ERNW Newsletter 33 / September 2010

Liebe Partner, liebe Kollegen,

willkommen zur 33. Ausgabe des ERNW-Newsletters mit dem Thema:

Das iPad im Unternehmenseinsatz

Version 1.0 vom 10. September 2010

von: Michael Thumann, mthumann@ernw.de & Rene Graf, rgraf@ernw.de

INHALTSVERZEICHNIS

1 EINFÜHRUNG

Apple landet mit seinen mobilen Geräten einen Verkaufsschlager nach dem anderen. Das neueste Gerät ist das Apple iPad, welches den Bereich des Mobile Computing revolutionieren soll, und dies auch tut. Das Gerät ist mobiler als jedes Notebook, einfach in der Bedienung und bietet bereits eine enorme Vielfalt an Applikationen, von denen viele auch im typischen Business Umfeld eingesetzt werden können. Beispiele sind die Programme Pages, Numbers und Keynote, Apple's Pendants zu MS Word, Excel und Powerpoint. Und selbstverständlich sind Apple iPad Benutzer auch technisch auf der Höhe der Zeit und setzen nur die neueste und modernste Technologie ein [;-)].

Entsprechend groß ist auch das Interesse vieler Mitarbeiter in den Unternehmen, das iPad im Tagesgeschäft einzusetzen. Während entsprechende Anfragen derzeit noch größtenteils abgewiesen werden, verbreitet sich das iPad bereits auf der Managementebene (die eine Ablehnung durch den IT-Fachbereich oft nicht zulässt). Allen Sicherheitsbedenken zum Trotz werden die Geräte angeschafft und an das Unternehmensnetzwerk angeschlossen. Speziell auf Managementebene überwiegt der „praktische Nutzwert" des Geräts.

Da Informationssicherheit in einem Unternehmen nicht als Selbstzweck verstanden werden darf, sondern vielmehr als unterstützender Prozess zur Erreichung der Unternehmensziele, sind Verbote besonderer Geräte wie z. B. des iPads meist nicht zielführend, insbesondere wenn sie bereits auf der Managementebene unterlaufen werden. Der sinnvollere Ansatz ist hier sicherlich die Integration dieser Geräte, basierend auf einem durchdachten und operablen Betriebs- und Sicherheitskonzept, um damit eine der Basisanforderungen einer Unternehmens-IT sicherzustellen: den kontrollierten Betrieb aller IT-Geräte.

Der Ihnen vorliegende Newsletter fasst die gängigen Bedrohungen des iPads in Bezug auf die Unternehmens-IT zusammen, enthält eine Risikoanalyse – basierend auf dem Rapid Risk Assessment Konzept von ERNW – und gibt Empfehlungen für einen akzeptabel sicheren Betrieb des iPads im Unternehmenskontext. Weiterhin werden bereits einige Neuerungen betrachtet, die das für Oktober/November 2010 erwartete iOS 4 für iPad mit sich bringen wird.

Da das iPad und das iPhone das gleiche Betriebssystem nutzen, treffen nahezu alle hier erwähnten Konzepte und Empfehlungen auch auf das iPhone zu.

2 AUFLISTUNG UND BESCHREIBUNG MÖGLICHER BEDROHUNGEN

2.1 Physikalischer Zugriff auf das Gerät

Für den physikalischen Zugriff auf das iPad sind zwei Szenarien maßgeblich: der Verlust des Gerätes und ein Diebstahl (Gelegenheitsdiebstahl oder zielgerichteter Diebstahl). Mit Hilfe forensischer Methoden kann der komplette Inhalt der Benutzer Partition auch ohne Kenntnis des Passcodes extrahiert werden. Die User Partition enthält alle veränderbaren Daten wie z. B.

- ❑ Gespeicherte bzw. gecachte Kennwörter (Keychain)
- ❑ Zertifikate
- ❑ Fotos
- ❑ SMS Nachrichten
- ❑ Browser Historie
- ❑ Konfigurationen (VPN, Mail usw.)
- ❑ Anruflisten
- ❑ Kontaktdaten
- ❑ Emails
- ❑ Kalendereinträge
- ❑ Keyboard Cache
- ❑ Spezifische Applikationsdaten

Da die forensischen Methoden auf einer Live Akquisition am laufenden Gerät basieren, verhindert auch die Hardware-Verschlüsselung des iPads nicht das extrahieren der Daten, da bereits beim Starten des Geräts die Entschlüsselung stattfindet.

Eine forensische Akquisition der Daten kann mit Hilfe dedizierter Werkzeuge durchgeführt werden, z. B. Lantern von Katana Forensics oder mit Hilfe der Zdiarski-Methode. Während die Werkzeuge üblicherweise „nur“ die oben aufgeführten Daten extrahieren, wird mit Hilfe der Zdiarski-Methode ein komplettes forensische Image der System und User Partition des iPads erstellt, aus dem sich auch gelöschte Informationen wiederherstellen lassen.

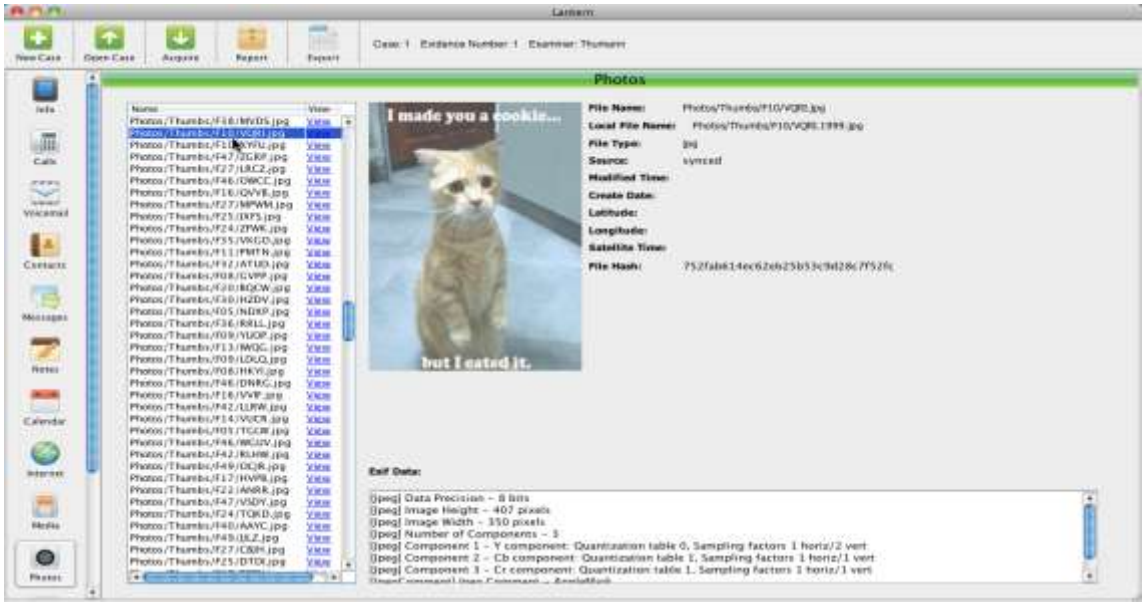

Figure 1: Lantern Photos

Mit Hilfe der Zdiarski-Methode kann auch der Passcode-Schutz deaktiviert werden, so dass bei einem physikalischen Zugriff auf das Gerät von einer kompletten Kompromittierung der Daten und des Gerätes ausgegangen werden muss.

2.2 Zugriff auf das Backup

Im Rahmen des Regelbetriebes eines iPads werden durch das Werkzeug iTunes regelmäßig Backups auf dem zur Synchronisation genutzten PC abgelegt. Dieses Backup enthält die gleichen Informationen, die auch mit Hilfe einer forensischen Analyse durch entsprechende Werkzeuge vom Gerät gewonnen werden können. Das Backup wird standardmäßig unverschlüsselt auf dem PC abgelegt, kann aber per Konfiguration auch verschlüsselt gespeichert werden. Auch hier existieren Werkzeuge, um relevante Daten aus dem Backup zu extrahieren wie z. B. der MobileSyncBrowser von Vaughn S. Cordero oder JuicePhone von addPod.

Figure 2: MobileSyncBrowser & JuicePhone

Sofern das Backup als „Encrypted Backup“ angelegt wird, ist ein Zugriff auf die Daten mit Hilfe der genannten Werkzeuge aber nicht möglich. Die Firma Elcomsoft aus Russland bietet jedoch im Rahmen ihrer Password Recovery Produkte auch ein Werkzeug an (iPhone Password Breaker), um das Kennwort für das „Encrypted Backup“ wiederherzustellen.

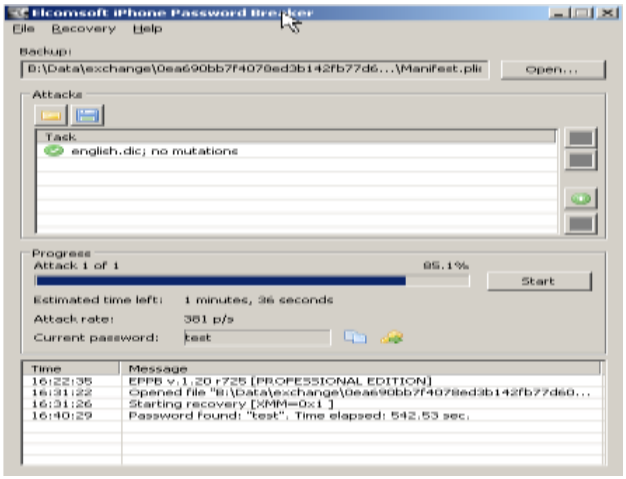

Figure 3: Elcomsoft iPhone Password Breaker

Dieses Werkzeug unterstützt, wie auch andere Produkte von Elcomsoft, die Grafikkartenprozessoren von NVIDIA und ATI und erlaubt damit ein sehr schnelles und effizientes Password Brute Forcing. Die verwendeten Kennwörter für das „Encrypted Backup“ bedürfen also einer entsprechenden Qualität, um diesem Werkzeug ausreichend lange standzuhalten.

2.3 Malwarezugriff auf sensible Daten

Das iPad enthält eine mobile Version des Apple Standardbrowsers Safari und kann analog eines Standard PCs zum Surfen innerhalb des Internets und/oder Intranets genutzt werden. Hierdurch wird das iPad allerdings auch den aktuellen Client Angriffen durch Malware ausgesetzt. Die Architektur des Betriebssystems enthält zum Schutz des Gerätes eine Sandbox in der die einzelnen Applikationen isoliert ablaufen, so auch der Safari Browser. Bei einer Kompromittierung des Gerätes z. B. über den Browser ist somit kein Zugriff auf die Daten anderer Applikationen möglich. Ausgenommen davon sind zentrale Bereiche des Gerätes, die von mehreren Applikationen verwendet werden wie z. B. die Keychain, in der u. a. Kennwörter in verschlüsselter Form abgelegt werden.

Weiterhin erlaubt das Gerät nicht die Ausführung von unsignierten und damit nicht vertrauenswürdigen Code auf dem System, so dass es nicht ohne weiteres möglich ist, beliebigen Code auf dem iPad auszuführen. Ausgenommen sind hier Code Fragmente die z. B. auf Javascript basieren oder Exploit Code, der beim Ausnutzen von Sicherheitslücken in das System eingeschleust wird.

2.4 Zugriff auf gecachte Tastatureingaben

Für das automatisierte Vervollständigen von Tastatureingaben werden diese in einer eigenen Datei gespeichert. Diese Datei kann sowohl aus den Backup Dateien als auch beim physikalischen Zugriff auf das Gerät ausgelesen, und ggf. können Nachrichtentexte, Kennwörter oder andere sensible Informationen extrahiert werden. Da es sich hier um eine zentrale Komponente handelt, wäre auch eine zielgerichtete Malware Komponente vorstellbar, die z. B. aus dem Browser Kontext Daten ausliest. Aktuell ist so eine Malware für das iPad allerdings noch nicht bekannt, so dass als reelle Bedrohungsszenarien die Backup Dateien und die forensische Analyse relevant sind, mit deren Hilfe die relevanten Dateien extrahiert werden können.

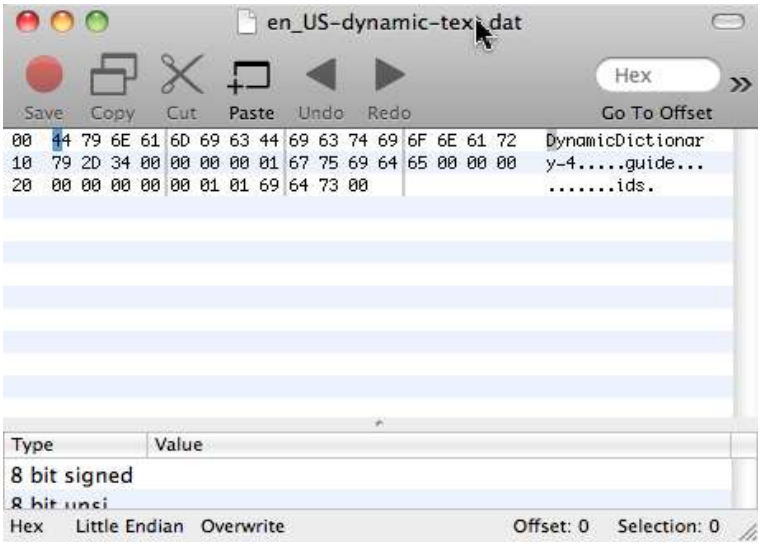

Figure 4: Keyboard Cache

Aus dem Keyboard Cache können Suchbegriffe, Inhalte von (gelöschten) Mails und sogar Kennwörter, die vom Betriebssystem nicht als solche erkannt worden sind und daher im Keyboard Cache abgelegt werden, extrahiert werden.

2.5 Patchmanagement

Um bekannt gewordene Sicherheitslücken zu beheben, bietet Apple für das iPad keinen besonderen Update Service wie Microsoft oder wie eben auch für das hauseigene Betriebssystem Mac OS X an. Sicherheitslücken werden auf dem iPad durch ein komplettes Update der Firmware behoben, was üblicherweise zu einem langen Zeitraum führt, in dem Geräte mit ungepatchten Sicherheitslücken betrieben werden (müssen). Ein Beispiel auf Basis des iPhones: Die letzte Version der iOS3 Familie wurde am 2. Februar 2010 veröffentlicht, das nächste Update inkl. mehr als 60 Security Updates erst am 21. Juni 2010. In der Zwischenzeit wurden einige kritische Sicherheitslücken bekannt, wie z. B. die unter CVE-ID CVE-2010-1775 geführte Password Lock Race Condition. Andererseits zeigt das aktuelle Beispiel der Jailbreakme Sicherheitslücke[1] , von der auch das iPad betroffen war, dass Apple durchaus in der Lage ist, einen kritischen Patch innerhalb von ca. 2 Wochen zur Verfügung zu stellen. Diese seitens des BSI und der Presse plakativ diskutierte Sicherheitslücke, die aufgrund eines nicht stattgefundenen „Responsible Disclosure Prozesses“ als 0-Day bezeichnet werden kann, wäre von anderen Herstellern auch nicht gravierend schneller behoben worden. Trotzdem verdeutlicht sie die Wichtigkeit eines funktionierenden Patchmanagement Prozesses für mobile Endgeräte wie das iPad. Durch die notwendige Installation der kompletten Firmware (auf mobilen Geräten) ist allerdings ein zuverlässiger Patchmanagment-Prozess nicht trivial implementierbar.

2.6 Jailbreak

Obwohl immer mehr Applikation für das iPad zur Verfügung stehen und Apple mit den aktuellen Firmware Versionen immer mehr geforderte Funktionen implementiert (z.B. Multitasking im iOS 4), müssen Entwickler von Apple spezifizierte Rahmenbedingungen einhalten, damit eine Anwendung über den offiziellen Kanal iTunes AppStore angeboten werden kann. Per Standardeinstellung können nur Anwendungen über diesen offiziellen Kanal installiert werden und auch nur mit einer gültigen Code Signing Signatur von Apple.

Eine Umgehung des offiziellen Distributionskanals ist mit Hilfe sogenannter Jailbreaks möglich. Ein Jailbreak basiert dabei auf der Ausnutzung einer vorhandenen Sicherheitslücke und setzt üblicherweise vorhandene Sicherheitsfunktionen wie die Sandbox und die Signed-Code-Only Anforderung außer Kraft. Nach einem erfolgreichen Jailbreak können beliebige Anwendungen, auch aus nicht vertrauenswürdigen Quellen, auf dem iPad installiert und betrieben werden.

Auch bei Veröffentlichung des iPads im Sommer 2010 war ein Jailbreak für die Firmware Version 3.2.1 innerhalb kürzester Zeit verfügbar.

[1] *vergl. dazu* http://www.heise.de/security/meldung/BSI-warnt-vor-Schwachstellen-in-iPhone-iPod-touch-und-iPad-1050706.html

2.7 Aufstellung der durchgeführten Proof of Concepts (PoC)

Die folgende Tabelle enthält eine Auflistung der durchgeführten PoCs für die Firmware Versionen 3.2.2 sowie Informationen, ob weitere PoCs (auch für das geplante iOS 4) mit entsprechenden Zeitaufwand möglich wären. Als PoCs werden üblicherweise praktisch durchgeführte Angriffe bezeichnet. Die Aussagen innerhalb der Tabelle beziehen sich dabei auf den aktuellen technischen Stand bzgl. praktisch durchführbarer Angriffe.

Bedrohung	PoC durchgef. iOS 3.2.1	PoC möglich iOS 3.2.1	PoC möglich iOS 4
Physikalischer Zugriff auf das Gerät	Ja	Ja	Nein
Zugriff auf das Backup	Ja	Ja	Ja
Malwarezugriff auf sensible Daten	Nein	Ja	Nein
Zugriff auf gecachte Tastatureingaben	Ja	Ja	Nein
Patchmanagement	Ja	Ja	Nein
Jailbreak	Ja	Ja	Ja

Weiterführende Informationen zum iOS4 und den neuen Sicherheitsfeatures entnehmen Sie bitte dem Kapitel 5.4 und der Tabelle 5.4.4. Hier werden u. a. Gründe, warum bestimmte Bedrohungen praktisch momentan nicht umsetzbar sind, näher erläutert.

2.8 Zusammenfassung

Mehrere der beschriebenen Bedrohungsszenarien sind abhängig von dem Eintreten einer anderen Bedrohung. Zum Beispiel können gecachte Tastatureingaben nur ausgelesen werden, wenn ein physikalischer Zugriff oder ein Zugriff auf das Backup möglich ist. Um einen geeigneten Maßnahmenkatalog zu definieren und eine realistische Ermittlung der Risiken durchzuführen, werden die Bedrohungen folgendermaßen zusammengefasst:

- ❑ Physikalischer Zugriff auf das Gerät
- ❑ Zugriff auf das Backup
- ❑ Malwarezugriff auf sensible Daten
- ❑ Patchmanagement
- ❑ Jailbreak

3 RAPID RISK ASSESSMENT

Zur Ermittlung der relevanten Risiken wird die von ERNW entwickelte Rapid Risk Assessment Methode (RRA) angewendet. RRA basiert dabei auf einer Auflistung der wesentlichen Bedrohungsszenarien (< 10) sowie einer Einschätzung bzgl. ihrer Eintrittswahrscheinlichkeit, Auswirkungen (sofern die Bedrohung eintritt) hinsichtlich der angestrebten Sicherheitsziele und der Anfälligkeit (Vulnerability) bezüglich der Bedrohungen.

Die Beschreibung der Eintrittswahrscheinlichkeit, Auswirkung und Vulnerability erfolgt an Hand einer numerischen Skala von 1-5, wobei diese Zahlen eine bestimmte Interpretation der Begriffe festlegen.

Begriff	1	2	3	4	5
Eintrittswahrscheinlichkeit	Am niedrigsten	niedriger	mittel	höher	Am höchsten
Auswirkung	Am niedrigsten	niedriger	mittel	höher	Am höchsten
Vulnerability (Anfälligkeit)	Am niedrigsten	niedriger	mittel	höher	Am höchsten

Eine Einordnung der Bedrohungen zu diesen drei relevanten Faktoren wird mit Hilfe einer Vorgehensweise aus dem Bereich Agile Development vorgenommen. Hierzu werden jeweils die Bedrohungen mit der niedrigsten und der höchsten Eintrittswahrscheinlichkeit ausgewählt, diese repräsentieren jeweils 1 und 5. Andere Bedrohungen werden danach im Vergleich zu diesen definierten Grenzwerten betrachtet und eingeordnet (das gleiche Vorgehen wird auf die Faktoren Auswirkung und Vulnerability angewendet). Durch diese vergleichende Betrachtung können Diskussion über die Begriffe „hoch“, „niedrig“ usw. vermieden werden.

Zur Ermittlung des Risikos selbst wird folgende Formel verwendet:
Risiko = Eintrittswahrscheinlichkeit * Auswirkung * Vulnerability

Die Bedrohungen mit dem höchsten Risikofaktor werden dann entsprechend priorisiert adressiert, ggf. können auch Schwellwerte definiert werden, deren Überschreitung Maßnahmen zwingend erfordern.

Da einige der Bedrohungen sich bzgl. der Vulnerability (Anfälligkeit) je nach eingesetzter Firmware unterscheiden, wird die Risikonanalyse für Version 3.2.x und das geplante iOS 4 gesondert durchgeführt.

3.1 iPad mit iOS 3.2.1 oder älter

Bedrohung	Eintrittswahr-scheinlichkeit	Vulnerability	Auswirkung	Risk
Physikalischer Zugriff auf das Gerät	3	5	5	75
Zugriff auf das Backup	2	1	4	8
Malwarezugriff auf sensible Daten	1	3	3	9
Patchmanagement	4	4	2	32
Jailbreak	5	5	1	25
Average Risk				**29,8**

3.2 iPad mit iOS 4.0 oder neuer

Bedrohung	Eintrittswahr-scheinlichkeit	Vulnerability	Auswirkung	Risk
Physikalischer Zugriff auf das Gerät	3	3	5	45
Zugriff auf das Backup	2	1	4	8
Malwarezugriff auf sensible Daten	1	3	3	9
Patchmanagement	4	2	2	16
Jailbreak	5	5	1	25
Average Risk				**20,6**

3.3 Ergebnis der Risikoanalyse

Basierend auf der durchgeführten Risikoanalyse kann das Ergebnis folgendermaßen zusammengefasst werden:

Das geringste Risiko entsteht bei einem Einsatz des iPads mit der geplanten Firmware iOS4.
Die drei größten Risiken entstehen durch

1. Physikalischen Zugriff auf das Gerät
2. Jailbreaks
3. Patchmanagement

4 MAßNAHMEN FÜR DEN EINSATZ EINES IPADS IM UNTERNEHMEN

Dieses Kapitel beschreibt die Maßnahmen, welche seitens ERNW empfohlen werden, um einen akzeptabel sicheren Betrieb des iPads zu ermöglichen. Alle Empfehlungen basieren auf den Ergebnissen der Risikoanalyse (und der in ihr enthaltenen Erfahrung der Autoren).

4.1 Technische Mindestanforderungen

Aufgrund der durchgeführten Risikoanalyse werden folgende Mindestanforderungen an Hard- und Software definiert:

- ❑ iPad WiFi+3G
- ❑ iOS4 oder neuer

Eine Unterstützung älterer Firmware insbesondere im Unternehmenseinsatz wird aufgrund einer signifikanten Erhöhung des Risikos nicht empfohlen, ebenso wenig wie das rein WiFi basierte Modell, da hier ein zentrales Management nur bei Konnektivität zu einem WLAN gewährleistet werden kann. Apple selbst empfiehlt, das iPad mit der aktuellen Firmware 3.2.2 *nicht* im Unternehmen zu betreiben.

4.2 Provisioning/Configuration Profile

Unter „Provisioning“ versteht man das Ausrollen von Geräten mit einer initialen, unternehmensspezifischen Konfiguration.

Es existieren verschiedene Möglichkeiten, das iPad zu konfigurieren. Welche davon genutzt werden sollte, hängt in erster Linie von der Anzahl auszurollender Geräte ab. Während eine kleine Anzahl (<10 – 20) Geräte noch relativ problemlos manuell konfiguriert werden kann, ist dies in großen Umgebungen schlicht unmöglich.

Die manuelle Konfiguration findet direkt am Gerät über das enthaltene Konfigurationsmenu statt. Dies ist die einfachste Form der iPad Konfiguration und sollte nicht im Unternehmenskontext eingesetzt werden. Eine einheitliche Konfiguration kann nicht sichergestellt werden und Änderungen durch den Endbenutzer können nicht verhindert werden. Des Weiteren stehen nicht alle Konfigurationsoptionen zur Verfügung (z.B. Benutzereinschränkungen).

Mittels der von Apple kostenlos bereitgestellten Software „iPhone Configuration Utility“ können sogenannte Konfigurationsprofile erstellt werden. Konfigurationsprofile sind XML-Dateien die sowohl eine Komplette Gerätekonfiguration, als auch eine Teilkonfiguration enthalten können. D.h. es können ein oder mehrere Konfigurationsprofile auf einem iPad (oder iPhone) installiert werden. Über Konfigurationsprofile können auch Einstellungen vorgenommen werden, die direkt am Gerät nicht zur Verfügung stehen (wie z.B. das Sperren bestimmter Funktionen).

Konfigurationsprofile können nach Erstellung wiederum auf verschiedene Art und Weise auf das Gerät gelangen. Sie können direkt auf ein am PC angeschlossenes iPad installiert werden, per Browser (Safari) von einem Webserver heruntergeladen werden (Link z.B. per SMS, Email, ...) oder per Email verteilt werden.

Dies sind die von Apple direkt unterstützten Methoden (ohne zusätzlich benötigte kostenpflichtige Software) zur Geräte-Provisionierung. Eine teilweise automatisierte Provisionierung der Geräte wird in Kapitel 4.3 (Provisioning Systeme) beschrieben.

Es wird empfohlen, die Konfigurationsprofile mittels elektronischer Signatur vor unbefugten Veränderungen zu schützen und das Profil zu sperren (User darf es nicht entfernen)! Dies ist für

den Einsatz im Unternehmenskontext unerlässlich. Für Details siehe „beschriebene Einstellungen“.

Folgender Screenshot zeigt das iPhone Configuration Utility:

Im Folgenden werden die sicherheitsrelevanten Einstellungen im Konfigurations-Profil beschrieben. Jeweils mit möglichen und empfohlenen Einstellungen der jeweiligen Punkte. Es wird an dieser Stelle auch bereits auf Optionen eingegangen, die erst mit iOS 4 genutzt werden können (können also aktuell nur mit iPhones genutzt werden, nicht aber mit dem iPad). Vor allem in Bezug auf ein zentrales Management der Geräte bringt das iOS 4 wichtige Neuerungen mit sich.

Die Rubrik „General“ ist immer vorhanden. Alle weiteren Rubriken sind nur im Profil enthalten, wenn für diese Rubrik ein sogenannter „Payload“ definiert wurde. Einige Rubriken können dabei mehr als einen Payload enthalten. Dies ermöglicht es, mehrere Profile kombiniert auf einem Gerät zu installieren (z.B. Standort bezogene WLAN Profile, unternehmensweite Profile (Restriktionen, Zertifikate, ...) und benutzerspezifische Profile mit Zugangsdaten o.ä..

Detaillierte Informationen zu den einzelnen Konfigurations-Optionen können im offiziellen „iOS Enterprise Deployment Guide“ nachgelesen werden.

Generell wird empfohlen, soweit möglich, durch SSL/TLS gesicherte Verbindungen zu konfigurieren. Werden bestimmte Verbindungen ausschließlich über eine VPN Verbindung genutzt (z.B. Emails abrufen) und die unternehmensweite Sicherheitsrichtlinie erlaubt unverschlüsselte Datenübertragungen innerhalb des Unternehmensnetzwerkes, kann auf eine SSL Verschlüsselung verzichtet werden. In allen anderen Fällen (Verbindung über nicht-

vertrauenswürdiges Netzwerk) wird dringend empfohlen, gemäß gängiger Best Practices, eine durch SSL/TLS gesicherte Verbindung zu verwenden.

Um SSL/TLS Verbindungen sicher zu nutzen, müssen Zertifikate validiert werden können. Hierzu muss das sogenannte Stammzertifikat, also das Zertifikat der Zertifizierungsinstanz dem Gerät bekannt sein. Diese, sowie zur Client Authentifizierung verwendete Zertifikate, können und müssen über die Rubrik „Credentials“ auf dem Gerät hinterlegt werden. Ein installiertes Stammzertifikat gilt als Voraussetzung für alle im Folgenden konfigurierten SSL/TLS Verbindungen.

Die folgenden Unterkapitel orientieren sich an der Struktur des Konfigurations-Profils.

4.2.1 General

Regelt allgemeine Profilinformationen, die jedes Profil enthalten muss.

Option	Mögliche Einstellung	empfohlen	Bemerkung
Name	Es sollte ein möglichst aussagekräftiger Name gewählt werden um Verwechslungen zu vermeiden.		
Identifier	Eindeutiger Identifier des Profils. Relevant für Profil Updates. Ist dieser bei einem zu installierenden Profil identisch mit einem Profil Identifier eines bereits installierten Profils, so wird dieses ersetzt.		
Organization	Name der Organisation / des Unternehmens		
Description	Möglichst aussagekräftige Beschreibung		
Security	Always With Authorization Never	With Authorization	Regelt, wann/wie das Profil wieder entfernt werden darf. „Always“ erlaubt es dem Nutzer das Profil einfach zu entfernen. „Never“ bedarf der Kompletten Löschung des Geräts, um das Profil wieder loszuwerden. „With Authorization“ erlaubt das Entfernen mittels Passwort (das dem Nutzer nicht bekannt sein sollte).
Authorization Password	Passwort zum Entfernen des Profils. Wählen Sie ein möglichst sicheres Passwort, das der im Unternehmen gültigen Passwortrichtlinie genügt.		

4.2.2 Passcode

Dieser Abschnitt regelt die Authentifizierung am Gerät sowie das Verhalten bei Falscheingaben.
Die empfohlenen Werte orientieren sich an gängigen Best Practices. Generell sollte die im Unternehmen gültigen Passwortrichtlinie für mobile Endgeräte verwendet werden.

Option	Mögliche Einstellung	empfohlen	Bemerkung
Require passcode on device	Aktiv Inaktiv	Aktiv	Diese Einstellung regelt, ob ein Passcode erforderlich ist
Allow simple value	Aktiv Inaktiv	Inaktiv	Zulässigkeit einfacher Zeichenfolgen
Require alphanumeric value	Aktiv Inaktiv	Aktiv	Es ist mindestens ein Buchstabe erforderlich
Minimum passcode length	0 – 16	8	Mindestlänge des Passworts
Minimum number of complex characters	0 – 4	1	Anzahl erforderlicher Sonderzeichen
Maximum passcode age	0 – 730	90	Maximales Alter des Passworts in Tagen
Auto Lock	0 - 5	5	Nach angegebener Anzahl Minuten Inaktivität ist ein Passwort erforderlich.
Passcode history	0 – 50	10	Nach welcher Anzahl „Passwortänderungen“ kann ein Kennwort wiederverwendet werden.
Grace period for device lock	None Immediatelly 1, 5, 15 Minutes 1, 4 hours	Immediatelly	Wie lange kann das Gerät gesperrt sein, bevor ein Passwort benötigt wird (verzögerte Passwort Aufforderung)

4.2.3 Restrictions

Dieser Abschnitt regelt Einschränkungen der nutzbaren Funktionalität.
Generell sollten Sie sich hier an der im Unternehmen gültigen Richtlinie bzgl. „Acceptable Use“ von mobilen Endgeräten orientieren.

Abschnitt: Device Functionality

Einschränkungen von Gerätefunktionen. Sämtliche hier aufgeführten Einstellungen können entweder aktiviert oder deaktiviert werden. Individuelle Werte können nicht angegeben werden.

Option	Bemerkung
Allow installing Apps	Können Applikationen durch den Benutzer installiert werden? Dies sollte deaktiviert werden. Nutzer können dann nur noch durch die IT bereitgestellte Applikationen nutzen. Dies wird jedoch bei den Nutzern (vor allem bei VIPs) nicht sehr gut ankommen). Ggf. kann es hier sinnvoll sein, für bestimmte Nutzergruppen unterschiedliche Profile zu verwenden.
Allow use of camera	Dieser Wert sollte abhängig von der im Unternehmen gültigen Sicherheitsrichtlinie konfiguriert werden. (z.B. ist in Produktionsumgebungen häufig das Mitführen verboten). Da aktuelle iPad Modelle keine Kamera enthalten, ist diese Einstellung lediglich für iPhones relevant.
Allow screen capture	Dürfen Screenshots aufgenommen werden. Diese Einstellung kann aktiviert bleiben. Ggf. sollten Benutzer darauf hingewiesen werden, keine Screenshots von vertraulichen Daten anzufertigen.
Allow automatic sync while roaming	Abhängig vom Mobilfunkvertrag. Hier kann es ebenfalls sinnvoll sein, verschiedene Profile anzufertigen (z.B. deaktiviert bei Benutzern ohne Auslandstarif, aktiviert bei Benutzern mit Auslandstarif)
Allow voice dialing	Kann aktiviert werden. Ggf. sollten Benutzer im Umgang mit mobilen Geräten in der Öffentlichkeit geschult werden.
Allow In App Purchase	Dürfen Applikationen Kaufvorgänge durchführen? Dies kann aktiviert bleiben.
Force encrypted backups	Dies muss aktiviert werden. Bewirkt, dass Backups grundsätzlich verschlüsselt gespeichert werden.

Abschnitt: Applications

Einschränkungen von Applikationen bzw. deren Nutzbarkeit.

Option	Mögliche Einstellung	Bemerkung
Allow use of YouTube	Aktiv Inaktiv	Abhängig von der „Acceptable Use“ Richtlinie für mobile Endgeräte.
Allow Use of iTunes Music Store	Aktiv Inaktiv	Abhängig von der „Acceptable Use“ Richtlinie für mobile Endgeräte.
Allow Use of Safari	Aktiv Inaktiv	Abhängig von der „Acceptable Use“ Richtlinie für mobile Endgeräte. Da die Nutzbarkeit des Gerätes massiv

		eingeschränkt würde, wird empfohlen dies aktiviert zu belassen. Die folgenden Einstellungen sind Safari spezifisch.
Safari: Enable autofil	Aktiv Inaktiv	Kann aktiviert bleiben.
Safari: Force fraud warning	Aktiv Inaktiv	Empfohlen: aktiv Aktiviert Safaris Betrugs Warnungen.
Safari: Enable JavaScript	Aktiv Inaktiv	Kann aktiviert bleiben, da Usability vieler Webseiten massiv eingeschränkt würde.
Block Pop-ups	Aktiv Inaktiv	Keine spezielle Empfehlung.
Accept Cookies	Always Never From visited sites	Orientierung an den sonst im Unternehmen üblichen Browsereinstellungen.

Abschnitt: Ratings

Kategorisierung von Inhalten, sowie Einschränkungen von expliziten Inhalten.

Option	Mögliche Einstellung	Bemerkung
Ratings region	Australia Canada France Germany Ireland Japan New Zealand United Kingdom United States	Entsprechend des Standortes.
Movies	Dont allow Allow all Diverse Altersgrenzen	Angepasst an Unternehmens Richtlinie (Acceptable Use) und an das Alter des Nutzers. (Ggf. verschiedene Profile erstellen, sofern minderjährige Nutzer vorhanden sind)
TV Shows		
Apps		

4.2.4 Wi-Fi

Dieser Abschnitt legt WLAN Zugangsprofile fest. Je Wi-Fi Payload wird ein WLAN konfiguriert.

Die empfohlenen Werte orientieren sich an gängigen Best Practices.
Generell sollten Sie sich hier an der im Unternehmen gültigen Sicherheitsrichtlinie für WLAN Netzwerke orientieren. Dieser Newsletter geht nicht auf sichere WLAN Konfiguration ein.

Unterstützt werden alle gängigen WLAN Sicherheitstypen (WEP, WPA, WPA2). Jeweils in der „Home“ und in der „Enterprise“ Variante. Die den aktuellen Best Practices für den sicheren WLAN Betrieb im Unternehmen entsprechende Variante ist „WPA / WPA2 Enterprise“. Diese nutzt als Authentifizierungsframework 802.1X basierte Authentifizierung. Dabei werden die folgenden EAP Methoden unterstützt:

- TLS
- TTLS
- LEAP
- PEAP
- EAP-FAST
- EAP-SIM

Neben der Auswahl einer EAP Methode/EAP Protokolls können außerdem noch Authentifizierungsoptionen sowie Trust Beziehungen konfiguriert werden.

Zur Authentifizierung im WLAN können entweder Benutzername/Passwort oder Zertifikate eingesetzt werden. Zertifikate zur Benutzer Authentifizierung, Trusted Certificate Authorities und Server Zertifikate können in der Konfigurations-Rubrik „Credentials“ hinterlegt werden.

Bei der Konfiguration ist darauf zu achten, dass die Einstellungen für „Protocols“, „Authentication“ und „Trust“ soweit als möglich eingeschränkt werden (z.B. nur noch das tatsächlich genutzte Protokoll erlaubt ist) und die zu akzeptierenden Zertifikate explizit angegeben werden.

Außerdem wird empfohlen, die Option „Allow Trust Exceptions“ zu deaktivieren, sodass Benutzer bei Authentifizierungsproblemen keine Ausnahmen („Connect anyway“) definieren können.

4.2.5 VPN

Dieser Abschnitt legt VPN Zugangsprofile fest. Je VPN Payload wird ein VPN Zugang konfiguriert. Die empfohlenen Werte orientieren sich an gängigen Best Practices.
Generell sollte die im Unternehmen gültige Sicherheitsrichtlinie für VPN Netzwerke beachtet werden und die Konfiguration entsprechend der VPN Infrastruktur angepasst werden. Dieser Newsletter geht nicht auf sichere VPN Konfiguration ein.

Vom iPad werden derzeit die folgenden VPN Protokolle/Hersteller unterstützt:

- L2TP
- PPTP
- IPSec (Cisco)
- Cisco Anyconnect (Ab iOS Version 4.1)
- Juniper SSL (Ab iOS Version 4.1)

Einziges zur Nutzung empfohlenes Protokoll für iPads mit iOS Version 3.x ist „IPSec (Cisco)“.
Die weiteren unterstützten Protokolle (L2TP, PPTP) gelten als unsicher und sollten nicht genutzt werden.

Unter iOS wird sowohl eine Maschinen Authentifizierung als auch eine Benutzer Authentifizierung (XAuth) unterstützt.

Maschinen Authentifizierung

Zur Maschinen Authentifizierung sollten Zertifikate eingesetzt werden. Zertifikate sollten unbedingt eindeutig einem Endgerät zuzuordnen sein, um diese im Verlustfall sperren zu können. Dies muss auch beim Design der PKI (CRL Support; Revocation Prozesse), sowie bei der Konfiguration der Einwahlknoten (regelmäßiges CRL Update) berücksichtigt werden.

Benutzer Authentifizierung

Zusätzlich zur Maschinen Authentifizierung wird empfohlen eine auf Einmalpasswörtern (OTP) basierende Benutzer Authentifizierung zu implementieren. Dies kann seitens des iPads über die Einstellung „Account“ und „Include User PIN“ erreicht werden.

Des Weiteren wird geraten, im VPN Profil einen Proxy Server zu hinterlegen, so dass sämtlicher Internet Verkehr über die unternehmensweite Internet Zugangs-Infrastruktur (zentraler Proxy, AV, ...) geleitet wird.

Dies stellt sicher, dass Sicherheitsmechanismen wie Contentfilter, zentraler Antivirus für Webtraffic usw. auch durch die iPhones/iPads genutzt werden können.

Sofern die VPN Konfiguration über Konfigurations-Profile auf ein iPhone/iPad eingespielt werden, wird im Hintergrund automatisch eine Option „Require Encrypted Backup“ aktiviert, um bei einem Backup relevante VPN Zugangsdaten ausschließlich verschlüsselt abzulegen.

4.2.6 Email

Dieser Abschnitt legt Email Zugangsprofile fest. Je Payload wird ein Email Zugang konfiguriert. Die empfohlenen Werte orientieren sich an gängigen Best Practices.

Das iPad unterstützt sowohl POP, als auch IMAP basierte Email Zugänge. Die Anbindung an einen Microsoft Exchange Server kann über die Rubrik „Exchange Active Sync“ Konfiguriert werden.

Generell wird empfohlen eine sichere Verbindung zum Email Server zu konfigurieren. Werden Emails ausschließlich über eine VPN Verbindung abgerufen und die unternehmensweite Sicherheitsrichtlinie erlaubt unverschlüsselten Email Verkehr innerhalb des Unternehmensnetzwerkes, kann auf eine SSL Verbindung zum Email Server verzichtet werden. In allen anderen Fällen wird dringend empfohlen, gemäß gängiger Best Practices, eine durch SSL/TLS gesicherte Verbindung zu verwenden.

4.2.7 Exchange Active Sync

Dieser Abschnitt legt Zugangsprofile für Microsofts Exchange Active Sync fest. Je Payload wird ein Zugang konfiguriert. Die empfohlenen Werte orientieren sich an gängigen Best Practices.

Mittels Active Sync können diverse Daten mit einem Exchange Server synchronisiert werden (Mail, Kalender, ...)

Außerdem kann Active Sync auch für die Verwaltung von iPads/iPhones, sowie zum Provisioning genutzt werden. Siehe hierzu auch Kapitel 4.3 „Provisioning Systeme“.

Generell wird empfohlen eine sichere Verbindung zum Server zu konfigurieren. Werden Informationen ausschließlich über eine VPN Verbindung synchronisiert und die unternehmensweite Sicherheitsrichtlinie erlaubt unverschlüsselte Datenübertragungen innerhalb des Unternehmensnetzwerkes, kann auf eine SSL Verbindung zum Server verzichtet werden. In allen anderen Fällen wird dringend empfohlen, gemäß gängiger Best Practices, eine durch SSL/TLS gesicherte Verbindung zu verwenden.

Soll zertifikatsbasierte Client Authentifizierung zum Einsatz kommen, muss ein Zertifikat angegeben werden. Im Gegensatz zu nahezu allen anderen Zugängen, wird ein Clientzertifikat für einen Active Sync Zugang nicht in der Rubrik „Credentials“ konfiguriert, sondern direkt im Payload.

4.2.8 LDAP

Dieser Abschnitt legt Zugangsprofile für LDAP basierte Verzeichnisdienste fest. Je Payload wird ein Zugang konfiguriert. Die empfohlenen Werte orientieren sich an gängigen Best Practices.

Mittels LDAP können z.B. Informationen aus einem unternehmensweiten Adressverzeichnis zugegriffen werden.

Generell wird empfohlen eine sichere Verbindung zum Server zu konfigurieren. Werden Informationen ausschließlich über eine VPN Verbindung abgerufen und die unternehmensweite Sicherheitsrichtlinie erlaubt unverschlüsselte Datenübertragungen innerhalb des Unternehmensnetzwerkes, kann auf eine SSL Verbindung zum Server verzichtet werden. In allen anderen Fällen wird dringend empfohlen, gemäß gängiger Best Practices, eine durch SSL/TLS gesicherte Verbindung zu verwenden.

4.2.9 CalDAV

Dieser Abschnitt legt Zugangsprofile für CalDAV basierte Kalenderdienste fest. Je Payload wird ein Zugang konfiguriert. Die empfohlenen Werte orientieren sich an gängigen Best Practices.

Mittels CalDAV können unternehmensweite Kalendersysteme, die den CalDAV Standard unterstützen, eingebunden werden.

Generell wird empfohlen eine sichere Verbindung zum Server zu konfigurieren. Werden Informationen ausschließlich über eine VPN Verbindung abgerufen und die unternehmensweite Sicherheitsrichtlinie erlaubt unverschlüsselte Datenübertragungen innerhalb des Unternehmensnetzwerkes, kann auf eine SSL Verbindung zum Server verzichtet werden. In allen anderen Fällen wird dringend empfohlen, gemäß gängiger Best Practices, eine durch SSL/TLS gesicherte Verbindung zu verwenden.

4.2.10 CardDAV

Dieser Abschnitt legt Zugangsprofile für CardDAV basierte Adressbuchdienste fest. Je Payload wird ein Zugang konfiguriert. Die empfohlenen Werte orientieren sich an gängigen Best Practices.

Mittels CardDAV können unternehmensweite Adressverzeichnisse, die den CardDAV Standard unterstützen, eingebunden werden.

Generell wird empfohlen eine sichere Verbindung zum Server zu konfigurieren. Werden Informationen ausschließlich über eine VPN Verbindung abgerufen und die unternehmensweite

Sicherheitsrichtlinie erlaubt unverschlüsselte Datenübertragungen innerhalb des Unternehmensnetzwerkes, kann auf eine SSL Verbindung zum Server verzichtet werden. In allen anderen Fällen wird dringend empfohlen, gemäß gängiger Best Practices, eine durch SSL/TLS gesicherte Verbindung zu verwenden.

4.2.11 Subscribed Calendars

Über diesen Konfigurations-Abschnitt können iCal Kalender eingebunden werden. Je Payload wird ein Kalender konfiguriert. Die empfohlenen Werte orientieren sich an gängigen Best Practices.

Mittels iCal können unternehmensweite Kalender „read-only“ eingebunden werden die im standardisierten iCal Format bereitgestellt werden.Zusätzlich stehen im Internet diverse öffentliche iCal Kalender zur Verfügung (z.B. Schulferienkalender, gesetzliche Feiertage, ...)

Für vertrauliche Kalender wird empfohlen eine sichere Verbindung zum Server zu konfigurieren. Werden Informationen ausschließlich über eine VPN Verbindung abgerufen und die unternehmensweite Sicherheitsrichtlinie erlaubt unverschlüsselte Datenübertragungen innerhalb des Unternehmensnetzwerkes, kann auf eine SSL Verbindung zum Server verzichtet werden. In allen anderen Fällen wird dringend empfohlen, gemäß gängiger Best Practices, eine durch SSL/TLS gesicherte Verbindung zu verwenden.

4.2.12 Web Clips

Webclips ermöglichen den schnellen Zugriff auf häufig genutzte Webseiten. Diese werden dann über ein eigenes Icon auf dem Homescreen wie eine App dargestellt.

Diese Rubrik ist für die Gesamtsicherheit des Geräts nicht relevant. Im Unternehmensumfeld kann dies jedoch eine nützliche Funktion darstellen (z.B. Intranet, Speiseplan, ...)

4.2.13 Credentials

Dieser Konfigurations-Abschnitt ermöglicht das Einbinden von Zertifikaten. Hierüber werden sowohl Stammzertifikate, als auch Zertifikate zur Maschinen-, und Client-Authentifizierung eingebunden.

Um SSL/TLS Verbindungen sicher zu nutzen, müssen Zertifikate validiert werden können. Hierzu muss das sogenannte Stammzertifikat, also das Zertifikat der Zertifizierungsinstanz dem Gerät bekannt sein.

Zertifikate für Active Sync Zugänge werden direkt im „Active Sync“ Payload definiert.

4.2.14 SCEP

Über diesen Konfigurations-Abschnitt können die Geräte automatisch Zertifikate von einer SCEP unterstützenden Zertifizierungsinstanz (CA) beziehen. SCEP steht für „Simple Certificate Enrollment Protocol“.

Es wird empfohlen eine Schlüssellänge von 2048 Bit zu verwenden.

Zum Thema „Automatisches Ausrollen von Zertifikaten“ siehe auch folgendes Kapitel 4.3 „Provisioning Systeme“.

4.2.15 Mobile Device Management

Ab iOS Version 4 werden so genannte „Mobile Device Management“ Systeme unterstützt. Hierzu sei auf das folgende Kapitel 4.3 „Provisioning Systeme“ verwiesen.

4.2.16 Advanced

Über diesen Konfigurations-Abschnitt können fortgeschrittene Einstellungen für das Mobilfunknetz vorgenommen werden.

Sofern im Unternehmenskontext kein dedizierter APN bereitgestellt wird, ist dies nicht für die Gesamtsicherheit des Geräts relevant.

(Einige sehr große Organisationen/Unternehmen/Behörden verfügen über einen eigenen APN, sodass eine „Einwahl“ eine exklusive Verbindung mit dem Unternehmensnetzwerk ermöglicht, das Endgerät aber nicht „über das Internet“ kommuniziert).

4.3 Provisioning Systeme/Mobile Device Management

Neben der manuellen Konfiguration der iPads/iPhones direkt am Gerät können Konfigurationsprofile, wie in Kapitel 4.3 beschrieben, erstellt werden und per Email oder Webbrowser auf dem Gerät installiert werden. Auch diese Vorgehensweise stößt an ihre Grenzen wenn die Anzahl der Geräte steigt.

Für den sicheren Betrieb von iPads/iPhones ist deshalb (wie es auch schon für andere Endgeräte gilt) eine zentrale Verwaltung und automatische Konfiguration unverzichtbar.

Dieser Abschnitt stellt einige Möglichkeiten hierzu vor.

Zur automatischen Konfiguration von Endgeräten kommen sogenannte Provisioning Systeme zum Einsatz. Im Idealfall beinhalten solche Systeme ein umfangreiches Management der iPads inkl. der Überwachung der eingesetzten Hard- und Software.

Um iOS Geräte automatisch zu konfigurieren, werden folgende Komponenten benötigt:

- ❑ Profile Distribution Service
- ❑ Certificate Authority (Mit SCEP Support)
- ❑ Directory/Authentication Service (AD, LDAP, ...)

Der Profile Distribution Service ist für die Auslieferung von Konfigurationsprofilen an die iPads/iPhones zuständig. Ein Profile Distribution Service muss entweder selbst entwickelt werden, oder kann von 3rd Party Anbietern gekauft werden.

Im Folgenden wird die Funktionsweise überblicksartig beschrieben. Eine detaillierte Beschreibung enthält Apples Enterprise Deployment Guide.

Zu Beginn des Enrollment Prozesses über den Profile Distribution Service können einige Device spezifische Informationen abgefragt werden, um z. B. Mindestanforderungen an Gerätetyp und Firmware Version sicherzustellen. Weiterhin können auch Informationen wie IMEI und MAC Adresse des Geräts geprüft werden, um eine Device „Authentifizierung“ vor der Installation des Configuration Profiles durchzuführen (Neben der Benutzerauthentifizierung per z.B. HTTP Basic).

Nachdem das iPad den Profile Distribution Service initial kontaktiert hat (Aufruf einer URL durch den Benutzer/Administrator, die manuell eingegeben oder per Email (ggf. SMS) verteilt werden kann) sendet dieser eine Anfrage nach weiteren Informationen. Das iPad antwortet auf diese Anfrage mit den angeforderten Informationen und signiert diese Antwort mit dem von Apple

vorinstallierten Gerätezertifikat. Das iPad erhält darauf als Antwort ein Konfigurationsprofil, das alle benötigten Informationen zum Erstellen einer Zertifikatsanfrage (CSR) und zur automatischen Installation eines Zertifikats mittels SCEP beinhaltet.

Nach erfolgreicher Installation eines Zertifikats per SCEP sendet das iPad erneut die vom Profile Distribution Service angefragten Informationen als HTTP POST zurück, Dieses Mal signiert mit dem soeben installierten Zertifikat. Als Antwort darauf erhält das iPad nun das/die finale(n) Konfigurationsprofil(e).

Damit der gesamte Ablauf bis auf die initiale URL Eingabe (bzw. das Versenden und Anklicken eines Links) automatisiert ablaufen kann, muss der Profile Distribution Service in der Lage sein für jedes Gerät/Benutzer automatisiert Konfigurationsprofile zu erstellen. Dabei sollten zur Authentifizierung/Autorisierung möglichst bereits vorhandene Infrastruktur (z.B. Verzeichnisdienste) genutzt werden.

Apples Enterprise Deployment Guide [8] beschreibt diesen Ablauf detailliert.

Da der gesamte Ablauf auf HTTP basiert und gut dokumentiert ist, kann ein Profile Deployment Service mit mäßigem Aufwand implementiert werden. Eine detaillierte Beispielimplementierung ist unter [9] zu finden. Alternativ können 3rd Party Produkte eingesetzt werden.

Diese Vorgehensweise ermöglicht eine effiziente Inbetriebnahme inklusive nitialer Konfiguration von iPads/iPhones. Atomatische Profil Updates, Inventarisierung, Asset Management, Reporting oder sonstige Remote Administration sind damit jedoch nicht möglich.

Um das Aufspielen unerwünschter Software zu verhindern, insbesondere die Durchführung von Jailbreaks und die Installation nicht vertrauenswürdiger Software, sollte das Provisioning System auch ein Live Inventory bzw. ein Asset Management beinhalten. Außerdem wird eine Reporting Funktion benötigt, um unautorisierte Software schnell zu erkennen (z. B. mit Hilfe von Whitelists und Blacklists) und ggf. den Zugriff für das betroffene Gerät zu sperren.

4.3.1 Mobile Device Management ab iOS 4

Ab iOS 4 gibt es die Möglichkeit, einen Mobile Device Management Server über das Konfigurationsprofil zu konfigurieren. Dieser übernimmt anschließend die weitere Verwaltung des Geräts.

Mit Hilfe des Mobile Device Managements kann die IT-Abteilung Konfiguration für das iPad ausrollen, überwachen, das Gerät sperren und aus der Ferne komplett löschen. Eingerichtet wird das Remote Management über die „Mobile Device Management Option“ des Configuration Profiles. Wenn der Management Server mit einem iPad kommunizieren möchte, versendet er eine Push Notification über einen Apple Push Notification Service (APNS), der bei dem iPad einen Zwangskonnekt zum Management Server initiiert. Das iPad prüft dann, welche Jobs auf dem Management Server bereit liegen und führt diese aus. Auf diese Weise können Policy Updates ausgeführt und eine Inventarisierung vorgenommen werden sowie eine Gerätesperrung oder Löschung.

Die Konfigurationsmöglichkeiten innerhalb der Mobile Device Management Kategorie unterteilen sich dabei in 4 Kategorien: Enrollment, Configuration, Querying und Management.

Enrollment:

Für die initiale Einbindung eines iPads/iPhones in ein Management System ist ein Enrollment Prozess notwendig. Dies kann auf verschiedene Weise durchgeführt werden wie schon in Kapitel 4.2 beschrieben.

Wird das Over-the-Air Enrollment durchgeführt, ist der Ablauf wie folgt:

- Verbindung zu einem Profile Distribution Service (über http) und Authentifizierung
- Übertragung der angeforderten Inventardaten und Empfang der SCEP Informationen (um das Zertifikat zu empfangen)
- Empfang des Zertifikats über SCEP
- Neue Verbindung zum Profile Distribution Service und Empfang der finalen Konfiguration, die auch die Konfiguration für das Mobile Device Management enthält

Über die Mobile Device Management Payload können folgende Konfigurationen vorgenommen werden:

- Server URL (Mobile Device Management Server)
- Check In URL (Required for Installation)
- Topic (For Notification Service)
- Identity (Certificate for Authentication)
- Access Rights (Entsprechend der Anforderungen des Management Systems zu konfigurieren)

Configuration

Alle weiteren Konfigurationsprofile können von nun an über das Mobile Device Management System verteilt und installiert werden. Eine ausführliche Beschreibung der Optionen befindet sich in Kapitel 4.2.

Querying:

Mit Hilfe des neuen Mobile Device Managements können diverse Informationen abgefragt werden:

- Device information
  - Unique Device Identifier (UDID)
  - Device Name
  - iOS und Build Version
  - Model name und number
  - Seriennummer
  - Kapazität
  - IMEI
  - Modem Firmware
- Network Information
  - ICCID
  - Bluetooth und Wi-Fi MAC Addressen
  - Aktuelles Carrier Network
  - SIM Carrier Network
  - Carrier Settings Version
  - Telefonnummer
  - Data Roaming Setting (On/Off)
- Compliance und Security Information
  - Installierte Configuration Profiles
  - Installierte Zertifikate mit Ablaufdatum

- Liste aller konfigurierten Einschränkungen
- Hardware Encryption vorhanden (ja/nein)
- Passcode gesetzt (ja/nein)

❑ Applications
- Installierte Applikationen (App ID, Name, Version, Größe der App sowei des durch Daten belegten Speicherplatzes)
- Installierte Provisioning Profiles inkl. Ablaufdatum

Management:

Des Weiteren können die folgenden Funktionen aus der Ferne ausgelöst:

❑ Remote Wipe: Bei Verlust Gerät durch eine Nachricht vom Management Server löschen.
❑ Remote Lock: Sperren des Geräts (Passwort Eingabe erforderlich)
❑ Clear Passcode: Temporäres Entfernen des Passwort Schutzes. Dies ermöglicht dem Benutzer ein neues Passwort festzulegen.

4.3.2 Mobile Device Management mit Microsoft Exchange ActiveSync

Mit iOS 4 können iPads/iPhones auch mittels Microsoft ActiveSync Policies gemanaged werden. Hierüber können eine ganze Reihe Restriktionen sowie Passwortanforderungen festgelegt werden. Remote Wipe Nachrichten können hierüber ebenfalls übermittelt werden.

Eine detaillierte Beschreibung hierzu ist unter [10] zu finden.

4.3.3 Auswahl Kriterien

Bei der Anschaffung bzw. Evaluierung von Provisioning Lösungen sollten folgende Punkte zwingend berücksichtigt werden werden:

❑ Erkennung des Gerätetyps (iPad WiFi und iPad WiFi+3G)
❑ Erkennung der installierten Firmware (> 4.0)
❑ Live Hard- und Software Inventory
❑ Software Whitelists und Blacklists
❑ Unterstützung aller Optionen der Configuration und Provisioning Profile für das iPad
❑ Unterstützun der neuen iOS 4 Features

Sollten bereits Systeme vorhanden sein, die um iPad/iPhone Management Funktionalitäten erweitert werden können, ist dies natürlich vorzuziehen.

4.3.4 3rd Party Produkte

Apple selbst bietet derzeit keine Profile Distribution Server und auch keine kompletten Mobile Device Management Server an. Es steht jedoch ausreichend Dokumentation zur Verfügung um diese Dienste selbst zu implementieren. Außerdem sind auf dem Markt diverse Produkte verfügbar, die iPads und iPhones verwalten können.

Einige Produkte können dabei ausschließlich iPads/iPhones verwalten, andere dagegen unterstützen die komplette Palette an Smartphones (Blackberry, Symbian, Windows Mobile). Möglicherweise setzen sie ja bereits ein solches System ein und können ihre iPads/iPhones dort einbinden. Diese Option sollte in jedem Fall geprüft werden.

Im Folgenden ein kleiner Auszug:

Afaria:

Vendor: Sybase

Website: http://www.sybase.com/products/mobileenterprise/afaria
Devices: Apple, Windows Mobile, Symbian, PalmOS SyncML Devices

Feature	Beschreibung
Device Type Detection	Ja
Firmware Detection	Ja
Inventory	Ja
Unterstützung aller iOS Optionen	Ja
iOS4 Features	Ja

TARMAC:
Vendor: Equinux
Website: http://www.equinux.com/us/products/tarmac/index.html
Devices: Apple only

Feature	Beschreibung
Device Type Detection	Erkennt iPad, iPhone (2,3,3G,3GS), iPod, aber nicht, ob das iPad mit 3G ausgestattet ist
Firmware Detection	Ja
Inventory	Nein
Unterstützung aller iOS Optionen	Ja. Configuration Profiles werden mit Apples iPhone Configuration Utility erstellt, exportiert und in das System importiert
iOS4 Features	Nein

Airwatch:
Vendor: Airwatch
Website: http://www.air-watch.com/
Devices: Apple, Windows Mobile, Symbian, Blackberry, Android

Feature	Beschreibung
Device Type Detection	Ja
Firmware Detection	Ja
Inventory	Nein
Unterstützung aller iOS Optionen	Ja
iOS4 Features	Neue Features werden aktuell noch nicht unterstützt.

Ubitexx:

Vendor: Ubitexx
Website: http://www.ubitexx.como
Devices: Apple, Windows Mobile, Symbian

Feature	Beschreibung
Device Type Detection	Ja
Firmware Detection	Ja
Inventory	Ja
Unterstützung aller iOS Optionen	Ja
iOS4 Features	Teilweise / geplant

Good for Enterprise

Vendor: Good Technologies
Website: http;//ww.good.com
Devices: Apple, Windows Mobile, Symbian, PalmOS SyncML Devices

Feature	Beschreibung
Device Type Detection	Ja
Firmware Detection	Ja
Inventory	Ja
Unterstützung aller iOS Optionen	Ja
iOS4 Features	Geplant; Advanced Management Features durch Installation einer dedizierten App auf den Clients.

Mobileiron:

Vendor: Mobileiron
Website: http://www.mobileiron.com
Devices: Apple, Windows Mobile, Symbian, Palm webOS, Blackberry

Feature	Beschreibung
Device Type Detection	Ja
Firmware Detection	Ja
Inventory	Ja
Unterstützung aller iOS Optionen	Ja
iOS4 Features	Ja

4.4 Neue Funktionalitäten von iOS 4

Neben diversen neuen Funktionen wie Multitasking, welche in erster Linie die Bedürfnisse der Benutzer adressieren, werden auch wichtige sicherheitsrelevante Änderungen vorgenommen, die direkt einige der spezifizierten Risiken vermindern und erfolgreiche Angriffe massiv erschweren. Das betrifft einerseits das Patchen von Schwachstellen, aber auch Änderungen in der prinzipiellen Funktionsweise.

Zu den relevanten Änderungen gehören die folgenden Punkte.

4.4.1 Data Protection

Nachdem die mit dem iPhone 3GS eingeführte Hardware Verschlüsselung, die auch für das iPad gilt, bereits innerhalb kurzer Zeit umgangen werden konnte, hat Apple mit dem iOS4 nachgebessert. Die Verschlüsselung erfolgt nicht mehr ausschließlich mit Schlüsseln, die sich auf dem Gerät selbst befinden, sondern der User Passcode wird in die Schlüsselgenerierung mit eingebunden. Außerdem kann pro Anwendung ein sogenannter Class Key generiert werden, um alle Anwendungsdaten auch anwendungsspezifisch zu verschlüsseln. Applikationen können somit nicht auf die Daten anderer Anwendungen zugreifen und diese entschlüsseln. Die folgende Grafik (aus einem Vortrag über neue Sicherheitsfunktionen in iOS4) verdeutlicht das Prinzip:

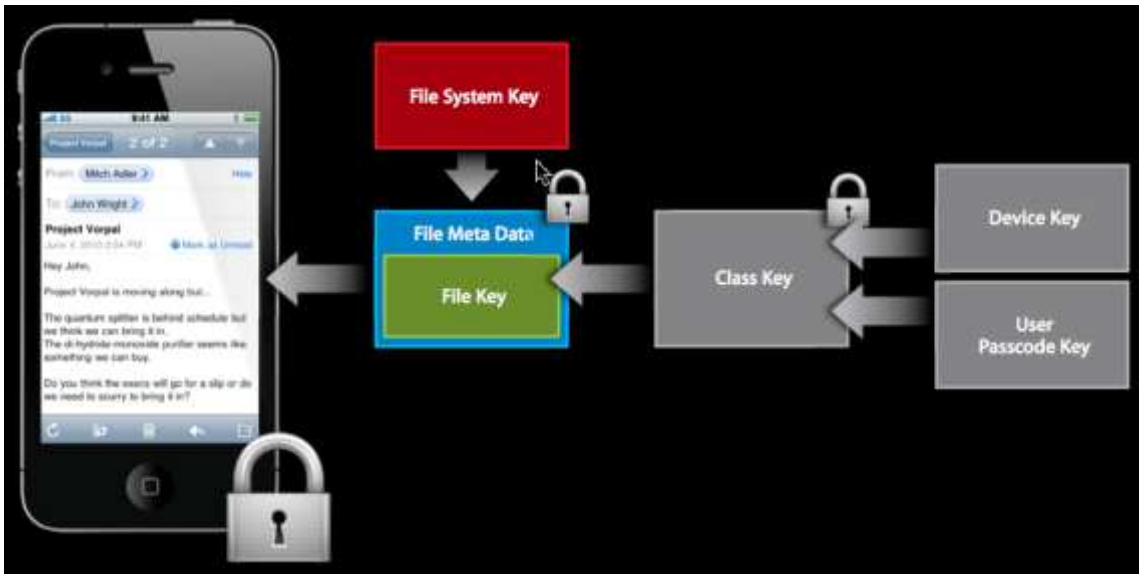

Figure 5: Data Protection

Die Implementierung erfolgt über neue Programmierschnittstellen des iOS4 und muss von den iPad Anwendungen auch unterstützt werden, es ist also Sache der Entwickler diese neuen Funktionen in die Applikationen einzubauen. Zum Start des iOS4 wird die anwendungsspezifische Verschlüsselung beispielsweise von der Mail Applikation bereits unterstützt.

4.4.2 Backup

Das iOS4 beinhaltet auch Änderungen in der Funktionsweise bzw. des Designs des Backup Prozesses. Während mit der Firmware 3.2.x die Daten in der Keychain mit Hilfe des Device Keys verschlüsselt werden und somit geräteabhängig und nicht auf ein anderes Gerät portierbar sind, ändert sich dies mit iOS 4. Die neue Firmware unterscheidet hier, ob ein normales oder ein „Encrypted“ Backup erstellt wird. Im Rahmen des normalen Backups bleibt die Funktionsweise unverändert, wird aber ein „Encrypted Backup“ erstellt, werden die Daten innerhalb des verschlüsselten Backups im Klartext abgelegt. Dies ermöglicht das Rückspielen eines solchen Backups auf andere Geräte und damit auch der in der Keychain gespeicherten Daten. Da das Backup selbst verschlüsselt ist, gelten diese Daten als ausreichend gesichert und ermöglichen trotzdem den Austausch von Geräten ohne Datenverluste beim Restore.

Die aktuelle Version des iPhone Password Breakers von Elcomsoft berücksichtigt diese Besonderheit des iOS 4 bereits und enthält einen sogenannten Keychain Explorer, der nach erfolgreichen Knacken des Passworts die Informationen aus der Keychain anzeigt, wie z. B. Mail Kennwörter, WLAN Zugangsdaten, VPN Zugangsdaten, iTunes Store Zugangsdaten, den Passcode des iPads, Zugangsdaten anderer installierter Applikationen und auch die SIM PIN.

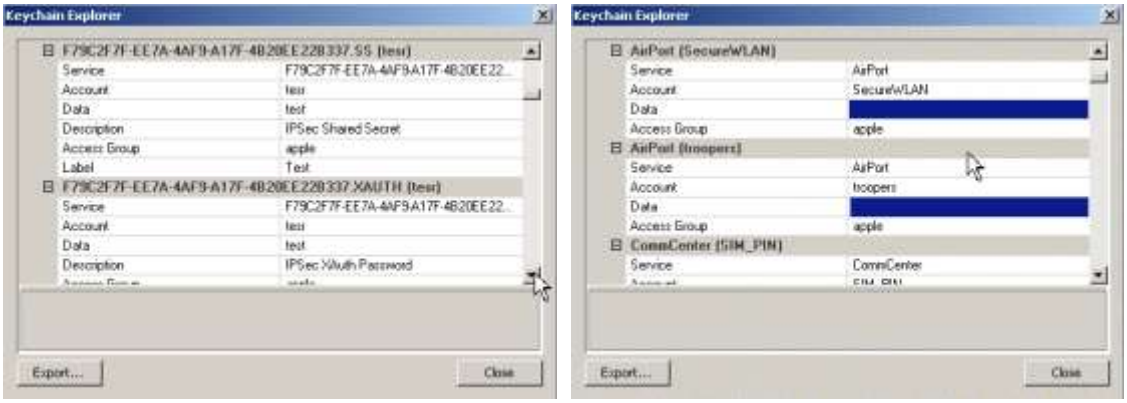

Figure 6: Keychain Explorer

Voraussetzung für einen erfolgreichen Angriff ist der Zugriff auf das verschlüsselte Backup und das erfolgreiche Ermitteln des Kennwortes. Durch die Nutzung besonders guter Kennwörter kann dieser Angriff massiv erschwert werden. Die empfohlene Password Policy sieht folgendermaßen aus:

- Zeichensatz: Full Keyspace, also Buchstaben (groß und klein), Zahlen sowie Sonderzeichen.
- Keine, in Wörterbüchern vorkommenden, Kennwörter und auch keine Permutationen von solchen.
- Mindestlänge: 16 Zeichen (ergibt bei aktuell max. Performance des Elcomsoft Tools eine Dauer von ca. $2{,}7 * 10^{26}$ Jahren, um alle möglichen Kombinationen zu testen)

4.4.3 VPN

Mit Einführung von iOS4 für das iPad werden zukünftig auch SSL VPNs unterstützt. Das betrifft die SSL Lösungen von Cisco und Juniper und damit die am häufigsten installierten SSL VPN Lösungen.

4.4.4 Mobile Device Management

Das iOS4 enthält jetzt auch einige neue Funktionen, welche Unternehmen für ein sinnvolles Management von mobilen Endgeräten benötigen. Die wichtigste Funktion ist hierbei der Remote Wipe bei Verlust des iPads, also das Löschen des iPads über einen Remote Befehl. Hierbei ist allerdings anzumerken, dass ein Remote Wipe bei zielgerichteten Diebstählen eines iPads in der Regel nicht mehr ausgeführt werden kann, da die SIM-Karte in der Regel sofort entfernt wird, um ein Löschen der Daten und auch eine Ortung des gestohlenen Gerätes zu verhindern. Weiterhin können Hardware Informationen und eine Liste der installierten Applikationen abgefragt und eine regelmäßige Zwangsverbindung zum Provisioning System konfiguriert werden. Dies erleichtert u. a. auch das Detektieren eines Jailbreaks, über das Software Inventory können unautorisierte Programme wie z. B. der Cydia Installer erkannt und entsprechende Maßnahmen eingeleitet werden. (siehe hierzu auch 4.3.1)

4.4.5 iOS4 und seine Möglichkeiten der Risikoreduzierung

Die folgende Tabelle zeigt, inwieweit iOS 4 Auswirkungen auf die festgestellten Bedrohungen hat:

Bedrohung	Durch iOS 4 Security Features verbessert	Erläuterung
Physikalischer Zugriff auf das Gerät	Ja	Sowohl das Patchen bekannter Sicherheitslücken, als auch die neu eingeführte Data Protection erschweren den unautorisierten Zugriff auf das Gerät erheblich.
Zugriff auf das Backup	Nein	Der vorhandene Password Cracker für verschlüsselte Backups von Elcomsoft wurde bereits an iOS 4 angepasst.
Malwarezugriff auf sensible Daten	Ja	Die mit der Data Protection eingeführte anwendungsspezifische Verschlüsselung verhindert bei korrekter Implementierung durch die Entwickler den unautorisierten Datenzugriff durch andere Applikationen.
Zugriff auf gecachte Tastatureingaben	Ja	Sowohl das Patchen bekannter Sicherheitslücken, als auch die neu eingeführte Data Protection erschweren den unautorisierten Zugriff auf das Gerät erheblich und damit auch den Zugriff auf sensible Informationen.
Patchmanagement	Ja	Mit dem iOS 4 Update werden absehbar wieder sicherheitsrelevante Probleme behoben.
Jailbreak	Ja	Mit dem Erscheinen von iOS 4 für das iPad muss zwar ebenfalls auch mit der Veröffentlichung eines passenden Jailbreaks gerechnet werden, allerdings bieten die neuen Management Funktionen (Software Inventory) die Möglichkeit, einen Jailbreak zu erkennen.

4.5 Infrastrukturmaßnahmen

Da insbesondere mobile Endgeräte schwer gegen Verlust zu schützen sind, sollten auch Infrastrukturmaßnahmen implementiert werden, um bei Offenlegung von Zugangsdaten (z. B. VPN) auf den verlorenen Geräten, den Zugriff auf Unternehmensressourcen zu erschweren. Der Zugang zum Unternehmensnetz sollte durch eigene Netwerksegmente erfolgen, die je nach Risikoklasse der Endgeräte gruppiert werden, z. B. also ein eigenes Segment für mobile Geräte wie das iPad und ein eigenes Segment für Notebooks (diese können z. B. mit Hilfe von Smart Card Readern besser geschützt werden, als iPads). Speziell mobile Geräte wie das iPad haben häufig geringere Anforderungen, was den Zugriff auf Unternehmensressourcen angeht und können daher auch strenger in ihren Kommunikationsbeziehungen reglementiert werden. Die Kommunikationsbeziehungen sollten per Firewallkonfiguration geregelt und implementiert werden.

4.6 Organisatorische Maßnahmen

Da immer einige Risiken gar nicht oder nur mit hohem Kostenaufwand adressiert werden können, sollten technische Maßnahmen durch organisatorische Maßnahmen unterstützt werden. Beim Einsatz des iPads betrifft dies in erster Linie eine Nutzungsvereinbarung mit dem Enduser. Diese sollte die folgenden Punkte beinhalten und regeln:

- ❑ Ein Duplizieren der Konfiguration für den Zugriff auf das Unternehmsnetzwerk auf ein anderes Gerät bedarf der schriftlichen Zustimmung durch das Unternehmen.
- ❑ Eine Nutzung von iPads mit einem iOS kleiner Version 4 ist untersagt.
- ❑ Eine Nutzung von iPads Modellen ohne 3G ist untersagt.
- ❑ Die Durchführung eines Jailbreak des iPads ist untersagt.
- ❑ Verstöße gegen die Nutzungsbedingungen führen zu einer sofortigen Sperre des Zugangs und zum Ausschluss aus dem Nutzungsverfahren für iPads.

Bei Bedarf sind weitere interne Anforderungen in den Nutzungsbedingungen zu ergänzen.

4.7 Zusammenfassung der Maßnahmen

Abschließend werden hier noch einmal die wichtigsten Maßnahmen für einen akzeptabel sicheren Betrieb des iPads im Unternehmenskontext zusammengefasst:

- ❑ Mindestanforderung: iPad Modell WiFi+3G und iOS4 oder neuer
- ❑ Einsatz eines Configuration Profiles auf Basis der ERNW Empfehlung
- ❑ Einsatz eines Provisioning Systems inkl. Hard- und Software Inventarisierung
- ❑ Segmentierung des Netzeinwahlsegmentes
- ❑ Vereinbarte Nutzungsbedingungen zwischen dem Unternehmen und den Endusern

Mit freundlichen Grüßen,

Michael Thumann und Rene Graf

ERNW Enno Rey Netzwerke GmbH
Breslauer Str. 28
69124 Heidelberg
Tel. +49 6221 480390
Fax +49 6221 419008
www.ernw.de

5 ONLINE RESOURCEN

[1] Apple Business Resources
http://www.apple.com/business/resources/
http://www.apple.com/de/business/resources/

[2] iPad Enterprise Overview
http://www.apple.com/support/ipad/enterprise/
http://www.apple.com/de/support/ipad/enterprise/

[3] iPhone Enterprise Overview
http://www.apple.com/support/iphone/enterprise/
http://www.apple.com/de/support/iphone/enterprise/

[4] iPad Security Overview
http://images.apple.com/ipad/business/pdf/iPad_Security_Overview.pdf
http://images.apple.com/de/ipad/business/pdf/iPad_Security_Overview.pdf

[5] iPhone Security Overview
http://images.apple.com/iphone/business/docs/iPhone_Security_Overview.pdf
http://images.apple.com/de/iphone/business/docs/iPhone_Security_Overview.pdf

[6] iPhone Device Configuration Overview
http://images.apple.com/iphone/business/docs/iPhone_Device_Configuration_Overview.pdf
http://images.apple.com/de/iphone/business/docs/iPhone_Device_Configuration_Overview.pdf

[7] iOS Reference Library / Enterprise Deployment
http://developer.apple.com/iphone/library/navigation/index.html#filter=Enterprise%20Deployment

[8] iPhone OS - Enterprise Deployment Guide
http://manuals.info.apple.com/en_US/Enterprise_Deployment_Guide.pdf
http://manuals.info.apple.com/de_DE/Einsatz_in_Unternehmen.pdf
http://discussions.apple.com/category.jspa?categoryID=246

[9] Over-the-air profile delivery and configuration (provisioning development example)
http://developer.apple.com/iphone/library/documentation/NetworkingInternet/Conceptual/iPhoneOTAConfiguration/Introduction/Introduction.html

[10] Exchange ActiveSync and iOS 4 Devices
http://developer.apple.com/iphone/library/featuredarticles/FA_Exchange_ActiveSync_and_iOS4_Devices/Introduction/Introduction.html

[11] Mobile Device Management
http://images.apple.com/iphone/business/docs/iPhone_MDM.pdf

6 ANHANG A: NÜTZLICHE APPS FÜR DEN UNTERNEHMENSEINSATZ

Die nachfolgende Tabelle enthält einige iPad Applikationen, die sich während der Evaluierung als nützlich für einige Aufgaben des Tagesgeschäftes erwiesen haben.

Name	Beschreibung	iTunes Link
iBooks	Apple's eBook Reader	http://itunes.apple.com/de/app/ibooks/id364709193?mt=8
Pages	Apple's Textverarbeitung	http://itunes.apple.com/de/app/pages/id361309726?mt=8
Numbers	Apple's Tabellenkalkulation	http://itunes.apple.com/de/app/numbers/id361304891?mt=8
Keynote	Apple's Präsentationssoftware	http://itunes.apple.com/de/app/keynote/id361285480?mt=8
GoodReader	Dokumentenverwaltung und Reader (PDF, MS-Office)	http://itunes.apple.com/de/app/goodreader-for-ipad/id363448914?mt=8
iAnnotate PDF	PDF Bearbeitung	http://itunes.apple.com/de/app/iannotate-pdf-kommentar/id363998953?mt=8
CHMate Lite	CHM Reader	http://itunes.apple.com/de/app/id335157929?mt=8
iSaveWeb	Webseiten Offline Browser	http://itunes.apple.com/de/app/isaveweb-website-download/id305594530?mt=8
Penultimate	Handschriftliche Notizen	http://itunes.apple.com/de/app/penultimate/id354098826?mt=8
Calculator	Taschenrechner	http://itunes.apple.com/de/app/calculator-hd-for-ipad/id364905554?mt=8
World Clock	Weltzeit Uhr	http://itunes.apple.com/de/app/the-world-clock/id368177365?mt=8
DevInfo	System Infos (laufende Prozesse, offene Netzwerkports)	http://itunes.apple.com/de/app/devinfo/id294217490?mt=8
iSSH	SSH, Telnet und VNC Client (inkl. X11 Support)	http://itunes.apple.com/de/app/issh-ssh-vnc-console/id287765826?mt=8