Trends in de beveiliging van mobiele apparaten

Waar bedrijven zich bewust van moeten zijn

M.R.A.M. Smeets MSc CISSP CISA
is adviseur bij KPMG IT Advisory en voert zowel IT-audits als ethical hacking opdrachten uit. Als enthousiaste gebruiker van mobiele apparaten van de nieuwe generatie en zijn interesse in de beveiliging van IT, is hij sinds het opkomen van deze nieuwe generatie druk bezig geweest met de beveiliging en het omzeilen van de beveiliging van deze mobiele apparaten. Denk hierbij aan infrastructuur reviews, audits en penetratietesten op de gehele ketens van iPhones en iPads in bedrijfsomgevingen.

smeets.marc@kpmg.nl

Marc Smeets MSc CISSP CISA

De introductie van een nieuwe generatie mobiele apparaten, onder aanvoering van Apple (met de iPhone) en Google (met het Android-systeem), heeft het gebruik van mobiele telefoons binnen en buiten het bedrijfsleven ingrijpend veranderd: nieuw, modern, mooi vormgegeven, altijd verbonden met het internet en legio Apps voor allerlei functies. Bovendien lijkt de iPad van Apple het succes van de iPhone te herhalen en is deze vinding bezig een breed segment van de zakelijke markt te veroveren, waardoor ook binnen het bedrijfsleven een lucratieve markt ontstaat voor tablet-pc's.
Het gebruik van deze nieuwe mobiele apparaten past geheel bij de huidige tijd en het is dan ook niet meer dan logisch dat deze apparaten een weg vinden naar de bedrijfsomgevingen. Productieverhogend en communicatie vergemakkelijkend zijn de positieve effecten van deze ontwikkeling. Maar er kleven ook risico's aan. En doordat de fabrikanten maar wat graag aangeven dat hun producten op-en-top veilig kunnen zijn, zijn deze risico's niet altijd even duidelijk. In dit artikel zal ik de voornaamste verschillen met traditionele apparaten bespreken, aanstippen waar de beveiligingsrisico's liggen en oplossingen aandragen voor de aanpak van deze risico's.

Inleiding

Het ontwerp van deze nieuwe generatie mobiele apparaten verschilt op twee belangrijke punten fundamenteel van dat van de vorige generatie 'smart phones'. Ten eerste beschikken zij over een veel grotere functionaliteit en ten tweede is er sprake van zogenaamde consumerization van dergelijke apparaten.

In het onderstaande wordt uitgebreid ingegaan op deze twee punten van verschil. Vervolgens komt aan de orde met welke nieuwe beveiligingsrisico's rekening gehouden dient te worden en meer in detail de achtergrond van deze risico's die ontstaan in de basissystemen van deze apparaten maar ook in de Apps. Als laatste wordt besproken welke set aan beveiligingsmaatregelen bestaat om de risico's te beperken.

Veel grotere functionaliteit

Dankzij de voortdurende verbetering van de hardware hebben deze apparaten nu enorme rekenkracht, vergelijkbaar met die van desktopcomputers van enkele jaren geleden. Hierdoor hoeven geen unieke besturingssystemen[1] ontwikkeld te worden; producenten kunnen hun apparaten baseren op bestaande besturingsystemen voor pc's. Het iOS-systeem van Apple is afgeleid van haar Mac OS X-besturingssysteem voor het Macintosh-platform. Het Android-besturingssysteem van Google is afgeleid van het open source besturingssysteem Linux. Er zijn wel enkele aanpassingen gemaakt aan het onderliggende besturingssysteem voor verbeterd mobiel gebruik. Deze aanpassingen zijn vooral gericht op het efficiënter omgaan met stroom om een vermindering van het batterijverbruik te realiseren, het verwijderen van functionaliteiten die op een mobiele telefoon geen nut hebben (zoals het ondersteunen van randapparatuur) en de toepassing van gebruikersinterfaces die met de vingers bediend kunnen worden in plaats van met een muis. Desondanks zijn de kern van het besturingssysteem en alle bijbehorende functionaliteit behouden, waardoor er op mobiele telefoons een enorm scala aan applicaties gebruikt kan worden. Hierdoor kun je dezelfde browser, Google Maps, chat-applicatie en applicaties voor het delen van bestanden[2] gebruiken als op je desktop.

Op mobiele telefoons kan een enorm scala aan applicaties worden gebruikt

Deze integratie van besturingssystemen werpt nu ook z'n vruchten af voor de desktop-pc's. Functionaliteiten die groot zijn geworden op het mobiele platform vinden hun weg naar de desktop-pc's. Denk hierbij aan de App store die Apple ook aanbiedt voor Mac OS X.[3] Maar bijvoorbeeld ook aan de voortgaande optimalisatie van webbrowsers op mobiele apparaten die zorgt voor snellere versies van dezelfde webbrowsers op de desktop-pc's. Er vindt dus een wederzijdse beïnvloeding plaats.

Tevens is, dankzij de vooruitgang in de mobiele connectiviteit (denk aan 3G-technieken zoals UMTS), de internetverbinding van deze apparaten effectiever en efficiënter geworden en zijn ook andere interactieve verbindingen zoals GPS en draadloos netwerken mogelijk. Vaak staan de applicaties op deze mobiele apparaten dan ook continu in verbinding met het internet. Zo kun je er bijvoorbeeld voor kiezen om je muziek niet langer op je mobieltje op te slaan maar uit de cloud te streamen.[4]

De ontwikkelingen staan dus zeker niet stil. En de mobiele apparaten ontpoppen zich dan ook tot volwaardige mobiele computers waarmee de meest voor de hand liggende taken kunnen worden uitgevoerd.

'Consumerization' van de mobiele apparaten

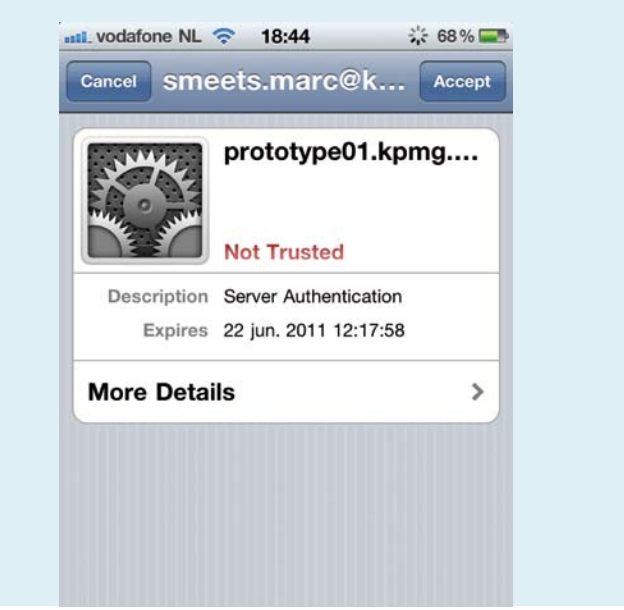
De scheiding tussen zakelijk en privé wordt minder strikt en de technische middelen die deze apparaten bieden, scheppen een omgeving waarbij dit nog meer wordt gefaciliteerd. De nieuwe generatie mobiele apparaten is namelijk ontworpen met het oog op de individuele consument in plaats van de zakelijke markt. Bovendien zijn de producenten en leveranciers er bijzonder goed in geslaagd om deze apparaten aan te prijzen als 'must haves'.

Het hoeft daarom geen verbazing te wekken dat veel werknemers liever gebruikmaken van hun eigen mobieltje, dat meer mogelijkheden heeft en er leuker uitziet, dan van de telefoon van de zaak. In plaats van één apparaat voor hun zakelijke en een ander voor hun privécommunicatie, gebruiken ze liever voor allebei het nieuwste en meest gebruiksvriendelijke apparaat. Dat dit vaak het apparaat is dat is bedoeld voor de reguliere consument en dat deze apparatuur zo ook in de bedrijfsomgeving belandt, noemen we 'consumerization'. Als gevolg hiervan raakt de privécommunicatie van de gebruiker, zoals interactie op sociale media, privégesprekken, sms'jes en web browsing, verweven met bedrijfsinformatie zoals zakelijke e-mails, documenten (ontvangen, aanpassen en versturen) en telefoonverkeer.

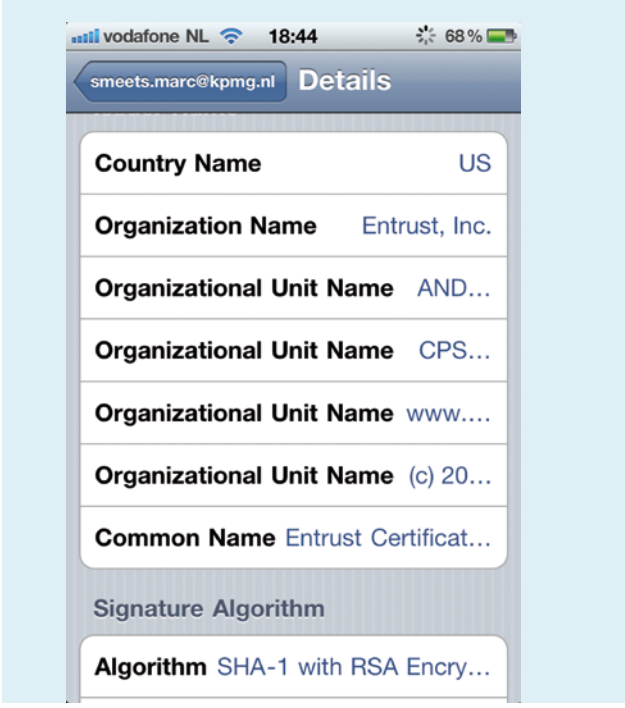
Nieuwe mogelijkheden gaan gepaard met nieuwe risico's

Deze nieuwe mobiele apparaten kunnen dus meer en we gebruiken ze daarom steeds vaker, ook zakelijk. Is dat erg? De nieuwe mogelijkheden van deze apparaten brengen aanzienlijke nieuwe veiligheidsrisico's met zich mee, vooral op het vlak van de technische beveiliging en vertrouwelijkheid van gevoelige persoonlijke en bedrijfsinformatie. Doordat deze apparaten zijn gebaseerd op standaardbesturingssystemen en een enorm scala aan

1 Een besturingssysteem, in het Engels operating system, is het geheel van programmatuur dat in het geheugen van de computer wordt geladen na het opstarten. Deze programma's bieden samen de functionaliteit om andere programma's uit te voeren.
2 Dropbox, een programma om bestanden tussen apparaten te delen, http://www.dropbox.com/iphoneapp.
3 Mac Store, een App Store voor Mac OS X http://www.apple.com/nl/mac/app-store/.
4 Spotify, een programma om streaming muziek te luisteren http://www.spotify.com/int/blog/archives/2009/07/27/spotify-for-iphone/.



Figuur 1. **Het certificaat van een e-mailserver klopt niet volgens de iPhone en springt in beeld voor de eindgebruiker.** We kunnen dit certificaat weigeren en als gevolg geen e-mail ontvangen, direct accepteren en mogelijk onderwerp zijn van een aanval, of we kunnen meer details bekijken over de uitgever van het certificaat.



Figuur 2. **Details over de uitgever van het certificaat.** Kunnen we met deze beperkte informatie goed beoordelen of dit een geldig certificaat is?

functionaliteiten bevatten, staan ze onvermijdelijk bloot aan een groter aantal risico's. De producenten van deze apparaten, en wellicht ook anderen die de risico's willen beperken, moeten zich nog aanpassen aan deze gewijzigde situatie. Zo is het moeilijk om informatie over een foutief SSL-certificaat[5] van een website te krijgen op zo'n klein scherm (zie ook de figuren 1 en 2). Op een traditionele computer is deze informatie wel goed toegankelijk.

Maar naast wijzigingen met betrekking tot bestaande beveiligingsmaatregelen hebben de fabrikanten ook te maken met technieken zoals SMS, 3G-communicatietechnieken en GPS die voor hen nieuw zijn. Daardoor zijn de beveiligingsmaatregelen ten aanzien van de gegevens die op deze apparaten worden opgeslagen of verstuurd, nog niet volledig uitontwikkeld en getoetst.[6] Bovendien bestaat bij deze apparaten een grotere kans op cyberaanvallen omdat ze continu in verbinding staan met het internet.

Problemen met de basisveiligheid van de mobiele apparaten

Een goed voorbeeld van een niet volledig uitontwikkelde beveiligingsmaatregel is de toepassing van encryptie op de iPhone, wat de suggestie wekt dat de opgeslagen gegevens zijn versleuteld. De telefoon hoeft echter alleen maar te worden aangezet om de gegevens te ontsleutelen. Een oneigenlijke gebruiker hoeft dan slechts het wachtwoord (ook wel pincode of passcode genoemd) te kennen om toegang te krijgen tot het toestel. Echter, als men dit invoerscherm van het wachtwoord kan omzeilen (zoals tweemaal eerder mogelijk was op de iPhone[7]) of op een andere manier toegang kan krijgen tot het toestel, bijvoorbeeld door zwakheid uitgebuit via het netwerk, dan is de informatie op de telefoon direct toegankelijk. Vergelijk het met een laptop uitgerust met 'full-disk' encryptie waarbij de laptop geheel zelfstandig kan opstarten. De eerste keer dat een eindgebruiker dan een wachtwoord hoeft in te voeren is pas bij het Windows-inlogscherm. Op dat moment is het besturingssysteem al volledig actief en er zijn dan ook al legio aanvallen mogelijk.

5 SSL-certificaat: een versleutelmechanisme gebruikt voor communicatie over internet om de identiteit van de andere partij vast te stellen en om de versleuteling van datatransport te initiëren. Websites zoals die van uw bank gebruiken vaak SSL over HTTP, ook wel te herkennen aan HTTPS:// in de adresbalk en een klein slotje gepresenteerd door uw browser.

6 Collin Mulliner en Charlie Miller, augustus 2009, *Fuzzing the Phone in your Phone* (Black Hat USA, 2009).

7 iPhone passcode fout augustus 2008, http://www.zdnet.com/blog/security/iphone-passcode-lock-rendered-useless/1809; iPhone passcode fout oktober 2010, http://www.zdnet.com/blog/security/iphone-passcode-lock-bypass-vulnerability-again/7544.

Om iets te doen aan dit probleem heeft de leverancier extra encryptie ingebouwd voor de versleuteling van e-mail, contactpersonen en agendagegevens.[8] Maar dit omvat lang niet alle gegevens op de telefoon en ook deze tweede encryptie is niet volledig effectief. Als resultaat kunnen sommige 'dubbel versleutelde' gegevens toch gelezen worden door een oneigenlijke gebruiker.

Bovendien kan deze oneigenlijke gebruiker (die het wachtwoord niet kent) door middel van 'jailbreaking' de door de leverancier ingebouwde sloten verwijderen. Hiermee is volledige toegang tot het apparaat verkregen en kan de oneigenlijke gebruiker data lezen en aanpassen. Jailbreaking is heel eenvoudig; men kan op de iPhone surfen naar JailBreakMe,[9] of de iPhone aansluiten op een computer en daarop applicaties draaien die vrijelijk beschikbaar zijn en het jailbreaken tot een koud kunstje maken.[10] De 'jail' kan op een laag niveau verwijderd worden vanwege kritische zwakheden in onderdelen van de iOS-software. Bovendien is jailbreaking in de Verenigde Staten nu legaal dankzij een recente wijziging in de copyrightwetgeving (deze wetswijziging is opgenomen in de Digital Millennium Copyright Act). Fabrikanten verwijderen dan ook de detectie van jailbreaks uit hun besturingssysteem.[11]

Het zakelijk gebruik van privételefoons maakt het lastiger om naleving af te dwingen van bedrijfsbeleid omtrent bedrijfscommunicatie en de vertrouwelijkheid en beveiliging van informatie. Het betreft immers een privételefoon. Maar een samensmelting van privé- en zakelijke data op het mobiele apparaat is dan wel een feit. Op de telefoons kunnen bijvoorbeeld wachtwoorden zijn opgeslagen waarmee men op websites inlogt voor privégebruik, maar ook voor zakelijk gebruik. Onderzoekers hebben al aangetoond dat door een jailbreak toe te passen volledige toegang tot wachtwoorden kan worden verkregen zonder voorkennis te hebben van het toestel.[12] Bent u als eigenaar van de IT-omgeving blij als inloggegevens tot deze IT-omgeving op straat belanden doordat een medewerker zijn privételefoon is verloren?

Volledige toegang tot wachtwoorden kan worden verkregen zonder voorkennis te hebben van het toestel

Oplossingen hiertoe komen later in dit artikel aan bod, maar het moge duidelijk zijn dat de oplossingen niet louter in technische maatregelen dienen te worden gezocht. Denk bijvoorbeeld aan een beleidsmatige maatregel dat diefstal van een mobiel apparaat direct dient te worden gemeld, zodat het bedrijf een actie tot 'remote-wipe' kan uitvoeren op de iPhone. Dat hierbij ook privédata worden verwijderd mag geen discussie meer zijn doordat de eindgebruiker eerder akkoord is gegaan met het beleid.

Problemen met Apps op de mobiele apparaten

Naast de basisveiligheid van de mobiele apparaten zelf dient ook nog rekening gehouden te worden met de factor Apps. Het is voor de gebruiker van de telefoon mogelijk duizenden Apps te installeren, ieder met z'n eigen functionaliteit, zoals het handig opslaan van documenten en notities in de cloud zodat de gebruiker er ook via andere computers nog bij kan. Daarnaast kunnen bedrijven zelf ook Apps maken om diensten aan te bieden aan hun klanten. Maar in die Apps kunnen ook beveiligingsfouten sluipen, zoals een gerenommeerde Amerikaanse bank onlangs ondervond.[13] In een door haar ontwikkelde App leidden fouten ertoe dat gegevens opgeslagen bleven op de telefoon. Hierdoor kwamen gegevens vrij die toegang gaven tot rekeningoverzichten en waarmee geld kon worden overgemaakt.

Het komt erop neer dat op deze mobiele apparaten in veel meer bestanden en folders (niet alleen in e-mails en de agenda) erg veel gegevens worden opgeslagen. Hoewel de eindgebruiker wellicht niet direct toegang kan krijgen tot al deze bestanden doordat de standaard-gebruikersinterface dit niet laat zien, worden de gegevens wel opgeslagen. En daar waar data worden opgeslagen, kunnen zij potentieel weglekken. Dit kan leiden tot het weglekken van bedrijfsgegevens maar ook het in gevaar brengen van de privacy van de gebruiker. Twee recente voorbeelden: elke iPhone heeft bijvoorbeeld een uniek nummer, de UUID. Onderzoekers hebben aangetoond dat diverse Apps dit UUID, de geografische locatie van de telefoon en informatie uit het adresboek gebruiken en opslaan om statistieken over de gebruikers van deze Apps te verzamelen,[14]

8 Data Protection functionaliteit op iOS, http://support.apple.com/kb/HT4175.

9 http://jailbreakme.com, een website die bepaalde versies van iPhone kan 'jailbreaken' via de webbrowser van de iPhone.

10 Uitgebreid artikel over jailbreaken, http://www.iphoneclub.nl/58620/jailbreaken-en-unlocken-hoe-moet-dat-eigenlijk/.

11 *Webwereld*-artikel over detectie van jailbreak, http://webwereld.nl/nieuws/68092/apple-zet-iphone-jailbreak-detectie-uit.html.

12 Volledige toegang tot wachtwoorden door jailbreak, http://www.sit.fraunhofer.de/en/presse/Lost_iPhone.jsp.

13 Bank applicatie slaat transactie gegevens en inlogcodes op van klanten http://online.wsj.com/article/SB10001424052748703700904575391273536355324.html.

14 Eric Smith, oktober 2010, iPhone Applications & Privacy Issues: An Analysis of Application Transmission of iPhone Unique Device Identifiers (UDIDs).

zonder dat de gebruikers hiervan volledig op de hoogte zijn. Het tweede voorbeeld betreft technieken zoals triangulatie van GSM-masten die de iPhone hanteert om te weten waar in de wereld de telefoon zich bevindt. Onderzoekers hebben duidelijk gemaakt dat door middel van een simpel programmaatje het mogelijk is – met een nauwkeurigheid van enkele honderden meters – de fysieke locatie van de telefoon te illustreren.[15] De iPhone slaat dit lokaal op in een database en verstuurt dit periodiek naar de leverancier. Apple heeft de fout erkend en hier ook al op gereageerd.[16]

Samenvattend bestaan er ernstige zorgen of de huidige beveiligingsmaatregelen voor mobiele apparaten afdoende zijn om de hierboven genoemde risico's te minimaliseren.

Hoe kan men dit aanpakken, en wat is al in gang gezet?

Momenteel bieden producenten van mobiele telefoons nog geen volledige beveiligingsoplossingen. Hierdoor is er ruimte in de markt voor andere leveranciers die dergelijke oplossingen aan bedrijven leveren. De oplossingen variëren van het creëren van meer maatregelen om de apparaten onder controle te houden tot het inbouwen van 'encrypted containers' voor de opslag van bedrijfsgegevens op het apparaat. Deze oplossingen maken het aanzienlijk moeilijker voor een oneigenlijke gebruiker om toegang tot gegevens te krijgen. Maar het oorspronkelijke probleem blijft: als de telefoon zelf niet is beveiligd, kunnen ook deze oplossingen geen volledige veiligheid bieden. Ze kunnen het echter wel heel moeilijk maken voor een aanvaller, dus er is hoop.

De markt voor deze oplossingen is pas recent opgekomen en dus volop in ontwikkeling en daardoor nog niet volwassen. Het is daarom niet reëel om nu al volledig uitontwikkelde oplossingen te verwachten. Het gaat er nu om te erkennen dat de grotere mogelijkheden van de nieuwe generatie mobiele apparaten gepaard gaan met andere en grotere risico's en meer dan ooit te waken over kritische bedrijfsinformatie. Totdat producenten en leveranciers volledig effectieve technische beveiligingsmaatregelen op de markt brengen, moeten eindgebruikers bewust gemaakt worden van de risico's van deze apparaten. Daarnaast dient erop toegezien te worden dat op de apparaten die verbinding maken met zakelijke IT-omgevingen de beschikbare beveiligingsmaatregelen worden gebruikt. Deze maatregelen vormen slechts een eerste verdedigingslinie. Onthoud daarbij dat het om een samenwerking gaat van technische en organisatorische maatregelen.

Gebruik deze eerste verdedigingslinie wel ten volle. Implementeer dus een strikt wachtwoordbeleid, sta alleen apparaten met een vorm van encryptie toe, implementeer een effectief proces dat verloren apparaten ontkoppelt van de IT-omgeving, zorg dat de gebruikers altijd de laatste updates installeren en informeer gebruikers voortdurend over de gevaren.

Verder dienen verstandige keuzes gemaakt te worden voor technische oplossingen waarmee de IT-afdeling middelen heeft om de uitdagingen aan te gaan en het gebruik van deze apparaten in lijn kan brengen met richtlijnen die volledig aansluiten op beleid omtrent de verwerking van bedrijfsinformatie.

Conclusie

Risico's in gebruik van deze mobiele apparaten bestaan, maar de wil van de eindgebruikers om deze mobiele apparaten te gebruiken bestaat net zo goed. Helaas zijn de maatregelen nog niet volwassen genoeg voor een simpele en kant-en-klare oplossing. En daar zit de crux. Alleen e-mailen via webmail toestaan, of kan lokale e-mail ook? Alleen het gebruik toestaan mits een aantal technische maatregelen is ingevoerd op het apparaat zelf, of is de standaard iPhone veilig genoeg? Mogen alle websites worden bezocht met het mobiele apparaat, of dient er iets gefilterd te worden? Welke Apps slaan geen vertrouwelijke data op in de cloud en kunnen we veilig gebruiken? Dient iTunes nu ook te worden ondersteund op de bedrijfs-pc's? En hoe gaan we om met de back-ups die iTunes maakt op de privé-pc's, en wat zit er precies aan zakelijke data in die back-ups? Hoe krijgen we als IT-afdeling inzage in het gebruik van het mobiele apparaat? En wat is het risico van het ophalen van e-mail via een onbeveiligd draadloos netwerk? Hoe reageren we snel en juist op het verlies of diefstal van een mobiel apparaat? Allemaal vragen waar passende antwoorden voor zijn, maar waarbij de antwoorden afhangen van de reeds bestaande beveiligingsmaatregelen in het bedrijf. Het is dan ook zaak een gedegen analyse te maken van de maatregelen die men dient te treffen per bedrijfsomgeving.

Nieuwe generatie mobiele apparaten: grotere mogelijkheden, grotere risico's

Interessante ontwikkeling, deze nieuwe mobiele apparaten. Maar werk aan de winkel voor de informatiebeveiliger!

15 iPhone location tracker applicatie, April 2011, http://www.vulnerabilitydatabase.com/2011/04/iphone-tracker-map-your-iphone-stored-information/.
16 Apple's antwoord over opslag van locatiebepalingen, April 2011, http://www.apple.com/pr/library/2011/04/27location_qa.html.