Jörg Völker

iPhone Security

Das iPhone von Apple gewinnt auch in Unternehmen zunehmend Anhänger und ist dabei, zum unmittelbaren Konkurrenten von Blackberry-Smartphones zu werden.[1] Der Beitrag gibt Auskunft über Sicherheitsmechanismen und Gefährdungen von Apples Smartphone.

Einleitung

In immer mehr Unternehmen kommen neben den klassischen Arbeitswerkzeugen wie Laptops und Notebooks verstärkt Smartphones zum Einsatz, die den Leistungsumfang eines Mobiltelefons mit dem eines Personal Digital Assistent (PDA) vereinen. Im Prinzip ist ein Smartphone also ein Mini-Computer, mit dem man unterwegs E-Mails und Dokumente bearbeiten und zusätzlich auch telefonieren kann.

Auf Grund seines Funktionsumfangs und hohen Bedienkomforts erfreut sich das von Apple Inc. stammende iPhone einer immer größeren Beliebtheit. Das wirft die Frage nach einer sicherheitstechnischen Bewertung auf, sowie die Frage, wie ein solches Endgerät in ein bestehendes Sicherheitskonzept für mobile Endgeräte eingebunden werden kann.

Grundsätzlich bietet das iPhone eine Reihe wesentlicher Sicherheitsfunktionen:

- So können beispielsweise Dateien (mit Ausnahme von Multimedia-Dateien) nicht direkt auf das iPhone übertragen werden;
- Anwendungen laufen in getrennten Sandboxen und können untereinander nur über definierte Schnittstellen Informationen austauschen;
- an den Passcode zum Freischalten des iPhones kann ein Fehlbedienungszähler gekoppelt werden, bei dessen Überschreitung sämtliche Benutzerdaten gelöscht werden;
- schließlich ist das iPhone mit einer Hardwareverschlüsselung ausgestattet (iPhone 3GS ab Betriebssystemversion 3.1), wodurch alle Benutzerdaten automatisch verschlüsselt auf dem Gerät gespeichert werden.

Dennoch weist das iPhone einige als kritisch einzustufende Sicherheitsschwachstellen auf, die bei der Entscheidung über einen Einsatz des Geräts im Unternehmen berücksichtigt werden sollten.

Jörg Völker

Security Consultant bei der Secorvo Security Consulting GmbH.Arbeitsschwerpunkte: Information Security Management, IT-forensische Analysen, Sicherheitsaudits.
E-Mail: joerg.voelker@secorvo.de

1 Security Features

Zu den zusätzlichen Funktionen des iPhones zählen insbesondere:

- Personal Information Management (PIM; z. B. E-Mail, Kalender, Kontakte)
- Mobiler Internetzugang
- Video- und Bildkamera
- Wireless Fidelity (Wi-Fi)
- Bluetooth
- Tethering
- Musik- und Videoplayer
- Voicerecorder

Über den Online-Shop der Firma Apple (App-Store) ist es möglich, eine Vielzahl kostenpflichtiger und kostenfreier Programme (im iPhone-Jargon Apps genannt) für das iPhone zu erwerben, auf das Gerät zu laden und auszuführen. Bereits heute gibt es über 185.000 solcher Apps[2], beginnend von Spielen über Navigationssoftware bis hin zu reinen Business-Anwendungen wie Online-Börsenkurse oder Lagerstandsverwaltung.

Mit der Einführung des iPhone 3GS stattete Apple das Smartphone mit einigen zusätzlichen Sicherheitsfeatures aus, die den Einsatz des iPhone im Unternehmensumfeld attraktiver gestalten sollen. Die wesentlichen Sicherheitsmerkmale sind:[3]

- **Gerätesicherheit**
  - *Passcode*: Das iPhone kann durch einen Passcode vor unberechtigter Nutzung geschützt werden. Die Verwendung eines Passcodes kann per Policy erzwungen werden, ebenso die Länge des Passcodes, die maximale Zahl erlaubter Fehlversuche, wie häufig der Passcode geändert werden muss und ob eine Passworthistory berücksichtigt werden soll.
  - *Automatische Sperrung*: Nach einer vordefinierten Zeit der Inaktivität kann das iPhone nur nach Eingabe des Passcodes benutzt werden.
  - *Geräteeinschränkungen*: Per Konfigurationsdatei kann bspw. festgelegt werden, welche Anwendungen ein Benutzer ausführen darf, ob ein Benutzer die Kamera verwenden kann und ob der Internet Browser oder YouTube genutzt werden dürfen.
- **Datensicherheit**
  - *Hardwareverschlüsselung*: Alle Benutzerdaten auf dem iPhone werden verschlüsselt abgelegt.
  - *Verschlüsselte Backups*: Benutzer haben die Möglichkeit, erstellte Backups der Benutzerdaten verschlüsselt zu erstellen.
  - *Local Wipe*: Nach Überschreitung einer eingestellten Anzahl an Fehlversuchen für die Passcodeeingabe werden sämtliche Benutzerdaten auf dem iPhone gelöscht.

1 Zur Sicherheit von Blackberry-Smartphones siehe Fox, DuD 11/2005, S. 647 ff.

2 http://www.heise.de/developer/artikel/Was-man-beim-Entwickeln-von-iPhone-Apps-wissen-sollte-1000264.html (21.05.2010)

3 Teilweise wird für die Aktivierung mancher Sicherheitsfunktionen ein zusätzliches Programm der Firma Apple benötigt.

- *Remote Wipe*: Apple bietet über den kostenpflichtigen Zusatzdienst „Mobile Me“ (Jahresbeitrag 79 € je iPhone) die Dienste „Mein iPhone suchen“ und „RemoteWipe“ an. Damit kann man ein abhanden gekommenes iPhone lokalisieren und bei Bedarf alle Benutzerdaten aus der Ferne löschen.
- *Sichere Gerätekonfigurationsdatei*: Alle notwendigen Geräteeinstellungen (wie Passcode-Policy, Wi-Fi-Einstellungen, VPN-Einstellungen etc.) können in einer Gerätekonfigurationsdatei zusammengefasst werden. Die Gerätekonfigurationsdatei kann verschlüsselt und gegen unberechtigte Änderungen geschützt werden.

- **Netzwerksicherheit**
  - *Sicherer Netzwerkzugang*: Mehrere Protokolle ermöglichen einen sicheren Zugang zum Unternehmensnetzwerk, wie VPN-Protokolle (Cisco IPSec, L2TP, PPTP), SSL/TLS (X.509-Zertifikate), WPA/WPA2 (802.1x-Unterstützung), Zertifikats-basierte Authentifikation, Unterstützung von RSASecurID und CRYPTOCard.
- **Plattformsicherheit**
  - *Runtime protection*: Apps auf dem iPhone werden in einer sogenannten „Sandbox“ ausgeführt. Dies sorgt dafür, dass Apps nicht auf gespeicherte Daten anderer Apps zugreifen können. Zusätzlich sind alle Systemdateien und Ressourcen sowie der eigentliche Kernel des iPhones vom Benutzerdatenbereich abgetrennt und auch physikalisch auf einer dedizierten Partition abgelegt. Zugriffe auf Systemdateien und –ressourcen sowie auf gespeicherte Daten sind nur über dedizierte, durch das Betriebssystem zur Verfügung gestellte Application Programming Interfaces (APIs) möglich.
  - *Code Signierung*: Applikationen, die auf dem iPhone ausgeführt werden sollen, müssen digital signiert sein. iPhone-Standardapplikationen sind von Apple signiert. Apps von Drittherstellern müssen durch den Hersteller mit einem von Apple herausgegebenen Zertifikat signiert sein.

3 Gefährdungspotential

Trotz der in Abschnitt 2 aufgeführten Sicherheitsmerkmale birgt der Umgang mit dem iPhone im Unternehmensumfeld einige Gefahren. So begrenzt das iPhone zwar den direkten Zugriff auf bestimmte Bereiche und Inhalte der Benutzerdaten über die Bedienoberfläche. Allerdings lassen sich fast alle Sicherheitsfunktionen des iPhones mit etwas Kenntnis umgehen. Die hier beschriebenen Probleme betreffen Stand alle heute verfügbaren iPhone Modelle und Firmwareversionen (aktuelle Firmwareversion 3.1.3).

3.1 Gefährdungseinstufung

Zur Beurteilung der realen Gefährdung sollten unterschiedliche Angreiferklassen unterschieden werden (siehe Tabelle 1).

Tabelle 1 | Angreiferklassen

Angreifer-klasse	Beschreibung
Typ I	Bei diesem Angreifer-Typ handelt es sich um einen iPhone-Nutzer, der bewusst oder unbewusst einen Schaden verursacht
Typ II	Hierbei handelt es sich um einen Angreifer, der über kein bzw. nur geringes Know-How verfügt, und dem nur sehr limitierte Ressourcen zur Verfügung stehen
Typ III	Hierbei handelt es sich um einen Angreifer, der über hohes bis sehr hohes Know-How verfügt, und dem erweiterte Ressourcen zur Verfügung stehen

Die Einstufung des Gefährdungspotentials erfolgt in den Stufen „gering“, „mittel“ und „hoch“. Dieser sehr generische Ansatz ersetzt keine unternehmensbezogene Risikobewertung bei der Frage des Einsatzes von iPhones, da die potentiellen Schadensauswirkungen je nach Einsatzzweck und Unternehmen sehr unterschiedlich ausfallen.

3.2 Informationen auf dem iPhone

Neben den PIM-Daten speichert das iPhone auch eine Vielzahl zusätzlicher, für den Anwender nicht direkt einsehbarer Daten, die durchaus eine hohe Sensitivität besitzen können. Hierzu zählen:

- *Tastatur Cache*: Hier speichert das iPhone fast alle Tastatureingaben, darunter auch Benutzernamen, Passwörter, Suchbegriffe und Fragmente tastaturbasierter Kommunikation (z. B. SMS-Eingaben), die selbst nach einem Löschen noch ausgelesen werden können.
- *Screenshots*: Wenn der Home Button gedrückt wird, wird der letzte Status einer aktiven Applikation als Bild gespeichert.
- *Gelöschte Bilder* aus der Bildergalerie des Benutzers, der Kamera oder dem Browser Cache.
- *Gelöschte Einträge* aus dem Adressbuch.
- *Vollständige Anruferlisten* ausgehender und eingehender Anrufe der letzten 100 Telefonate.
- *Kartenausschnitte* der Google Maps App, inklusive Streckeninformationen und GPS-Koordinaten.
- *Browser Cache* und gelöschte Browser Objekte.
- Gecachte und gelöschte *E-Mail-Nachrichten, SMS* und Daten aus anderen Kommunikationsverbindungen.
- Gelöschte *VoiceMail-Nachrichten*.
- *Pairing Informationen* von Verbindungen des iPhones mit einem oder mehreren Computern (z. B. Bluetooth-Passworte).

Viele dieser Informationen werden auch noch längere Zeit auf dem Gerät vorgehalten, wenn der Benutzer diese gelöscht zu haben glaubt. Über forensische Analysen (siehe Abschnitt 4.4) können solche Informationen wieder hergestellt und lesbar gemacht werden.

3.3 Backup-Benutzerdaten

Über iTunes, das zentrale Desktop-Verwaltungstool von Apple für das iPhone, kann ein Anwender ein Backup sämtlicher Benutzerdaten erstellen und auf einem Computer speichern. Das Backup ist per Default nicht verschlüsselt. Eine Verschlüsselung erfolgt nur, wenn der Benutzer diese Option explizit aktiviert.

Unverschlüsselte Backup Daten können durch entsprechende Tools[4] ausgelesen werden. So kann beispielsweise auf SMS-Nachrichten, Anruferlisten, das Adressbuch und Adressbuch-Bilder, Notizen und Kalendereinträge zugegriffen werden. Da ein Anwender prinzipiell die Möglichkeit hat, auch auf anderen Computern außer seinem Dienstgerät ein solches Backup zu erstellen[5], könnten Daten so unkontrolliert nach Außen abfließen. Ein unberechtigter Externer muss dazu aber Zugriff auf das Backup erlangen.

Das Gefahrenpotential durch „unerlaubte“ Backups ist allerdings als gering einzustufen, da ein Zugriff auf das Backup der Daten immer einen Zugriff auf das Backup-Medium erfordert.

4 Zum Beispiel: MDBackup Extract.

5 Siehe http://www.andrewgrant.org/2008/03/30/how-to-sync-an-iphone-with-two-or-more-computers.html (21.05.2010).

3.4 Local / Remote Wipe

Durch Remote Wipe soll einem Anwender bzw. einem Administrator die Löschung von Benutzerdaten möglich sein, auch wenn er keinen direkten Zugriff mehr auf ein iPhone hat, falls dieses z. B. gestohlen wurde. Remote Wipe setzt jedoch voraus, dass das Gerät an das Unternehmensnetzwerk angeschlossen bzw. eine SIM-Karte eingelegt und aktiv ist. Bei einem gestohlenen iPhone ist jedoch davon auszugehen, dass die SIM-Karte entfernt wurde und das iPhone auch keinen Kontakt mehr zum Unternehmensnetzwerk herstellen kann. Der Nutzen der Sicherheitsfunktion Remote Wipe muss daher als eher gering eingestuft werden.

Die Local Wipe Funktion ermöglicht es, alle Benutzerdaten des iPhones nach einer bestimmten Anzahl falscher Passcode-Eingaben zu löschen. Diese Sicherheitsfunktion ist unabhängig von dem Vorhandensein einer SIM-Karte bzw. einer bestehenden Netzwerkverbindung zum Unternehmensnetz. Passcode und Local Wipe schützen aber nur vor Angreifern mit geringen Kenntnissen, denn Angreifer mit einem soliden Basiswissen können die Sicherheitsfunktionen umgehen (siehe hierzu Abschnitt 3.5). Das Gefährdungspotential durch Diebstahl muss als „mittel" bis „hoch" eingestuft werden.

3.5 Umgehung von Passcode und Verschlüsselung

Auch wenn ein iPhone zusätzlich zur hardware-basierten Geräteverschlüsselung durch einen Passcode und Local Wipe geschützt ist, ist es einem Unberechtigten möglich, sämtliche Daten des iPhones auszulesen, sofern er physischen Zugriff auf das Gerät erhält.

Jonathan Zdziarski hat in einem Interview mit „Wired"[6] ein entsprechendes Verfahren beschrieben, das für alle iPhone Modelle 2G, 3G und 3GS mit den Firmwareversionen 1.0 bis 3.1.2 angewendet werden kann.[7] In seinem Buch „iPhone Forensics" zeigt er, wie Daten aus einem iPhone 2G/3G beweissicher kopiert werden können. Und auch beim iPhone 3GS ist eine solche „Sicherung" der Benutzerdaten möglich, ohne dass dazu ein so genannter „Jailbreak" (siehe Abschnitt 3.7) oder ein Brechen der Verschlüsselung notwendig wäre.

Die Sicherung der Daten erfolgt in einem zweistufigen Verfahren: Im ersten Schritt wird das iPhone von einer RAM-Disk aus gebootet, in einem zweiten Schritt wird dann die Partition (MAC OS Dateisystem HFS, Hierarchical File System) mit den Benutzerdaten als Raw-Disk-Image gesichert. Das iPhone entschlüsselt bei diesem Vorgang alle Benutzerdaten automatisch – ohne dass dazu die Eingabe des Passcodes erforderlich wäre.

Das so erstellte Raw-Disk-Image kann anschließend unter Mac OS eingebunden oder mit gängigen Forensik-Tools (bspw. FTK, X-Ways, ...) analysiert werden.

Auf diese Weise lassen sich fast sämtliche in Abschnitt 3.2 genannten Daten rekonstruieren. Außerdem ist es auf diesem Weg möglich, das iPhone mit einer modifizierten Firmware zu versehen, ohne dass das einem Anwender ersichtlich wäre. Auf diese Art und Weise kann es einem Angreifer gelingen, auf Dauer Zugang zum iPhone (über Netzwerkverbindungen) und so u. U. auch Zugriff auf das Unternehmensnetzwerk zu erhalten. Insgesamt wird das Gefährdungspotential durch diesen Angriff als „hoch" eingestuft.

3.6 Datensammlung durch Apps

Durch den iTunes Store von Apple können Anwender auf über 185.000 unterschiedliche konstenpflichtige und kostenlose Apps zugreifen und diese auf einem iPhone installieren. Viele dieser Apps leiten dabei Benutzerinformationen an die Firma Pinchmedia weiter, die daraus Statistiken z. B. zur Nutzungshäufigkeit und -dauer erstellt.[8]

Dass und welche Daten die iPhone Apps übermitteln, ist für einen Anwender nicht erkennbar. Das ist vergleichbar mit dem Dienst Google Analytics[9], der das Verhalten von Webseitenbesuchern an Google übermittelt, das daraus Webanalysen für das die Webseite betreibende Unternehmen durchführt. Die an Pinchmedia übermittelten Daten sind jedoch weit kritischer. So können die ID-Nummer des Geräts, das Geburtsdatum des Nutzers (falls Facebook genutzt wird) und sogar der aktuelle Standort als Geokoordinate darunter sein. Um Zustimmung zu dieser Übermittlung werden Nutzer von den wenigsten Apps gebeten – nach Ansicht von Pinchmedia genügt dazu die allgemeine Nutzervereinbarung von Apple. Mit diesen Daten lassen sich detaillierte Benutzer- und Bewegungsprofile erstellen und auswerten. Insgesamt wird das Gefährdungspotential durch diesen Angriff als „mittel" eingestuft.

3.7 iPhone Jailbreak

Unter einem iPhone Jailbreak versteht man das Aufspielen einer modifizierten Firmware auf das iPhone, um die Bindung des iPhones an den Apple iTunes Store aufzulösen. Auf einem iPhone mit Jailbreak lassen sich eine Vielzahl von Funktionen des iPhone Betriebssystems nutzen, die in der Regel deaktiviert sind, und lassen sich iPhone-Applikationen installieren, die nicht im Apple iTunes Store verfügbar sind (wie z. B. ein Secure Shell Server). Ein Jailbreak lässt sich Stand auf allen heute verfügbaren iPhone Modellen bis einschließlich der derzeit aktuellen Firmwareversion 3.1.3 durchführen. Auch für das neue iPad mit Firmwareversion 3.2 sowie die für den Herbst angekündigte Firmwareversion 4.0 (bis dato nur als Beta Version veröffentlicht) wurden Jailbreaks demonstriert.

Welche Applikationen auf solchen Jailbreak iPhones installiert werden und welche Sicherheitsrisiken dadurch entstehen, lässt sich nicht abschätzen. Allerdings wurden schon die ersten erfolgreichen Angriffe auf Jailbreak iPhones bekannt.[10] Erschwerend kommt hinzu, dass für die Durchführung eines Jailbreaks nur geringe bis mittlere Kenntnisse notwendig sind. Abhängig von den anschließend installierten Applikationen kann dadurch eine Gefährdung des gesamten Unternehmensnetzwerks entstehen. Insgesamt wird das Gefährdungspotential durch diesen Angriff als „hoch" eingestuft.

3.8 Malicious Code

Für einen Anwender ist es sehr einfach, über den iTunes Store eine große Zahl an Apps auf seinem iPhone zu installieren. Die Apps laufen zwar prinzipiell in einer „Sandbox" (s. o.) und durchlaufen eine zumindest rudimentäre Prüfung durch

6 Siehe http://www.wired.com/gadgetlab/2009/07/iphone-encryption (21.05.2010).

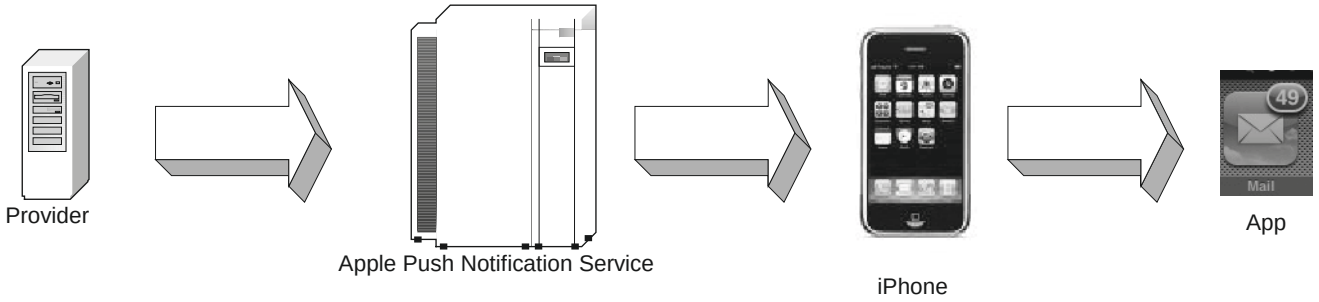
7 Siehe http://www.iphoneinsecurity.com/ (21.05.2010).

8 Siehe Secorvo Security News 08/2009 http://www.secorvo.de/security-news/.

9 Siehe http://www.google.com/intl/de/analytics/ (21.05.2010).

10 Siehe http://www.heise.de/newsticker/meldung/ohshit-neues-Passwort-auf-dem-iPhone-866291.html (21.05.2010).

Abbildung 1 | APNS Architektur



Apple, bevor sie in den AppStore eingestellt werden. Allerdings können sie über API-Schnittstellen auf andere Daten zuzugreifen. So ist es möglich, dass auf diesem Wege sensitive Informationen aus dem Gerät ausgelesen werden.

Beispielhaft sei hier das Funambol App[11] genannt: Mit diesem App ist es möglich, die Kontaktdaten des iPhones auf einem externen Funambol-Server zu speichern und mit anderen Geräten zu synchronisieren. Insgesamt wird das Gefährdungspotential durch diesen Angriff als „hoch" eingestuft.

3.9 Apple Push Notification Service

Unter dem Apple iPhone OS können Applikationen nicht parallel ausgeführt werden. Dies führt dazu, dass auf einem Server wartende Informationen für einen Anwender bzw. eine Anwendung nicht aktiv durch die Applikation abgerufen werden können, sofern das Programm nicht ausgeführt wird. Sinnvoll wäre solch ein Abrufmechanismus zum Beispiel für ein E-Mail-Programm, das einen Anwender über auf dem Server neu eingetroffene E-Mails selbst dann informieren könnte, wenn das E-Mail-Programm nicht aktiv ist. Apple begründet diese Einschränkung damit, dass die Belastungen für Performance und Batterie erheblich steigen würden, wenn mehrere Programme im Hintergrund regelmäßig Daten von einem Server abrufen würden.

Um diese Einschränkungen zu umgehen, hat Apple mit Version 3 des iPhone OS den Apple Push Notification Service (APNS) eingeführt. Informationen, die für einen Anwender bzw. eine Anwendung auf einem Server bereitstehen, können damit aktiv vom Server an das iPhone übertragen werden. Die grundlegende Architektur für APNS beinhaltet drei Komponenten:

- Den Server, der die Informationen für den Anwender bzw. die Anwendung zur Verfügung stellt, kurz Provider genannt,
- das Push Gateway, welches von Apple betrieben wird und die Daten vom Provider übernimmt und an das iPhone weiterleitet und
- das iPhone samt dazugehöriger App, das durch das Push Gateway kontaktiert wird und die Daten entgegen nimmt.

Abbildung 1 gibt einen Überblick über die grundlegende APNS Architektur.

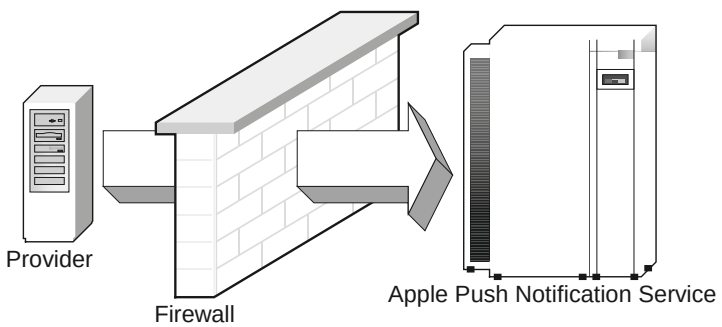
Wie in Abbildung 1 dargestellt, erfolgt der Informationsfluss bei APNS immer nur in eine Richtung, vom Provider zum iPhone. Der Provider kontaktiert hierzu den APNS Server „gateway.push.apple.com" auf Port 2195. Die Verbindung vom Provider zum APNS Gateway sowie vom APNS Gateway zum iPhone ist per SSL/TLS geschützt.

APNS identifiziert das zu kontaktierende iPhone über ein sogenanntes „device token", das der Provider samt der eigentlichen Information („payload") an APNS übergeben muss. Sowohl der Provider als auch das iPhone müssen am APNS registriert sein. Der sogenannte „payload" kann dabei vom folgenden Typ sein:

- *Badges*: „Anstecker"-Symbole (siehe Abbildung 1, Mail App). Hier wird über das Programmicon symbolisch dargestellt, wie viele neue Nachrichten auf den Nutzer warten.
- *Tonmeldungen*: Es können akustische Signale übermittelt werden, um den Benutzer zu benachrichtigen.
- *Text-Popups*: Es können Textnachrichten definiert werden, die auf dem Bildschirm des iPhone erscheinen. Zudem kann über Buttons beispielsweise das entsprechende Programm sofort gestartet werden.

Sollte APNS die Informationen dauerhaft nicht an das Zielgerät übermitteln können oder das Zielgerät die Annahme der Informationen ablehnen (z. B. weil die Zielapplikation durch den Anwender deinstalliert wurde), speichert APNS pro Service eine Liste der Geräte, die nicht beliefert werden konnten. Der Provider hat die Möglichkeit, diese Liste über das Gateway

Abbildung 2 | Kommunikation Provider – APNS



11 Siehe http://www.funambol.com/solutions/iphone.php (21.05.2010).

„feedback.push.apple.com“ (Port 2196) abzurufen.[12]

Zur Beurteilung des Gefährdungspotentials durch APNS müssen zwei Aspekte betrachtet werden:

- Welche Gefährdungen bestehen bei der Kommunikation zwischen Provider und APNS?
- Welche Gefährdungen bestehen bei der Kommunikation zwischen APNS und iPhone?

Kommunikation Provider und APNS

In der Regel dürfte der Provider Service in der DMZ eines Unternehmens angesiedelt und durch eine Firewall geschützt sein (siehe Abbildung 2).

Damit die Kommunikation erfolgen kann, müssen auf der Firewall die Ports 2195 und 2196 für ausgehende Verbindungen geöffnet werden. Sofern möglich sollten die Verbindungen eingeschränkt werden auf die Server „gateway.push.apple.com“ und „feedback.push.apple.com“. Da die Verbindung nur durch den Provider initiiert und die Kommunikation per SSL/TLS geschützt werden kann, wird die Gefahr für das interne Netzwerk als „gering“ und somit als unbedenklich eingestuft.

Kommunikation APNS und iPhone

Die Kommunikation zwischen APNS und iPhone erfolgt verschlüsselt und ebenfalls uni-direktional vom APNS zum iPhone. Derzeit sind keine Angriffe über APNS bekannt, wodurch sich Informationen auf einem iPhone durch Push Notification auslesen lassen könnten. Allerdings wurde eine Designschwäche von APNS publik, die dazu führt, dass Notifications für ein Zielgerät auf einem Fremdgerät angezeigt werden.[13] Dennoch wird das Gefährdungspotential aufgrund bislang wenig bekannter Angriffe bzw. Fehler als „gering“ eingestuft.

4 Empfehlungen

Zur Verringerung der in Abschnitt 3 beschriebenen Gefährdungen beim Einsatz des iPhone im Unternehmensumfeld sollte die Umsetzung der in den folgenden Abschnitt beschriebenen Sicherheitsmaßnahmen in Erwägung gezogen werden.

Zur Erstellung und Ausbringung der entsprechenden Gerätekonfigurationen kann das von Apple zur Verfügung gestellte iPhone-Konfigurationsprogramm[14] verwendet werden.

Abbildung 3 | Passcode Einstellungen

4.1 Allgemeine Einstellungen

Prinzipiell sollten folgende Grundsätze beachtet werden:

- Sofern möglich, sollten alle Geräte auf die gleiche Firmware-Version gebracht werden.
- Alle Geräte sollten mit einer einheitlichen Gerätekonfiguration ausgestattet werden.
- Dem Endanwender sollte nicht erlaubt werden, die Konfiguration zu ändern.

4.2 Passcode Einstellungen

Die Einstellungen für den Passcode sollten sich generell an den allgemeinen Vorgaben für die Verwendung von Passwörtern im Unternehmen orientieren. Sofern keine zusätzlichen Sicherheitsmaßnahmen getroffen werden (siehe Abschnitt 4.3) werden die in Abbildung 3 zusammengefassten Einstellungen empfohlen.

4.3 Einsatz zusätzlicher Sicherheitssoftware

In Abhängigkeit von der Sensitivität der Daten, die auf dem iPhone gespeichert werden, sollte zusätzliche Sicherheitssoftware eingesetzt werden.

So bietet zum Beispiel die Firma Sybase mit ihrem Produkt iAnywhere Mobile Office eine Client-Server-Infrastruktur, um E-Mails, Personal Information Management und Geschäftsprozesse auf mobile Umgebungen zu erweitern. Über den iAnywhere Mobile Office Server werden E-Mails und PIM-Daten sicher, d. h. verschlüsselt auf den iAnywhere Mobile Office iPhone Client übertragen. Die iPhone Mobile Office Client Anwendung läuft dabei in einer „Sandbox“ (siehe oben) und speichert E-Mails und Kalendereinträge zusätzlich zur iPhone Hardwareverschlüsselung verschlüsselt ab.

12 Apple Push Notification Service Programming Guide, Networking & Internet, Apple Inc.

13 Siehe http://www.benm.at/2009/07/21/sicherheitsrisiko-push-notifications-mit-hacktivated-iphones/ (21.05.2010).

14 Siehe http://www.apple.com/de/support/iphone/enterprise/ (21.05.2010).

Abbildung 4 | Einstellungen für Programme und Inhalte

4.4 Einschränkungen für Programme und Inhalte

Bevor ein iPhone App im Apple App-Store angeboten wird, durchläuft das App einen Zulassungsprozess bei Apple. Welche konkreten Zulassungskriterien und Prüfungen Apple dabei zu Grunde legt, ist für einen Endanwender nicht transparent. Auf Grund der immensen Flut an iPhone Apps muss davon ausgegangen werden, dass keine ausreichende Sicherheitsprüfung für jedes einzelne App durchgeführt wird. Es ist also durchaus möglich, dass ein Schadprogramm selbst über den Apple App-Store angeboten werden könnte.[15]

Es sollte deshalb geprüft werden, ob nur Apps verwendet werden, die durch das Unternehmen selbst erstellt wurden bzw. eine interne Zulassung durchlaufen haben und eine entsprechende digitale Signatur tragen.[16]

Die in Abbildung 4 zusammengefassten Einstellungen für Programme und Inhalte werden empfohlen.

Die Verwendung des iTunes Music Stores sowie von YouTube sollte sich an den Erfordernissen der Anwender orientieren.

4.5 Wireless Fidelity Einstellungen

Für den Zugang zum Unternehmensnetzwerk per Wireless LAN werden folgende Einstellungen empfohlen:

- Wi-Fi Verbindungen sollten nur mit starker Verschlüsselung erfolgen.
- Zur Identifizierung der Anwender sollten digitale Zertifikate verwendet werden.
- Sofern möglich, sollte der Zugang ins Unternehmensnetzwerk über dedizierte VLANs erfolgen.

4.6 VPN Konfiguration

Für den Remote-Zugang zum Unternehmensnetzwerk per Wireless LAN werden folgende Einstellungen empfohlen:

- Identifizierung der Anwender per RSA-SecureID oder digitale Zertifikate.
- Sofern digitale Zertifikate verwendet werden, sollte die Verwendung einer Benutzer-PIN erzwungen werden.
- Bei PPTP-Verbindungen sollte starke Verschlüsselung aktiviert werden.

5 Schlussbemerkung

Bei der Umsetzung und Ausprägung der Maßnahmen (beispielsweise hinsichtlich der Länge und Komplexität der Passwörter oder der Einschränkung der installierten Apps) bewegt man sich im klassischen Spannungsdreieck zwischen Benutzerfreundlichkeit (Usability), Administrierbarkeit (Operability) und Sicherheit (Security).

Hier gilt es zwischen Nutzen und Bequemlichkeit für Endanwender, Aufwand und damit Kosten für die Verwaltung der Endgeräte und Erfüllung der Sicherheitsanforderungen abzuwägen.

Grundlage für die Umsetzung und Ausgestaltung der in Abschnitt 4 empfohlenen Maßnahmen bildet dabei die Sensitivität der auf dem iPhone gespeicherten Informationen, sowie das aus dieser Sensitivität abgeleitete Risiko, das mit einer Gefährdung von Vertraulichkeit, Integrität oder Verfügbarkeit dieser Informationen verknüpft ist. Für die Bestimmung des Risikos ist es notwendig, anhand einer Informationsklassifizierung (bspw. öffentlich, intern, vertraulich, streng vertraulich) das Schadenspotential bei Eintritt einer Gefährdung zu bestimmen. Damit lässt sich die Angemessenheit der umzusetzenden Maßnahmen überprüfen.

Die konkreten Maßnahmen sollten sich dabei an der generellen Sicherheitsstrategie des Unternehmens orientieren und dem bestehenden bzw. angestrebten Sicherheitsniveau für Informationssicherheit genügen.

Erst auf der Grundlage einer solchen Risikobetrachtung kann begründet entschieden werden, bestimmte Risiken zu tragen oder Schutzmaßnahmen auch unter Inkaufnahme eines erhöhten Administrationsaufwands oder einer Einschränkung der Nutzung oder Bedienungsbequemlichkeit umzusetzen.

15 Siehe auch http://www.heise.de/newsticker/meldung/Sicherheitsforscher-warnt-vor-iPhone-Schurkenprogrammen-879245.html (21.05.2010).

16 Details hierzu: http://developer.apple.com/iphone (21.05.2010).