienz (z.B. Active Directory Integration) -> was ist durchsetzbar/wirksam?
- Kontrollierte Gerätelandschaft sichern durch eindeutige User-Device-Verknüpfung -> Zugriff nur durch autorisierte Endgeräte/Betriebssysteme
- Individuelle und/oder rollenbasierte Content Kontrolle über Active Sync Zugänge, z.B.
  - E-Mails begrenzt auf die letzten 2 Wochen
  - PDF-Attachments verboten, XLS erlaubt
  - Zugriff auf eigene Kontakte, aber nicht auf fremde Kalender

- Wie lassen sich Sicherheitsstrategien mit Hilfe von MDM Lösungen automatisieren und damit langfristig durchsetzen?
  - Konsequente Trennnung privater und geschäftlicher Nutzung durch zeitgesteuerte Profile
  Carrot & Stick: nicht-konformes Sicherheitsverhalten der User wird durch Entzug von Zugriffs privilegien „bestraft"

- iOS spezifische Backupstrategien entwickeln -> iTunes abhängig, kann nicht eingefordert werden

Quick View – Mobile Device Management Planung

Bei der Konzeptionierung einer zentralen Managementlösung für iOS Geräte sind verschiedene Punkte zu beachten, die eine direkte Auswirkung auf den Einsatz und die Verwendung der Geräte haben können. Hier einige wichtige Fakten und Stolperfallen, die es zu beachtet gilt, die häufig keinen Workaround erlauben und/oder auf Vorgaben oder Einschränkungen seitens Apple beruhen.

Anbindung:
Apple erlaubt keinen eigenen Client auf den Geräten. Eine Anbindung ist nur durch die Mitarbeit des Nutzers möglich. WICHTIG: Dieses Anbindungsprofil kann vom Nutzer jederzeit gelöscht werden. Eine automatische Installation oder Neuinstallation der Anbindung ist nicht möglich. Die eigentliche Verbindung zum iOS Device hält der Apple Push Notification Service.

Konfiguration:
Der Nutzer ist Administrator. Sie können nicht verhindern, dass der Nutzer z.B. eigene E-Mail Accounts, WLAN Zugänge oder ähnliches selbst konfiguriert.

Sie können Backups nicht initiieren. iTunes Backups können nicht verhindert werden. Ebenso kann der Speicherort nicht „umgebogen" werden.

Sie können Systemupdates nicht Verhindern oder Anstoßen. iCal Daten und Adressbuchdaten liegen unverschlüsselt auf dem Device.

Applikationen:
Es gibt keine „Silent" Installation von Apps, egal ob selbstentwickelte oder aus iTunes. Der Nutzer muss immer zustimmen.

Es gibt kein Black- oder Whitelisting von Applikationen, sondern nur einen Workaround: Sind unerlaubte Apps installiert, gibt es keinen Zugang zu bestimmten geschäftsrelevanten Daten.

Beachten Sie die Regularien bezüglich App-Einkauf im iTunes Store. Es ist derzeit noch nicht möglich Volumenlizenzen zu kaufen.

Für weitergehende Informationen:

brainworks Website:

www.brainworks.de/ipad-im-business.html

Webcast-Reihe: iPad® im Business:

www.brainworks.de/events/webcasts.html

Ich möchte auf dem Laufenden bleiben:
Aktualisierte Kompendien und Expertentage.

www.brainworks.de/ipad-im-business-registrierung.html

Herausgeber
brainworks computer technologie GmbH
Paul-Heyse-Str. 28
80336 München

Tel. +49 89 326764-0 I Fax +49 89 326764-44
info@brainworks.de I www.brainworks.de

Erscheinungsdatum: Februar 2012 I 3. komplett überarbeitete Auflage
Autoren dieser Ausgabe: Christian Rattmann, Aurel Takacs, Stefan Haberland