WAAR LIGGEN DE RISICO'S EN WAAR IS DE CONTROLE?

Smartphones en tablets in de **bedrijfsomgeving**

Smartphones en tablets, zowel zakelijk als privé-eigendom, overspoelen de werkomgeving. Op deze apparaten wordt voor het ontsluiten van bedrijfsgegevens steeds vaker contact gelegd met onderdelen van het bedrijfsnetwerk. Hoe om te gaan met het groeiend aantal mogelijkheden van deze apparaten? En hoe kan deze mix van privé en zakelijk gebruik op een goede manier worden beheerst? In dit artikel zullen we inzicht geven in de huidige ontwikkelingen op het gebied van smartphones en tablets, de mogelijkheden die deze apparaten bieden. En we gaan in op risico's en beheersmaatregelen voor deze nieuwe technologieën.

MARC SMEETS EN PIETER CEELEN

De opmars van de nieuwe generatie mobiele apparaten is niet te stoppen[i]. Onder aanvoering van Apple – met de iPhone en iPad – en Google – met Android voor telefoons en tablets – wordt de bedrijfsomgeving overspoeld met nieuwe apparaten die er mooi en modern uitzien en handig in gebruik zijn. Het zijn echter niet zomaar nieuwe mobiele apparaten. Altijd verbonden met het internet en voorzien van legio applicaties (hierna apps) voor allerlei functies, luiden deze apparaten een wijziging in van onze manier van werken met makkelijkere communicatie en productieverhoging tot gevolg.

Vanuit het oogpunt van efficiëntie bieden deze apparaten veel voordelen, maar vanuit het perspectief van informatiebeveiliging introduceren ze ook een aantal beveiligingsrisico's. Het is de vraag hoe wij hiermee als IT-auditor moeten omgaan. In dit artikel geven we inzicht in de huidige ontwikkelingen op dit gebied, de verschillen ten opzichte van de traditionele computeromgeving, de gevoeligheid en dreigingen van deze technologie en als laatste de beveiligingsmaatregelen en hun beperkingen, met het doel de IT-auditor beter te informeren.

WAT ZIJN SMARTPHONES EN TABLETS EIGENLIJK?

Tot enkele jaren geleden was een BlackBerry de de facto standaard voor zakelijke mobiele telefoons. De BlackBerry werd door de werkgever aan de gebruiker uitgeleverd om onderweg zijn zakelijke email, contacten en agenda te kunnen beheren. In het algemeen wordt de BlackBerry door gebruikers ervaren als een zakelijk apparaat dat beperkt privé gebruikt wordt, hooguit om enkele privécontacten te bellen.

De introductie van de iPhone door Apple in 2007 veroorzaakte veel opwinding, een smartphone met een touchscreen gericht op de consumentenmarkt. Het toestel maakte het mogelijk dat consumenten altijd en overal bij hun email, agenda en contacten konden. Net zo belangrijk voor het succes was het altijd online kunnen zijn door de diverse laatste draadloze technieken aan boord én dat de gebruikersinterface het ook erg gemakkelijk maakte deze te benutten. De laatste troef was het maken van een App Store: een digitale omgeving waar ontwikkelaars hun programmatuur konden aanbieden. Hierdoor was er volop gelegenheid, vaak gratis of voor een gering bedrag, de ▸

iPhone qua functionaliteit uit te breiden met handige programmaatjes voor bijvoorbeeld het bijwerken van je sociale netwerk, verrichten van online betalingen, verhogen van je productiviteit op kantoor, het spelen van leuke spelletjes maar ook voor bedrijven om op een andere manier diensten aan hun klanten aan te bieden (zie ook kader 'apps ontwikkeld door een organisatie').

De iPhone kon nu wat de BlackBerry ook kon – het sturen en ontvangen van zakelijke email – zij het zonder IT-afdeling en met een handige interface. Een smartphone voor de massa, en het was een gat in de markt. Sinds de introductie zijn er meer dan 100 miljoen van verkocht[i]. Dat komt ook omdat in de afgelopen jaren voornamelijk ontwikkelingen zijn geweest op het gebied van smartphones, met als belangrijkste feiten flinke prijsverlagingen, meer mogelijkheden om verbinding te leggen met kantoornetwerken en de komst van Apple's grootste concurrent: Google. Als gevolg van deze ontwikkelingen is het tegenwoordig mogelijk dat de consument bij een telefoonabonnement 'gratis' een smartphone krijgt. En als je in een telefoonwinkel kijkt, dan zijn smartphones het leeuwendeel van het aanbod.

Wat kun je ermee?

De functionaliteit die een smartphone biedt, omvat voor veel mensen het grootste deel van wat ze überhaupt met een computer doen. Het surfen op het web, snel doorlezen van een rapportage die zojuist is gemaild, bijwerken van je Facebook-status, opzoeken van iemands LinkedIn-profiel, bekijken van de vakantiefoto's, raadplegen van de zakelijke agenda en het bekijken van de gezamenlijke huishoudagenda. Het gaat allemaal heel goed en gemakkelijk op een smartphone. Je zou de mogelijkheid om te kunnen bellen haast nog vergeten te vermelden.
En wanneer het scherm van een smartphone als te klein wordt ervaren, dan is er nog altijd de tabletcomputer.

Apple versus Google

De besturingssystemen van Apple (iOS) en Google (Android) vertonen veel overeenkomsten, maar er zijn ook enkele essentiële verschillen. De voornaamste overeenkomsten zijn:

- Beide zijn gebaseerd op bestaande besturingssysteem (Mac OS X en Linux).
- Beide zijn sterk gericht op het gebruik van apps. Gebruikers kunnen apps zoeken en installeren via een centrale registratie, de zogenaamde Apple App Store en Android Market.

Echter, belangrijke verschillen zijn er ook:

- Apple maakt en levert de gehele keten zelf. De hardware, het besturingssysteem (iOS), iTunes en toegang tot de App Store worden allemaal door Apple ontwikkeld en beheerd. Google levert in principe alleen het besturingssysteem Android en de toegang tot de Market zelf. De hardware wordt gemaakt door leveranciers als Samsung, HTC en Motorola.[1] Deze leveranciers leveren zelf nog beheersoftware mee, en ze hebben de mogelijkheid delen van de gebruikersinterface van Android aan te passen om zo hun eigen 'branding' toe te passen.
- Een iOS-smartphone of - tablet kun je beheren door middel van iTunes. Dit is software die de gebruiker installeert op zijn computer voor het maken van back-ups, het installeren van de laatste updates en het doen van aankopen in de Apple Store. Door middel van iTunes kunnen contacten, muziekbestanden, applicaties en overige data worden gesynchroniseerd tussen smartphone/tablet en computer. Later in 2011 zal Apple iOS versie 5 met iCloud introduceren . Hiermee wordt online opslag van foto's, email, contacten, et cetera en het updaten van iOS ook mogelijk gemaakt. Bij Android gebeurt veel al online, zoals het updaten van Android en het synchroniseren van bestanden bij de cloud service van Google. De beheersoftware die je van de hardware fabrikant bij je Android smartphone krijgt, heeft een beduidend kleinere rol in vergelijking met iTunes.
- Apple hanteert een strikte keuring voor apps in de App Store. Als gevolg hiervan worden veel Apps geweigerd in de App Store, bijvoorbeeld doordat ze concurrerend zijn met Apple's eigen Apps[8], of omdat de App niet precies doet wat de ontwikkelaar heeft opgegeven aan Apple. Google is hierin vrijer en laat meer apps toe tot haar Market. Tevens is het bij Android mogelijk andere 'Markets' toe te voegen via het configuratiescherm. Hardware leveranciers en de hackersgemeenschap zijn bekende bronnen van deze alternatieve Markets. Hoe daar de controle plaatsvindt, is onbekend. Hoewel bij beide apps met malware bekend zijn, is dit aantal bij de Android Market beduidend hoger.

De tablet, de bekendste verschijningsvormen zijn de iPad en de Samsung Galaxy Tab, biedt dezelfde functionaliteit als de smartphone, maar heeft daarbij een beduidend groter scherm (grofweg vijf keer groter). Net even wat makkelijker voor taken zoals een elektronisch boek lezen, net even wat fijner foto's bekijken en net even wat handiger surfen: het grotere scherm biedt hierin meer voordelen. Bellen kan ook, maar dan alleen via internetbellen, zoals Skype en Facetime.

Wat kun je er niet mee?

Maar er zijn zeker ook taken waar een smartphone of tablet niet handig voor is. Het typen van grote stukken tekst is wellicht de voornaamste. Maar ook de grotere opslagcapaciteit van de computer zal zeker de komende tijd nog zorgen dat de computer de centrale opslag blijft van foto's, muziek en wellicht ook zakelijke documenten.
Daar komt nog bij dat de eindgebruiker geen volledige controle heeft over zijn smartphone of tablet, zoals op zijn computer. De fabrikanten van smartphones en tablets leggen namelijk restricties op zodat de eindgebruiker minder problemen en storingen heeft op het apparaat en zodat het makkelijker is in gebruik. Maar daardoor is toegang tot de onderliggende lagen techniek niet meer mogelijk. Er zijn mogelijkheden deze restricties op te heffen door het toestel te hacken. Dit wordt ook wel *jailbreaking* (Apple-producten) of *rooting* (Android-producten) genoemd, doordat respectievelijk de *jail* van de fabrikant wordt opgeheven of doordat toegang tot de techniek wordt verkregen op het hoogste niveau *root*. Na jailbreaking of rooting is volledige

toegang tot het apparaat mogelijk en kunnen applicaties en functionaliteit worden geïnstalleerd die voorheen niet mochten van de fabrikant. Zie het kader 'Jailbreaking' voor meer informatie.

De onderliggende techniek

De twee grootste besturingssystemen voor smartphones zijn op dit moment het door Apple ontwikkelde iOS en het besturingssysteem Android dat door Google ontwikkeld is[ii]. Windows Mobile (Microsoft), RIM OS (BlackBerry) en Symbian (Nokia) hebben een beduidend kleiner marktaandeel wat de smartphonemarkt betreft, maar werken hard om deze achterstand in te halen en hun nieuwe producten te voorzien van vergelijkbare functionaliteit als die van Apple en Google.

De Android- en iOS-besturingssystemen berusten technisch gezien al op bestaande desktop besturingssystemen. Android heeft als kern het open source besturingssysteem Linux, en iOS heeft als kern Apple's eigen Mac OS X. In beide gevallen zijn de besturingssystemen zo opgebouwd dat de kern wordt behouden maar een aantal componenten wordt aangepast voor mobiel gebruik. Denk hierbij aan optimalisatie van energieverbruik, het implementeren van een ander soort toetsenbord, het niet hoeven ondersteunen van randapparatuur zoals printers, muizen, et cetera. Omdat deze systemen zo flexibel zijn opgebouwd, is het niet meer dan een logische keus dat ook Android en iOS op tablets actief kunnen zijn. Je kunt in wezen stellen dat tablets niets anders zijn dan iets grotere smartphones. De onderliggende techniek is hetzelfde, alleen de gebruikerservaring is anders.

SMARTPHONE EN TABLET VERSCHILLEN VAN DE TRADITIONELE COMPUTEROMGEVING

We hebben al een aantal punten genoemd waarop de smartphone en tablet verschillen van de traditionele computeromgeving binnen bedrijven. Met 'traditioneel' bedoelen we dat de gebruiker eigenlijk alleen gebruikmaakt van een desktop of laptop en een BlackBerry van de oude generatie. Echter, er zijn nog meer verschillen en die zijn niet louter technisch, maar betreffen de beweging van privételefoons naar de zakelijke omgeving. Hieronder vermelden we de verschillen die vooral voor de IT-auditor van belang zijn:

- Eigenaarschap: de eigenaar van het mobiele apparaat hoeft niet het bedrijf te zijn. De werknemer kan de voorkeur geven aan zijn privé smartphone, en technisch gezien kan de privételefoon worden verbonden aan het bedrijfsnetwerk.
- Beheerder: dit punt hangt samen met het vorige punt rondom eigenaarschap. Het kan zijn dat de eindgebruiker de beheerder is, niet de IT-afdeling. Het invoeren van instellingen zal dan door de eindgebruiker gebeuren.
- Privé- en bedrijfsdata: op het mobiele apparaat is geen scheiding van privé- en bedrijfsdata. Het apparaat wordt voor beide gebruikt, en er zullen dan ook zowel privé - als bedrijfsdata op het apparaat aanwezig zijn.
- Apps: de Apple App Store en Android Market maken het gemakkelijk duizenden apps te installeren. Nieuwe functionaliteit en diensten worden gemakkelijk toegevoegd, waarbij meer en meer diensten online plaatsvinden (bijvoorbeeld cloud computing).
- Back-ups: back-ups, en daarmee ook bedrijfsdata, worden op diverse plekken bewaard. De iPhone laat automatisch een back-up achter bij iedere iTunes waarmee wordt gesynchroniseerd. Dat is mogelijk op de computer bij de werknemer thuis. Later dit jaar zal ook een back-up worden bewaard in Apple's online dienst iCloud. Voor Android geldt dat back-ups automatisch online worden bewaard bij Google.
- Online: doordat de smartphones altijd online zijn én een handig te gebruiken browser aan boord hebben, is het ook mogelijk toegang te krijgen tot het intranet van het bedrijf. Mocht de browser net niet helemaal fijn werken dan kan het bedrijf ervoor kiezen een eigen app te ontwikkelen die direct het intranet of interne applicaties aanspreekt. Een dergelijke app kan de beveiliging van de verbinding op zich nemen waardoor de gebruiker niet eerst een VPN hoeft op te zetten.
- Ecosysteem: De nieuwe smartphones en tablets zijn veel meer een ecosysteem dan louter alleen het mobiele apparaat zelf. Dit zullen we hieronder verder bespreken.

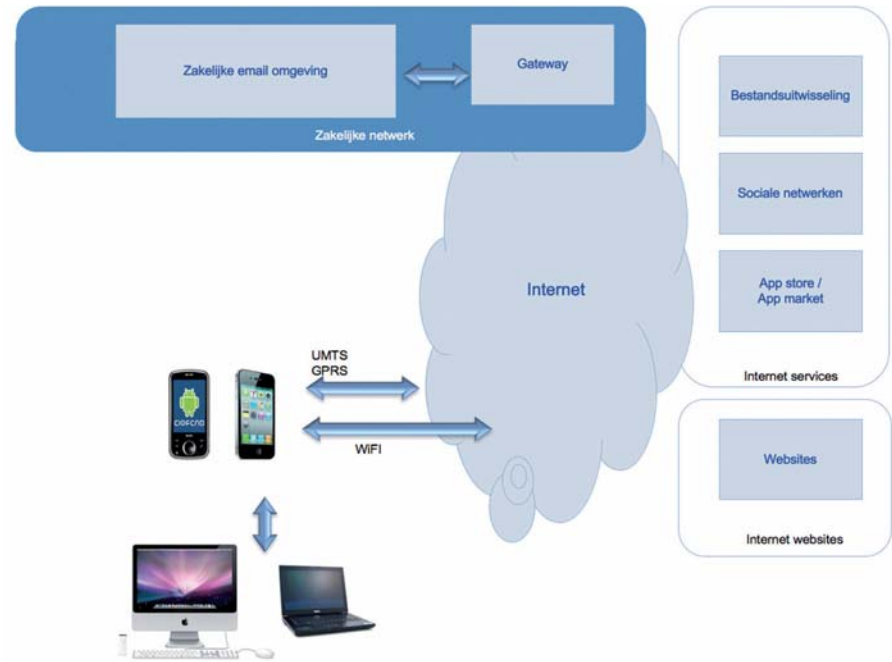
Apps ontwikkeld door een organisatie

Het publiceren van organisatiegebonden apps namens een bedrijf biedt mogelijkheden op een andere manier direct met klanten in contact te staan en kan vaak een interessante manier zijn van service verlenen. Het ontwikkelen van dergelijke apps gebeurt in aparte ontwikkelomgevingen en veelal door gespecialiseerde ontwikkelaars. Echter, zoals met alle software kunnen ook hier problemen met de informatiebeveiliging optreden en dit kan gevolgen hebben voor de informatieverwerking, maar zeker ook voor het imago van een organisatie. Denk bijvoorbeeld aan het onveilig opslaan van klantgegevens of het niet wissen van privacygevoelige data. Controle hierop kan plaatsvinden met IT-audits, *source code reviews* en *security tests*. Maar gezien de specialistische omgeving is het nodig dat de IT-auditor bekend is met de onderliggende technieken.

Telefoon of ecosysteem?

Bij het analyseren van risico's van smartphones is het belangrijk de volledige omgeving te karakteriseren en te analyseren. Het is immers niet alleen het apparaat zelf waar de IT-auditor aan moet denken. In figuur 1 is grafisch weergegeven welke componenten relevant zijn en hoe deze componenten onderling verbonden zijn.

We zien dat de smartphone verbonden is met het internet en met computers. De aansluiting op de computer wordt gebruikt om de telefoon te beheren, back-ups te maken en data en muziekcollecties ▶



Figuur 1: Het ecosysteem van de moderne smartphone en tablet

te synchroniseren.[2] De internetverbinding wordt gebruikt om websites te bezoeken en voor de verbinding naar het zakelijke netwerk. Daarnaast zijn er nog diverse internetdiensten specifiek voor de smartphone, bijvoorbeeld sociale netwerken (apps voor Hyves, FaceBook en LinkedIn), bestandsuitwisseling (apps voor DropBox) en de App Store waarmee nieuwe applicaties kunnen worden geïnstalleerd. Het betreft dus veel meer dan alleen de smartphone zelf. De centrale vraag voor de IT-auditor is dan ook 'Waar staat de data?'.

GEVOELIGHEID EN DREIGINGEN

Gevoeligheid

Bij de introductie van nieuwe technologieën in de zakelijke omgeving is het de rol van de IT-auditor om te onderzoeken welke risico's deze nieuwe technieken met zich meebrengen. Bij de uitrol van smartphones in de zakelijke omgeving is het lezen van zakelijke e-mail vaak de eerste toepassing. Onze ervaring leert dat de nieuwe generatie smartphones vaak als eerste aan het hogere management worden uitgereikt. De mailboxen van medewerkers op dit niveau bevatten over het algemeen de meest gevoelige gegevens. Op basis hiervan is al snel de conclusie te trekken dat er gevoelige gegevens op deze apparaten kunnen staan.

Het lekken van een email met daarin de conceptversie van het jaarverslag die via een onbeveiligde smartphone aangepast wordt, kan direct invloed hebben op de jaarrekening of de aandelenkoers van het specifieke bedrijf. Maar in andere gevallen kan louter de inzage in de mailbox of agenda van een lid van de Raad van Bestuur al voldoende gevoelig zijn.

Overigens is het niet alleen het management dat met mogelijk interessante data rondloopt. De opslagcapaciteit van smartphones is enorm. Gehele contactgeschiedenissen, bestanden die zijn geannoteerd maar ook privédata van werknemers, alles staat erop en blijft er lang op staan vanwege de grote opslagcapaciteit. Die data kan allemaal mogelijk de vertrouwelijkheid aantasten wanneer deze wordt gelekt. Maar de integriteit en beschikbaarheid van de dataverwerking komen ook in het gedrang wanneer kwaadwillenden wachtwoorden van een 'gevonden' smartphone kunnen uitlezen. Hiermee kan toegang tot het beveiligde bedrijfsnetwerk worden verkregen en is de schade zonder additionele monitoring software vaak niet te overzien.

Dreigingen

Er zijn diverse dreigingen die de beschikbaarheid, integriteit en vertrouwelijkheid van data op een telefoon kunnen aantasten. Naast de welbekende risico's van verlies en diefstal zijn er ook dreigingen die niet zo voor de hand liggend zijn, maar die voor smartphones wel van belang zijn. Denk bijvoorbeeld aan:

Virussen en malware

De sterke groei van de smartphonemarkt maakt deze interessant voor de makers van virussen en malware. Er worden al regelmatig virussen aangetroffen op deze apparaten.

Integratie met online diensten
Met een smartphone kan ook gebruikgemaakt worden van de diverse apps die aangeboden worden op het internet. Deze apps kunnen integreren met zakelijke data. Denk hierbij aan koppelingen met sociale netwerken of het automatisch synchroniseren van bedrijfsdata naar online opslagdiensten (bijvoorbeeld DropBox).

Privéwerkstations van medewerkers
Zoals in figuur 1 te zien, is er ook een koppeling tussen werkstations en de smartphone. Wat gebeurt er als een medewerker zijn telefoon beheert vanaf zijn privé laptop? Wordt zakelijke apps data ook gekopieerd naar deze laptop? Welke data zitten er in back-ups en zijn deze versleuteld? Wat gebeurt er als de privélaptop met een virus is geïnfecteerd? En hoe staat het met wet- en regelgeving (denk aan privacywetgeving) op het moment dat opslag van data op buitenlandse servers (bijvoorbeeld in de VS) wordt opgeslagen wanneer je een back-up van je smartphone of tablet maakt?
De exacte dreigingen bij het implementeren van smartphones zijn sterk afhankelijk van de manier waarop smartphones worden uitgerold en bovenstaande lijst is dan ook zeker niet compleet. Kiest een organisatie ervoor om alleen één type smartphone te ondersteunen die volledig is afgeschermd of kan elke gebruiker zijn privételefoon aansluiten op het zakelijke netwerk? Wie is juridisch eigenaar van het apparaat? Mag de smartphone worden aangesloten op een privé-pc? Ongeacht de exacte antwoorden op deze vragen is het belangrijk om je als auditor niet alleen te richten op de smartphone, maar het gehele ecosysteem te beschouwen in een analyse van de dreigingen.

BEVEILIGINGSMAATREGEL OF WASSEN NEUS?

Door Apple en Google worden diverse maatregelen geïmplementeerd om smartphones veiliger te maken. Echter, in de praktijk blijkt een aantal van deze maatregelen niet zo sterk als men zou verwachten. In tabel 1 hebben we enkele beveiligingsmaatregelen uitgelicht.

Aanvullende maatregelen

Uit de informatie in tabel 1 blijkt dat de beveiligingsmaatregelen die standaard door iOS en Android worden geboden, niet afdoende zijn om het risico van een verloren telefoon te mitigeren. Immers, de *remote wipe* functionaliteit en de encryptie kunnen eenvoudig worden omzeild.
Er zijn enkele leveranciers die producten leveren om deze risico's beter te kunnen beheren. Deze Mobile Device Management-oplossingen leveren ▶

Maatregel	Beperking van maatregel
Remote wipe	In smartphones is functionaliteit geïmplementeerd om data op afstand te wissen. Via het internet kan het commando worden gegeven dat alle data gewist moet worden in het geval dat de telefoon verloren is geraakt. Een aanvaller die toegang heeft tot een telefoon en zakelijke data wil inzien zal de telefoon in de 'vliegtuigmodus' zetten of de SIM verwijderen. Hierdoor zal de telefoon niet kunnen verbinden met het internet en zal het commando om de data te wissen niet ontvangen worden. In deze modus kan de aanvaller nog steeds de informatie die op de smartphone is opgeslagen uitlezen.
Encryptie	Op de iPhone is hardwarematig disk encryptie geïmplementeerd. Dit is echter een ander type disk encryptie dan we kennen van laptops. Om de data te ontsleutelen is het niet nodig om een wachtwoord of PIN op te geven; de telefoon ontsleutelt de data zonder tussenkomst van de gebruiker. De passcode die de gebruiker kan instellen is een beveiligingsmaatregel die pas na het volledig opstarten optreedt en is louter bedoeld kwaadwillenden geen kans te geven via het touchscreen. Binnen de informatiebeveiliging wordt dit gezien als een zwakke beveiligingsmaatregel. Een aanvaller kan dan ook met specifieke software alle data van de telefoon uitlezen ongeacht de disk encryptie door de smartphone te starten in een modus die te vergelijken is met de Recovery Console van Windows. Voor Android is overigens geheel geen disk encryptie aanwezig in de huidige versies.
Permissie model voor applicaties	Op de smartphones wordt afgedwongen dat een app alleen specifieke acties kan uitvoeren en data kan benaderen. De gebruiker wordt bij installatie geïnformeerd over de benodigde rechten van een app en kan op basis hiervan kiezen of hij de app wel deze rechten geeft. In de praktijk blijkt dat veel apps gevoelige permissies vereisen[iii]. Hierdoor slaat de balans tussen het informeren van gebruiker al snel om naar het negeren van deze meldingen.
Kwaliteitscontroles in App Store en Market	Apple heeft er in de App Store voor gekozen de broncode van alle apps te reviewen voordat ze worden opgenomen in de App Store. Deze reviews blijken in de praktijk echter niet 100% waterdicht te zijn. Er zijn voorbeelden van apps waarbij de ontwikkelaar code had verborgen in een goedgekeurde applicatie[iv]. Tevens is het mogelijk om op een jailbroken iPhone of iPad de alternatieve app Store Cydia te installeren. Zie ook het kader 'Jailbreaking'. Google heeft initieel gekozen geen enkele controle toe te passen op de Android Market. Als gevolg hiervan is het risico op apps met virussen of malware relatief hoog. Google heeft ondertussen ingezien dat een geringe controle toch noodzakelijk is[v], maar een effectieve controle is nog niet gevonden.

Tabel 1: Maatregelen en beperkingen

een omgeving waarmee het beheer van smartphones centraal plaatsvindt. Daarbij wordt hen de ruimte gegeven door Apple en Google. Op dit moment zijn er twee implementatierichtingen. Zie figuur 2.

Eén mogelijkheid is een zogenaamde *secure container*. Hierbij wordt een app geïnstalleerd op de telefoon. Deze app maakt een versleutelde opslaglaag aan op de telefoon. De app maakt een beveiligde verbinding met het bedrijfsnetwerk en slaat emails en data op binnen deze versleutelde opslaglaag. Versleutelde data wordt pas ontsleuteld nadat het juiste wachtwoord is ingegeven. De standaard apps voor email, agenda, et cetera blijven behouden voor privégebruik, maar het lezen van zakelijke email en bedrijfsdata vindt plaats in de versleutelde app. Het weergeven van bijlagen wordt afgehandeld door componenten in de secure container. Hierdoor hoeven de data nooit onversleuteld opgeslagen te worden. Nadeel hiervan is wel dat er mogelijk maar beperkte bestandsformaten ondersteund worden en dat er qua gebruikersvriendelijkheid wordt ingeboet. Er wordt immers voor het zakelijke deel geen gebruik meer gemaakt van de standaardbrowser en emailprogramma waar de gebruiker aan gewend is.

Een andere mogelijkheid richt zich op meer geavanceerde controles op beveiligingsinstellingen van de bestaande smartphone. Met deze oplossingen is het mogelijk om vanuit een centrale managementomgeving af te dwingen dat alle telefoons minstens voldoen aan bepaalde beveiligingsinstellingen. Door het toepassen van maatregelen zoals passcodes, jailbreak detectie, versiedetectie en controles op overige geïnstalleerde apps kunnen risico's verlaagd worden. Het nadeel van deze oplossing is het steunen op de beveiliging van iOS en Android. Als daar kritieke fouten in worden ontdekt (wat nog steeds regelmatig[vi] gebeurt[vii]) dan ondermijnt dit ook deze oplossing.

Jailbreaking

Jailbreaking is het proces van verwijderen van softwarematige restricties die aanwezig zijn op de smartphone. Tijdens dit proces worden beveiligingsfouten in de software van de smartphone gebruikt voor het verkrijgen van meer toegang. Voor Android-toestellen wordt dit ook wel 'rooten' genoemd omdat hiermee de rechten van de rootgebruiker worden bemachtigd.

Na een jailbreak kun je meer met je smartphone. Zo is het mogelijk apps gratis te installeren of apps te installeren die niet zijn goedgekeurd en dus niet beschikbaar zijn in de App Store of Market. Ook is het mogelijk directe commandoprompt toegang te krijgen met beheerdersrechten en is daarmee volledige interactie met het onderliggende besturingssysteem mogelijk. Een jailbreak wordt ongedaan gemaakt via een update van iOS of Android. Het behoud van een jailbreak is dan ook een belangrijke reden voor gebruikers om niet te updaten of te wachten totdat een jailbreak van de laatste softwareversie beschikbaar is.

Het proces zelf is niet moeilijk en diverse handleidingen zijn beschikbaar op het internet. Soms is het zelfs alleen nodig een specifieke website te bezoeken.[ix] Exacte cijfers over het aantal jailbreaks ontbreken, maar onderbouwde schattingen lopen uiteen van 15 procent tot 40 procent, afhankelijk van de regio in de wereld. Het is een kat-en-muisspel tussen de hackers en leverancier, waarbij een belangrijke slag gewonnen is door de hackers doordat jailbreaking is toegestaan door Amerikaanse wetgeving[x] en detectie ervan weer is verwijderd uit iOS11.[xi]

Figuur 2: Illustratie van de twee implementatierichtingen. Links is een app toegevoegd die controles op de smartphone uitvoert, gebruikmakende van de standaardfunctionaliteit van de smartphone. Rechts is een app geïnstalleerd die standaardfunctionaliteit heeft nagemaakt binnen de beveiligde opslag.

Beide technische oplossingen helpen veel, maar zijn niet voldoende om risico's volledig te mitigeren. Aanvullende beheersmaatregelen op het gebied van mensen en processen zijn dan ook nodig. Als smartphones hun weg vinden naar een organisatie, houd dan rekening met in ieder geval de volgende algemene maatregelen op het gebied van techniek, mensen en processen.

Techniek

Gebruik de technische maatregelen zoveel mogelijk als volgt:

- Geen implementatie zonder Mobile Device Management-oplossing. Selecteer de juiste die past bij het gebruik van de smartphone in de bedrijfsomgeving.
- Sta geen jailbroken of rooted devices toe.
- Pas een strikt beveiligingsbeleid toe op de smartphone (bijvoor-

beeld lengte en complexiteit van de passcode, alleen laatste versie van iOS en Android, bekende apps met malware niet toestaan).
- Zorg voor juiste filtering tussen emailomgeving en het internet waar de smartphones zich bevinden.
- Sta alleen apps toe voor specifieke bedrijfstoepassingen als bekend is hoe deze apps omgaan met de bedrijfsdata.

Mensen

Voor mensen zijn de volgende acties van belang:
- Maak eindgebruikers bewust van de gevaren van het gebruik van smartphones.
- Informeer eindgebruikers regelmatig over de acties in geval van verlies en diefstal van de smartphone en in het geval van vreemde beveiligingsmeldingen op het scherm.

Processen

De volgende processen dienen zeker te bestaan:
- Een proces voor het melden en wissen van verloren/gestolen smartphones.
- Een proces dat aansluit op het bovenstaande proces voor het afsluiten/vervangen van IT-data waarvan ook gegevens (bijvoorbeeld wachtwoorden) bekend waren op de verloren smartphone.
- Een proces voor vervanging van een privétoestel.
- Een proces voor de uitdiensttreding van een personeelslid.

Het is belangrijk hierbij op te merken dat dit algemene richtlijnen zijn. Afhankelijk van hoe smartphones worden gebruikt in een bedrijfsomgeving, bijvoorbeeld alleen specifieke apps of volledige email, kalender en contacten toegang, kunnen de maatregelen nogal verschillen. Ogenschijnlijk kleine details maken veel verschil in het waarborgen van beschikbaarheid, integriteit en vertrouwelijkheid van de bedrijfsvoering. Het advies is dan ook gebruik te maken van de kennis van materiedeskundigen bij het inrichten en toetsen van omgevingen met smartphones.

CONCLUSIE

Dit artikel gaat over smartphones in de bedrijfsomgeving en welke substantiële risico's dit oplevert indien er geen aanvullende maatregelen worden getroffen. Een smartphone of tablet kan worden beschouwd als een onbeveiligde USB stick die verbonden is met het internet en daardoor zichzelf updatet met de laatste emails, documenten en andere data, zowel van privé- als zakelijke bronnen.

Om de risico's en dreigingen te kunnen beheersen, is het nodig inzicht te verkrijgen in het gebruik van en het ecosysteem waarin deze apparaten zich bevinden. Het opstellen van de juiste beheersmaatregelen is een complexe aangelegenheid waarbij er afhankelijk van de behoefte en wensen van een organisatie verschillende oplossingsrichtingen zijn. Technische oplossingen alleen zijn hierbij zeker niet afdoende en beheersmaatregelen op het gebied van mensen en processen zijn nodig.

Tevens is het belangrijk te weten dat dit een zich snel ontwikkelend gebied binnen de IT is en zal blijven in de komende jaren. We kunnen dan ook in de komende tijd meer mogelijkheden verwachten van de smartphones zelf. Gelukkig staan de ontwikkelingen van beveiligingsoplossingen ook niet stil en zijn steeds meer mogelijkheden voor beheersing van de risico's voorhanden. Al met al weer een interessante tijd voor de IT-auditor! ■

Noten

1. Op het moment van schrijven is bekend geworden dat Google Motorola heeft gekocht. Het lijkt er vooralsnog op dat dit vooral is gedaan om een aantal patenten in handen te krijgen. Er zijn nog geen plannen voor een officiële Google-telefoon bekend gemaakt, al is dat voor de toekomst niet uit te sluiten.
2. We zien overigens een trend waarbij steeds meer beheertaken ook online kunnen plaatsvinden. De cloud diensten van Apple en Google hebben daarbij een centrale rol. Zie ook kader 'Apple vs. Google'.

Internetverwijzingen

i. http://mashable.com/2011/03/02/100-million-iphones/
ii. http://www.telecompaper.com/nieuws/android-meest-gebruikte-smartphone-os-in-nederland
iii. http://www.cs.berkeley.edu/~afelt/felt-permissions-webapps11.pdf
iv. http://seriot.ch/resources/talks_papers/iPhonePrivacy.pdf
v. http://webwereld.nl/nieuws/105952/android-malware-dwingt-google-tot-beveiliging.html
vi http://support.apple.com/kb/HT4564
vii http://web.nvd.nist.gov/view/vuln/search-results?query=android
viii http://webwereld.nl/nieuws/105574/apple-weigert-sony-reader--scherpt-app-store-regels-aan.html
ix http://www.jailbreakme.com
x http://www.engadget.com/2010/07/26/library-of-congress-adds-dmca-exception-for-jailbreaking-or-root/
xi http://webwereld.nl/nieuws/68092/apple-zet-iphone-jailbreak-detectie-uit.html

M. (Marc) Smeets MSc. CISSP CISA is werkzaam bij KPMG en adviseert over IT-beveiliging. Sinds de opkomst van de eerste smartphones houdt hij zich bezig met de beveiliging ervan. Denk hierbij aan infrastructuur reviews, IT-audits en penetratietesten op de gehele ketens van bijvoorbeeld iPads en iPhones in bedrijfsomgevingen. Dit artikel is op persoonlijke titel geschreven.

P.(Pieter) Ceelen MSc. is sinds 2008 werkzaam bij KPMG als adviseur op het gebied van IT-beveiliging. Ceelen heeft diverse onderzoeken uitgevoerd op het gebied van smartphonebeveiliging. Hij is een fervent gebruiker van het Android-besturingssysteem. Dit artikel is op persoonlijke titel geschreven.