FORSCHUNGSZENTRUM JÜLICH GmbH
Jülich Supercomputing Centre
D-52425 Jülich, Tel. (02461) 61-6402

Interner Bericht

Das iPad im wissenschaftlichen Umfeld
Sicherheitsbetrachtungen zum Einsatz im Unternehmen

Egon Grünter, Markus Meier, Thomas Schmühl

FZJ-JSC-IB-2011-01

Juni 2011

(letzte Änderung: 30.06.2011)

1. Einleitung

Mobilität in der Informationstechnologie war lange Zeit gleichbedeutend mit der Nutzung tragbarer Rechner, wie Laptops, Notebooks, Subnotebooks und Netbooks. Diesen Geräteklassen stellt die Firma Apple Inc.[1] ihr neuestes Gerät, das iPad, entgegen. Durch seine geringe Größe und sein geringes Gewicht ist es scheinbar „mobiler" als jedes Netbook, und stellt eine Neuerung im Personal Information Management (PIM) dar. Es ist einfach in der Bedienung und bietet eine Vielzahl von Anwendungen, die auch im Berufsleben eingesetzt werden können. Als Beispiel dienen dafür die Apps[2] Pages, Numbers und Keynote, welche Apples Pendants zu Microsoft Word, Excel und Powerpoint darstellen.

Daher hält das iPad auf Managementebene schon Einzug in viele IT-Landschaften unterschiedlichster Firmen. Allen Sicherheitsbedenken zum Trotz werden die Geräte angeschafft und an das Unternehmensnetzwerk angeschlossen. Für das IT-Management eines Unternehmens ist eine sinnvolle Integration auf Basis eines durchdachten und operablen Betriebs- und Sicherheitskonzeptes daher ratsam.

Im vorliegenden Bericht sollen Sicherheitsbetrachtungen im Mittelpunkt stehen, die den Einsatz eines iPads in einem wissenschaftlichen Umfeld wie dem Forschungszentrum Jülich GmbH beeinflussen. Ausgehend von einer kurzen Beschreibung der Technik und daraus abgeleiteten Bedrohungsszenarien werden Empfehlungen für den praktischen Einsatz abgeleitet. Basis des Berichts bilden die Erfahrungen mit dem Betriebssystem iOS4. Da iPhone, iPod Touch und iPad aus sicherheitstechnischer Sicht fast gleich sind, gelten alle Empfehlungen und Konzepte auch für das iPhone und den iPod Touch der Firma Apple.

[1] http://www.apple.com
[2] Kurzform für Application (Anwendung)

2. Technik

Das iPad basiert auf dem Apple eigenen 1GHz A4-Prozessor, der für den mobilen Einsatz optimiert wurde. Es hat Speicherkapazitäten von 16, 32 oder 64 GB und einen Arbeitsspeicher von 256 MB. Basis des Betriebssystems bildet der Darwin-Kernel, der auch dem hauseigenen Mac OS zugrunde liegt. Im Wesentlichen wurden hier Anpassungen für den mobilen Einsatz des Gerätes vorgenommen. Insbesondere die Integration der Multitouch-Benutzerschnittstelle (Touchscreen) ist hier hervorzuheben. Seit der Version 4 heißt das Betriebssystem „iOS".

Als Festplatte dient eine Solid-State-Disk mit Hierarchical File System Plus (HFS+). Unterteilt ist der Speicherplatz in eine System- und eine Mediapartition. Auf der Systempartition werden das Betriebssystem, Bibliotheken und vorinstallierte Programme gespeichert. Der Zugriff auf diese Partition ist nur lesend möglich. Nur während einer Systemaktualisierung erhält diese Partition für die Dauer dieses Vorgangs Schreibrechte.

Alle übrigen Daten sind auf der Media Partition gespeichert. Zu diesen Daten zählen nicht nur über den AppStore[3] installierte Anwendungen, sondern auch Konfigurationseinstellungen für WLAN-Zugänge, E-Mail-Zugänge, Bilder, Kontakte, Videos, Musik, Lesezeichen des Browsers, zwischengespeicherte Tastatureingaben etc. Während des normalen Betriebs muss diese Partition also mit Schreibrechten dem Nutzer zur Verfügung gestellt werden.

Beim Startvorgang eines iPads setzt Apple auf eine sog. Vertrauenskette, die Manipulationen ausschließen soll. Die notwendigen Code Images der Bootloader werden nacheinander in den Arbeitsspeicher geladen und einer Signaturprüfung unterzogen [1]. Jedes Image ist verschlüsselt und mit einer RSA-Signatur versehen [2], so dass eine fehlgeschlagene Signaturprüfung den eigentlichen Bootvorgang unterbindet. Das Apple-Gerät springt dann in einen „Device Firmware Upgrade"-Modus, der die Wiederherstellung des Betriebssystems und des fehlerhaften Bootloaders ermöglicht.

Außer den Bootloadern sind die Bibliotheken und Programme ebenfalls mit einem Apple-Zertifikat signiert, so dass beim Start einer Applikation deren Signatur geprüft werden kann. Die Prüfung der Apps durch Apple ist eine Grundvoraussetzung für den Vertrieb über den AppStore.

Wird eine Applikation gestartet, so wird sie in einer Sandbox ausgeführt. Durch Einsatz dieser Technik wird die Anwendung so weit eingeschränkt, dass Zugriffe nur auf das eigene Verzeichnis innerhalb des Dateisystems und auf gemeinsam genutzte Dateien möglich sind. Zugriff auf Systemressourcen und Daten anderer Komponenten kann nur über definierte Schnittstellen realisiert werden. Damit soll Fehlverhalten der Programme und die Ausnutzung von Schwachstellen verhindert werden.

Zusätzlich hat Apple das sog. eXecute-Never-Bit (XN-Bit) als Schutz eingeführt. Das XN-Bit markiert Stack und Heap (den Datenbereich von Anwendungen) als nicht ausführbar, und erschwert so das Einschleusen von

[3] Vertriebsplattform für Apps

Schadcode durch Ausnutzen einer besonders häufigen Klasse von Schwachstellen in Programmen.

Passwörter und/oder Zertifikate kann das iPad in der sog. „Keychain“ ablegen. Diese dient als Passwort-Safe, der mit einem gerätespezifischen Master-Passwort verschlüsselt wird. Die Entschlüsselung erfolgt transparent für den Benutzer. Zugreifbar ist dieser Schlüsselbund nur dann, wenn eine zugreifende Anwendung mittels eines Zertifikats authentifiziert wurde.

Das Apple iPad kommuniziert in der Regel über die integrierte WLAN- oder Mobilfunkschnittstelle innerhalb öffentlicher Netzwerke, wie z.B. WLAN-Hotspots oder Mobilfunknetze. Daher sollten Zugriffe auf Anwendungen des Firmennetzwerkes in der Regel über Virtual Private Network Technologien erfolgen. Vertrauliche Informationen, die in Konfigurationseinstellungen für Zugangswege ins Unternehmensnetzwerk, E-Mails, Kalender- und Adressbucheinträgen oder in Dokumenten enthalten sind, stehen nicht nur auf dem iPad zur Verfügung, sondern sie werden oftmals über die erwähnten öffentlichen Netzwerke hinweg ungesichert übertragen. Darüberhinaus werden Daten während der Benutzung des iPads gespeichert. Dazu zählen nicht nur die üblichen temporären Internetdateien, die aus der Nutzung des Webbrowsers resultieren, sondern auch Tastatureingaben, Snapshot-Bilder bei Betätigung der Hometaste oder markierte Orte in Google-Maps[4].

Sicherungen der auf dem iPad gespeicherten Daten erfolgen über die Apple eigene Anwendung iTunes, die unter Mac OS und Windows-Betriebssystemen nutzbar ist. Typischerweise werden die Daten unverschlüsselt im Dateisystem desjenigen Rechners abgelegt, mit dem das iPad synchronisiert wurde. Allerdings können diese Backups auch verschlüsselt abgelegt werden. Bei der folgenden Darstellung der Bedrohungsszenarien ist daher der Rechner, mit dem das iPad verbunden und synchronisiert wurde, mit einzubeziehen.

[4] Bei Nutzung des iPhones werden SMS-Kurznachrichten in einer Datenbank auf dem Gerät gespeichert.

3. Bedrohungsszenarien

Bei den Sicherheitsrisiken muss man zwischen physikalischem und netzwerkseitigem Zugriff auf das Gerät unterscheiden.

Bei physikalischem Besitz des iPads sind Vertraulichkeit, Integrität und Verfügbarkeit äußerst gefährdet. Eine schnelle Akquisition der Daten am laufenden System mit Hilfe forensischer Methoden kann innerhalb weniger Minuten vollkommen unbemerkt erfolgen [3]. Diebstahl und Verlust des Gerätes gehören ebenfalls in diese Risikoklasse.

Die Klasse der Bedrohungen, welche nicht vom physikalischen Besitz des iPads abhängen umfasst zum einen die Ausnutzung von Schwachstellen im Betriebssystem oder in Systemdiensten durch installierte Anwendungen. Weiterhin gehören Angriffe auf die Kommunikationsschnittstellen zu dieser Klasse. Angriffe wie ARP-Poisoning können die Vertraulichkeit der Daten gefährden.

Ein oft nicht kalkuliertes Risiko gehen Benutzer ein, die mit Hilfe eines sog. „Jailbreaks“ die von Apple auferlegten Restriktionen umgehen wollen. Unter Ausnutzung einer Schwachstelle im Betriebssytem wird Quellcode zur Ausführung gebracht, der das Code Signing während des Bootvorgangs deaktiviert und die Systempartition dauerhaft mit Schreibrechten zur Verfügung stellt [7]. Standardmäßig wird während dieses Vorgangs ein SSH-Server installiert, der über alle Kommunikationsschnittstellen erreicht werden kann und mit einem Standardpasswort ausgestattet ist, so dass ein Zugriff auf das System und damit auf die Daten möglich ist.

Die Apple Anwendung iTunes erstellt vor einem Synchronisationsvorgang Backups, die im Dateisystem des PCs standardmäßig unverschlüsselt abgelegt werden. Damit stellt der Zugriff auf das Backup ebenfalls ein Risiko hinsichtlich Verfügbarkeit, Vertraulichkeit und Integrität der Daten dar.

4. Risikobewertung

Im Folgenden sollen die Bedrohungsszenarien hinsichtlich ihrer Eintrittswahrscheinlichkeit bewertet werden.

Hinsichtlich der Bedrohungsszenarien, die sich aus dem physikalischen Besitz des iPads ergeben, haben Verlust und Diebstahl des Gerätes eine hohe Eintrittswahrscheinlichkeit. Dabei kann die Dauer des unberechtigten Besitzes vernachlässigt werden, da mit Hilfe forensischer Methoden in kurzer Zeit ein Abbild des iPad-Dateisystems erstellt werden kann, so dass eine Auswertung zu einem späteren Zeitpunkt detailliert vorgenommen werden kann.

Die Umgehung verschiedener Sicherheitsmaßnahmen mit Hilfe eines Jailbreaks durch den Benutzer hat eine mittlere Eintrittswahrscheinlichkeit. Hier sind unterschiedliche Faktoren von Bedeutung: Einerseits sind das technische Interesse und das Know-how des Benutzers von Bedeutung. Andererseits sollten seitens des Unternehmens zur Verfügung gestellte Geräte auch nur zu dienstlichen Zwecken eingesetzt werden. Dennoch kann das Eintreten dieses Angriffs nicht ausgeschlossen und auch nicht unterbunden werden.

Der Zugriff auf sensible Daten durch Malware kann aufgrund der von Apple umgesetzten Maßnahmen wie Code-Signing und XN-Bit als mittleres Risiko betrachtet werden.

Das Risiko durch Angriffe gegen die Vertraulichkeit der Daten durch Techniken wie ARP-Poisoning ist aufgrund der einfachen Gegenmaßnahmen wie z.B. kryptographisch gesicherte Übertragung der Daten eher als gering zu betrachten.

Der Zugriff auf das Backup der Daten hat eine mittlere Eintrittswahrscheinlichkeit, da der Synchronisations-PC oftmals auch in verschiedenen Umgebungen genutzt wird und sein Sicherheitszustand das Risiko mit beeinflusst.

5. Empfehlungen zum Einsatz

In diesem Abschnitt sollen Maßnahmen beschrieben werden, die einen sicheren Einsatz des iPads gewährleisten.

Grundsätzlich sollte das iPad nur mit dem Betriebssystem iOS4 oder neuer Zugang zum Unternehmensnetz haben, da vom Hersteller selbst ältere Versionen nicht für einen Einsatz im Unternehmen empfohlen werden. Als Kommunikationsschnittstellen sollte das iPad über die WiFi- und 3G-Schnittstelle verfügen, um Updates der zentralen Konfigurationseinstellungen nicht nur bei Konnektivität zu einem WLAN installieren zu können.

Apple stellt kostenlos die „iPhone Configuration Utility“ zur Verfügung. Mit dieser Software können unter Windows- und Apple-Betriebssystemen Konfigurationsprofile erstellt werden. Konfigurationsprofile sind XML-Dateien, die komplette Geräte- oder Teilkonfigurationen enthalten können. Insbesondere können hier Einstellungen vorgenommen werden, die direkt am Gerät nicht zur Verfügung stehen. Per elektronischer Signatur können diese Konfigurationsprofile vor unbefugten Änderungen geschützt werden. Ebenfalls können die Profile gesperrt werden, was in der täglichen Benutzung bedeutet, dass der iPad-Benutzer das Profil nicht vom Gerät entfernen darf. Beides – elektronische Signatur und Sperrung eines Profils – wird daher empfohlen.

Eine Verteilung der Konfigurationsprofile kann bei einer sehr kleinen Anzahl der eingesetzten Geräte direkt per USB-Verbindung erfolgen. Bei größeren Zahlen bietet sich der Download von einem Web-Server oder die Zustellung per E-Mail an. Insbesondere per Microsoft Active Sync (Push-Mail) kann diese Methode bei vielen Systemen eingesetzt werden. Im Forschungszentrum Jülich bietet der Geschäftsbereich IT-Services (ITS) einen Download-Bereich[5] für Profile an. Zur Authentifizierung werden E-Mail-Benutzer-ID und Passwort genutzt.

Generell sollten alle konfigurierten Verbindungen durch SSL/TLS gesichert werden. Damit SSL/TLS Verbindungen sicher genutzt werden können, müssen die Stammzertifikate der PKI des Forschungszentrums Jülich hinterlegt werden. Erst dann können Zertifikate der entsprechenden Server validiert werden. Da das iPad standardmäßig L2TP-Over-IPSec und die IPSec-VPN-Lösung der Firma Cisco Systems unterstützt, beides auch im Forschungszentrum Jülich unterstützte Verfahren, sollte immer ein VPN-Profil existieren. Empfohlen wird die Verwendung der L2TP-over-IPSec-Lösung, da hier über öffentlich ungesicherte Netze alle Daten kryptographisch gesichert zum VPN-Endpunkt im Forschungszentrum übertragen werden, unabhängig von der konfigurierten VPN-Gruppe.

Das iPad sollte vom Benutzer zwingend mit einem Zugangspasswort versehen werden, welches der generellen Passwort-Policy des Unternehmens genügt. Das Konfigurationsprofil sollte die Anzahl der verwendeten Zeichen auf mindestens acht einstellen und die Verwendung von Zahlen, Buchstaben und Sonderzeichen erzwingen. Auch sollte die Lebensdauer des Passwortes eingestellt werden, z.B. 90 Tage, und eine Passworthistorie von mindestens 5 gespeichert werden, so

[5] https://itsprofiles.fz-juelich.de

dass die Wiederverwendung eines Passwortes für einen längeren Zeitraum ausgeschlossen wird. Ebenfalls sollte eingeschaltet werden, dass nach 10 fehlerhaften Eingaben des Passcodes alle Daten auf dem iPad gelöscht werden.

Die Funktionalität des iPads sollte so eingestellt werden, dass der Benutzer keine Apps aus dem Apple AppStore installieren kann, so dass nur getestete und für den Unternehmenszweck sinnvolle Anwendungen installiert werden können. Obschon Apple durch das praktizierte Code Signing nur geprüfte Applikationen zum Download bereitstellt, kann so die Installation von Anwendungen, die gezielt vertrauliche Informationen ausspähen, vermieden werden.

Erstellen von Bildschirmfotos kann zwar innerhalb des Konfigurationsprofils unterbunden werden, jedoch zeigen Anwenderstudien, dass diese Funktionalität häufig genutzt wird, um Informationen aus Apps per Mail zu versenden. Damit eine möglichst hohe Mobilität gewährleistet ist, sollte die Funktionalität nutzbar sein, aber vom Benutzer nur mit einem hohen Sicherheitsbewusstsein genutzt werden. Gänzlich unterbunden werden können die Screenshots nicht, da bei jeder Betätigung der sog. Home-Taste ein Bildschirmfoto erstellt wird, welches beim Applikationswechsel wieder eingeblendet wird.

Die Applikation iTunes sollte ebenfalls dem Verantwortungsbewusstsein des Benutzers anheim gestellt werden. Insbesondere im wissenschaftlich-universitären Umfeld bietet iTunes University eine Plattform zur Publikation wissenschaftlicher Ergebnisse und Erfahrungsberichte. Falls in einer zukünftigen Version der Konfigurations-Utility und des iOS-Betriebssystems einzelne iTunes-Bereich, z.B. der Music Store, deaktiviert werden können, sollte dieses Mittel genutzt werden.

Für den dienstlichen Gebrauch des iPads sollte die Applikation YouTube deaktiviert werden. Der Webbrowser Safari sollte zur Verfügung stehen, aber vor etwaigen Betrugsversuchen warnen. Der Pop-Up-Blocker kann aktiviert werden. JavaScript sollte aktiviert bleiben, da andernfalls die Usability vieler Web-Seiten in erheblichem Masse eingeschränkt würde.

WLAN-Zugangsprofile sollten so weit möglich vordefiniert werden. Im wissenschaftlichen Umfeld ist es ratsam, das WLAN „eduroam“ per Konfigurationsprofil zu installieren, da zum Einen die Konfigurationseinstellungen direkt am Gerät für den Benutzer schwierig ist und zum Anderen aber die mobile Konnektivität bei Besuchen unterschiedlicher Organisationen gegeben ist. Einstellungen für das interne WLAN im Forschungszentrum (sfzj) können nur dann vorgenommen werden, wenn der private Schlüssel zum zugehörigen Zertifikat verfügbar ist.

6. Nützliche Applikationen für den Unternehmenseinsatz

In diesem Abschnitt werden einige nützliche Applikationen für den Einsatz im Unternehmen vorgestellt.

Name	**Beschreibung**	**iTunes Link**
Pages	Textverabeitung von Apple	http://itunes.apple.com/de/app/pages/id361309726?mt=8
Numbers	Tabellenkalkulation von Apple	http://itunes.apple.com/de/app/numbers/id361304891?mt=8
Keynote	Präsentationssoftware von Apple	http://itunes.apple.com/de/app/keynote/id361285480?mt=8
iAnnotate PDF	PDF-Bearbeitung	http://itunes.apple.com/de/app/iannotate-pdf-kommentar/id363998953?mt=8
Calculator	Taschenrechner	http://itunes.apple.com/de/app/calculator-hd-for-ipad/id364905554?mt=8
DevInfo	Informationen zum System, wie laufenden Prozesse, offene Netzwerkports, IP-Adressen, Routing Informationen	http://itunes.apple.com/de/app/dev-info/id294217490?mt=8
iSSH	SSH-Client, inkl. X11-Support	http://itunes.apple.com/de/app/dev-info/id294217490?mt=8

7. Literaturhinweise

[1] iRisiko – Sicherheitsaspekte bei iPhone und iPad
Sackmann, R.
iX Special 3/2010

[2] Sicherheitsarchitektur beim Booten eines Geräts
ip.com/patapp/US20090257595

[3] iPhone Forensics Whitepaper
viaforensics.com/education/white-papers/iphone-forensics

[4] iPad Enterprise Overview
www.apple.com/de/support/ipad/enterprise
www.apple.com/support/ipad/enterprise

[5] iPad Security Overview
images.apple.com/de/ipad/business/pdf/iPad_Security_Overview.pdf

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

[7] iPhone Forensic Method FAQ
www.zdziarski.com/blog/?p=524