



# iPad als beveiligd verlengstuk van uw werkplek

whitepaper

v1.2, juni 2011





## Colofon

Documentnaam Whitepaper Beveiliging Smart Devices\_Strict v1.2

Titel iPad als beveiligd verlengstuk van uw werkplek

Versie, datum v1.2, 16-06-2011

Samengesteld door Mark Jenniskens, Kelvin Rorive, Arnold Jessurun

Op basis van Bevindingen miniseminars d.d. 25-01-2011, 16-03-2011, 19-05-2011 en 24-05-2011

Afdeling Security Management

© Strict, 2011

Niets uit deze uitgave mag worden verveelvoudigd en/of openbaar gemaakt door middel van druk, fotokopie, microfilm of op welke andere wijze ook, zonder voorafgaande toestemming van Strict.  
No part of this publication may be reproduced in any form by print, photo print, microfilm or any other means without written permission by Strict.

Contactadres voor deze **Strict**  
publicatie Lange Dreef 11-f  
4131 NJ Vianen  
Postbus 12  
4130 EA Vianen  
T. 088 55 55 800  
F. 088 55 55 801  
[info@strict.nl](mailto:info@strict.nl)  
[www.strict.nl](http://www.strict.nl)

## Versiebeheer

Datum	Status	Versie	Auteur	Omschrijving
11-02-2011	Final	1.0	AJES	Final obv bevindingen miniseminar 25-01-2011
22-03-2011	1 <sup>e</sup> Revisie	1.1	KR	Update obv 2 <sup>e</sup> miniseminar 16-03-2011
16-06-2011	2 <sup>e</sup> Revisie	1.2	MJEN/KR	Update na de seminars 19-05-2011 en 24-05-2011



## 1. INLEIDING

Sinds eind 2010 is het erg hard gegaan met de verkoop van de iPad. Dat was ook te zien in de kwartaalcijfers van Apple. Maar het is ook merkbaar in onze directe werkomgeving. Veel collega's, op alle niveaus, hebben een iPad en voor verschillende redenen. De één voor het lezen van vakbladen, de ander voor het eenvoudig kunnen raadplegen van internetinformatie of het bijhouden van e-mail en agenda.

Door frequent zakelijk gebruik wil men met de iPad ook toegang kunnen krijgen tot de bedrijfsnetwerken. Soms gaat dit eenvoudig en zonder hindernissen, maar meestal stuit men op barrières, zoals firewalls en gateways, waar de informatie niet doorheen komt.

De ervaring leert dat security-afdelingen nog worstelen met de nieuwe risico's bij het ontsluiten van onbekende devices op het bedrijfsnetwerk. Dat is een vraagstuk op beleidsniveau. Meer en meer komen directies met de vraag naar een goede, betrouwbare en werkbare oplossing. Die er dan ook snel moet komen.

Om hier een reactie op te geven wordt in deze whitepaper een aantal mogelijkheden geschetst.

Deze whitepaper is tot stand gekomen naar aanleiding van de miniseminars "iPad als beveiligd verlengstuk van uw werkplek", die op 25 januari, 16 maart, 19 en 25 mei 2011 werden georganiseerd door Strict. De deelnemers aan deze seminars vertegenwoordigden organisaties uit de Financiële sector, Openbare Orde en Veiligheid (OOV), de Zorg, Waterschappen, Tetranet en de Retail sector.



## 2. OVERZICHT CONCLUSIES

In aansluiting op de miniseminars van Strict zijn de volgende conclusies getrokken rond de inzet van smart devices als verlengstuk van de werkplek, welke in de volgende hoofdstukken van deze whitepaper verder worden uitgewerkt:

1. Conclusie 1: Smart devices zijn niet tegen te houden
  - De ontwikkelingen gaan hard, dus anticipeer ook op toekomstige devices en diensten.
  - Uitwerking zie hoofdstuk 3.
2. Conclusie 2: Goed beleid vormt de basis
  - Zorg voor een goed beleid en gebalanceerde maatregelen.
  - Uitwerking zie hoofdstuk 4.
3. Conclusie 3: Risicoprofiel en cultuur bepalen succes van BYO concept
  - Managed concept wordt vooral toegepast bij een zwaar dreigingsprofiel, terwijl Unmanaged (BYO – Bring Your Own) vooral bij lichtere dreigingsprofielen voorkomt.
  - Uitwerking zie hoofdstuk 5.
4. Conclusie 4: Nu is het moment om bewustwording extra aandacht te geven
  - Deze ontwikkeling wordt gezien als ultiem moment om bewustwording te verhogen.
  - Uitwerking zie hoofdstuk 6.



### **3. CONCLUSIE 1: SMART DEVICES ZIJN NIET TEGEN TE HOUDEN**

#### **3.1 De ontwikkelingen gaan hard**

Een goede tablet zat er al lange tijd aan te komen. Vanaf 1980 is er veel mee geëxperimenteerd geweest. Microsoft en Apple probeerden het, maar aanvankelijk met weinig succes. Over het algemeen waren de apparaten te duur en kwalitatief niet goed genoeg. Dat gold voor zowel de hardware als de software. Ook liet de gebruiksvriendelijkheid te wensen over.

In feite is de iPad de eerste succesvolle tablet. Apple had de weg natuurlijk al vrijgemaakt met de iPhone. Een solide premium apparaat met een focus op gebruiksvriendelijkheid (usability). Het iPhone concept is door Apple bijna één op één uitgevoerd op een nieuw apparaat met een groter scherm, de iPad.

De eerste echte concurrentie voor Apple komt van de Samsung Galaxy Tab, met het door Google gemaakte Android besturingssysteem, voortbordurend op het succes van de Galaxy S smartphones. Echter Android 2.x vertaalt zich minder goed naar het grotere scherm.

Vanuit China zijn er op dit moment ook veel tabletcomputers de markt op. Deze zijn gebaseerd op smartphone hardware, meestal met Android als operating systeem. De kwaliteit is niet vergelijkbaar met de iPad, maar de kosten zijn aantrekkelijk.

2010 was het jaar van de iPad, waarmee de toon is gezet. 2011 wordt het jaar van de tablets. Waar Apple de hardware zelf heeft ontworpen, komen alle chipmakers nu met referentieontwerpen voor de PC fabrikanten. Hierdoor komt nagenoeg iedere PC fabrikant in 2011 met een tablet. Gelukkig is er nog wel differentiatie. Android 3.0, het Tablet-OS van Google zal de basis zijn voor veel tablets, zoals de Motorola Xoom en de Samsung Galaxy Tab 10.1. De BlackBerry Playbook van RIM zal QNX draaien en de HP TouchPad WebOS.

Ook zullen er allerlei hybride apparaten volgen. Leveranciers zullen proberen te variëren in ontwerpen en toepassingsmogelijkheden. De meest geziene variaties zijn gebaseerd op toetsenborden, als docking of als schuifmechanisme.

De diversiteit van het tabletaanbod zal fors toenemen en het is niet te ontkennen dat, net zoals dat met de smartphone is gegaan, de tablet de zakelijke markt van alle kanten zal infiltreren.

#### **3.2 Businessstoepassingen**

Op zakelijk gebied is er veel mogelijk, maar de belangrijkste 'killer App' van dit moment blijft nog altijd e-mail en de agenda. Daarnaast zien we veel Social Media Apps (Twitter, Yammer, Facebook, LinkedIn, etc.), presentatie Apps en Apps die de gebruiker helpen zichzelf te organiseren, zoals mindmapping, whiteboarding en to-do lijsten.

#### **3.3 'Apps' zijn de sleutel, ook zakelijk**

De meeste organisaties zijn nog aftastend in het gebruik van zuivere businessstoepassingen. Naar verwachting is dit een kwestie van tijd. Bedrijfsspecifieke informatie zal via Apps ontsloten worden. Dit zal in de vorm van Business Intelligence Dashboards of bijvoorbeeld SAP urenregistratiesystemen gebeuren. Ook is het mogelijk real-time te communiceren via tablets, bijvoorbeeld in de vorm van Facetime of Skype, zowel met als zonder video. Zo gaan gemeenteraden en boardrooms digitaal met vergaderingondersteunende documentmanagement Apps en ook zullen er Apps voor in de schoolbanken komen.



De meeste grote leveranciers van zakelijke applicaties hebben al aangekondigd dat ze Apps beschikbaar gaan stellen voor het gebruik van businessapplicaties. De verwachting is dat daardoor de smart devices, mits goed beveiligd, een bredere zakelijke toepassing krijgen.

Een alternatief op deze specifieke Apps is het gebruik van applicatievirtualisatie. Hiermee wordt de applicatie virtueel beschikbaar gesteld op het smart device. Een aandachtspunt bij virtualisatie naar smart devices is dat de applicaties daarvoor niet geoptimaliseerd zijn. Bepaalde kleine knoppen, die normaal gesproken met de muisaanwijzer worden geklikt, zijn via de touch screens op smart devices met de vinger lastig te selecteren. Zowel de virtualisatieproviders als de applicatie- en besturingssysteemsschrijvers zijn bezig om de gebruikerservaring met touch-gebaseerde interfaces te verbeteren.

### **3.4 Toegankelijkheid gaat voor beveiliging**

Nu de iPad enige tijd op de markt is blijkt dat het apparaat voor privétoepassingen overwegend voldoende beveiliging biedt. Maar voor zakelijk gebruik zijn er zorgen. Want, zo blijkt, in handen van de professional is de iPad eenvoudig te kraken. Hiermee wordt ogenschijnlijk beveiligde informatie toegankelijk. Voor zover bekend is het apparaat nog niet op afstand gekraakt.

Daarnaast kunnen Apps die beschikbaar gesteld worden vanuit de 'App Store' van de leverancier kwaadwillende code bevatten, ondanks de integriteitscontroles die worden uitgevoerd voor publicatie van de App. Kwaadwillenden vinden altijd een weg om onder de radar van de integriteitscontrole te blijven. Het ophalen van een leuk, gratis spel uit de App Store lijkt onschuldig, maar kan ondertussen allerlei gebruikersdata verzamelen.

Voor zakelijk gebruik van een smart device zijn er dus zorgen over de betrouwbaarheid van de Apps, gedreven door de grote schaal waarop deze beschikbaar worden gesteld. Overwogen kan worden om een eigen App Store in te richten of om Mobile Device Management middleware in te zetten. Zo kunnen applicaties aangeboden worden die aan de eigen kwaliteit- en beveiligingscriteria voldoen.

## 4. CONCLUSIE 2: GOED BELEID VORMT DE BASIS

### 4.1 Beleid richten op beperken van risico's

Een smart device, zoals de iPad, integreren in een organisatie vergt goede overweging en de nodige voorbereiding. Denk daarbij bijvoorbeeld aan het vormen van beleid om de verschillende aandachtsgebieden in te kaderen. Een mobiel en veelzijdig apparaat als de iPad brengt een aantal risico's met zich mee. Het is daarom aan te bevelen deze risico's eerst te bekijken, waarop vervolgens een beleid kan worden afgestemd. De risico's zijn over het algemeen niet nieuw, maar worden met de brede acceptatie van de iPad opnieuw actueel.

Mogelijke risico's zijn:

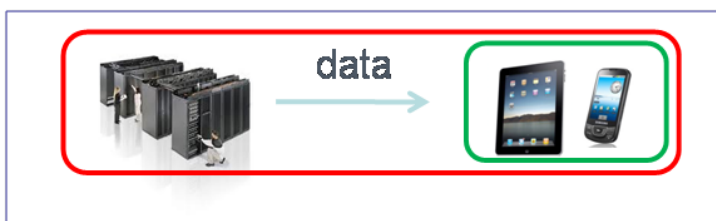
1. Verlies van informatie (meekijken in openbare ruimtes, of een device dat gestolen wordt omdat het een mooie gadget is)
2. Diefstal van informatie (de informatie wordt bewust gestolen)
3. Ongeautoriseerd toegang tot bedrijfsnetwerk (via de smart devices of via de Wi-Fi netwerken die hiervoor aangelegd worden)
4. Imagoschade (vooral afhankelijk van de publieke rol van een organisatie)
5. Traceren van gebruikers van mobiele devices (via netwerklijsten en mac-adressen)

### 4.2 Risico beperken met beveiligingsconcepten

Strict onderscheidt vier beveiligingsconcepten:

1. Lokale beveiliging
2. Beperken informatie
3. Virtuele applicatie (sandbox)
4. Virtuele desktop

#### 4.2.1 Lokale beveiliging



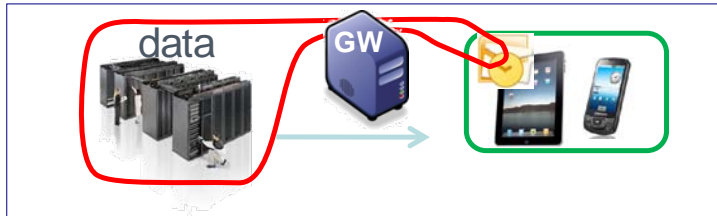
De groene lijn geeft de lokale beveiligingsmaatregelen op het device weer. De rode lijn is de 'invloedsfeer' van de centrale IT-voorzieningen.

In dit concept streeft de organisatie naar volledige beheersing van de beveiliging op mobiele devices. Hierdoor is de beheerlast hoog, zeker als er meerdere type devices ondersteund worden. Alle type devices moeten immers voorzien worden van virusscanners, Intrusion Detection Systemen (IDS) en VPN software.

Met laptops werkt dit concept omdat de beveiliging voornamelijk afhangt van OS en bij laptops is het minder bezwaarlijk te beperken in types en modellen. Bovendien is het met laptops eenvoudiger om een veilige basisinrichting te maken en deze te distribueren.

Visie Strict: Dit concept is niet goed toe te passen op komende ontwikkelingen rond mobiele devices, zeker wanneer het Bring Your Own principe wordt gehanteerd.

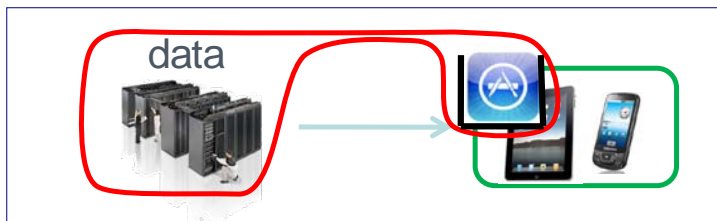
#### 4.2.2 Beperken informatie



Het tweede concept streeft naar beperking van informatie op de mobiele devices. Het is bijvoorbeeld mogelijk om opslag van lokale e-mail te beperken tot 50kb per bericht, waardoor bijlagen meestal niet standaard worden ontvangen op het device. Afhankelijk van het beleid kan de gebruiker zelf beslissen over het ophalen van de bijlage. Dit is dan een bewuste en een afgewogen actie. Mogelijke oplossingen hiervoor zijn: 1. Een portaal waarop bedrijfsinformatie opgehaald kan worden via SSL of 2. Het via Active Sync afdwingen van bepaalde beveiliging, zoals een sterk wachtwoord. Dit concept kan zowel 'connected' als 'not-connected' worden toegepast.

Visie Strict: Dit concept is bruikbaar in omgevingen waar de infrastructuur voorziet in het beperken van informatie naar mobiele devices. Meestal is dit al het geval, waardoor dit concept breed wordt toegepast om de risico's te beperken bij het gebruik van mobiele devices bij het ontsluiten van bedrijfsinformatie.

#### 4.2.3 Virtuele applicatie (sandbox)



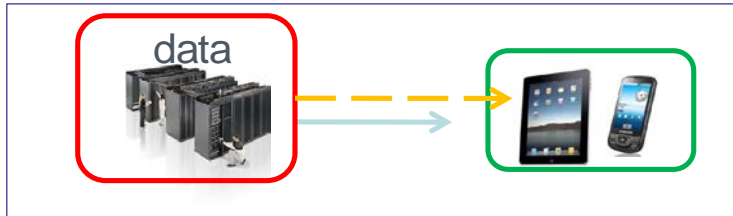
In het geval van een *sandbox* wordt de applicatie, inclusief data, in een afgeschermd deel van het device gedraaid. Op deze manier wordt een deel van het device gemanaged. De virtuele applicatie kan ook offline gebruikt worden (eventueel met een retentieperiode waarna de data vernietigd wordt).

Deze omgeving kan ook versleuteld worden, zodat bij verlies van het device de informatie niet bij ongeautoriseerde personen terecht kan komen.

Op dit moment zijn er zeer beperkt voorbeelden van dergelijke applicaties te noemen. Een voorbeeld is Good mobile messaging ([www.good.com](http://www.good.com)). De verwachting is dat spoedig meerdere bedrijfsapplicaties invulling gaan geven aan dit sandbox model.

Visie Strict: Dit concept is goed bruikbaar voor bedrijfsapplicaties, doordat de toegang tot de applicaties afhankelijk te maken is van plaats, tijd en autorisaties.

#### 4.2.4 Virtuele desktop



Bij een virtuele desktop wordt alleen beeld en toetsenbordinformatie uitgewisseld, desgewenst over een beveiligd kanaal. Hierdoor blijven de applicatie en de informatie in het rekencentrum. Door deze techniek kunnen de huidige bedrijfsapplicaties rechtstreeks ontsloten worden zonder specifieke aanpassingen voor elk device. Leveranciers als Citrix en VMware bieden hier oplossingen voor. Ook is het mogelijk alleen specifieke applicaties virtueel beschikbaar te stellen.

Visie Strict: Dit concept is goed toepasbaar, maar gaat wel uit van “always connected”.

#### 4.2.5 Combinaties van beveiligingsconcepten

Logischerwijs zijn er ook combinaties van de voorgaande vier beveiligingsconcepten denkbaar. Zo kan minder gevoelige informatie beschikbaar gesteld worden via een gateway, terwijl een kritische applicatie via een virtuele desktop loopt.

### 4.3 Kenmerken organisatie bepalen beveiligingsconcept

#### 4.3.1 Organisatie en cultuur

Afhankelijk van de (publieke) rol van de organisatie zal bepaald worden welke beveiligingsmaatregelen dienen te worden toegepast. Een bank of overheidsinstantie ondervindt doorgaans meer imagoschade dan een adviesbureau. Ook de mate van werken met vertrouwelijke informatie is bepalend. Daarnaast is de cultuur binnen de organisatie van belang. Een organisatie waar openheid heerst zal meer vrijheid geven rond het gebruik van mobiele devices. Uiteraard speelt het bewustzijnsniveau van de medewerkers hierbij een essentiële rol.

#### 4.3.2 Dreigingsprofiel

Met betrekking tot het dreigingsprofiel is de vraag die beantwoord moet worden: *Wie zou met welke motivatie informatie willen compromitteren of beschikbaarheid willen beperken van de organisatie?* Bij een instantie binnen de veiligheidssector komt de dreiging uit een andere hoek dan bij een beursgenoteerd bedrijf of een researchafdeling.

#### 4.3.3 Type applicatie

Bij toepassingen voor kantoorautomatisering (KA) wordt over het algemeen minder gevoelige en gefragmenteerde informatie beschikbaar gesteld dan bij bedrijfsapplicaties. Met zakelijke toepassing bestaat het gevaar dat bij toegang de volledige database met gevoelige informatie beschikbaar wordt gesteld. Daarom wordt voor zakelijke toepassingen vaak een bredere risicoanalyse uitgevoerd dan voor KA. In dat geval zullen de maatregelen voor KA anders zijn dan voor de zakelijke toepassing. De gebruikers begrijpen dat de maatregelen strikter worden naarmate de vertrouwelijkheid toeneemt.

#### 4.3.4 Plaats en tijd

Er kan onderscheid worden gemaakt tussen een verbinding via het gebouwnetwerk en een verbinding via een openbaar netwerk. Als de gebruiker buiten het bereik van het gebouwnetwerk is, dan gelden andere maatregelen. Ook kunnen autorisaties afhankelijk worden gemaakt van het tijdstip, GPS-coördinaten en/of het dienstrooster van de gebruiker.



## 5. CONCLUSIE 3: RISICOPROFIEL EN CULTUUR BEPALEN SUCCES VAN BYO CONCEPT

### 5.1 Organisaties kiezen tussen Unmanaged (BYO) en Managed omgeving

Veel bedrijven worden geconfronteerd met het BYO (Bring Your Own) concept, vanwege het grote succes van de iPad en adoptie ervan tot op bestuursniveau. Zij kiezen hiermee voor de *Unmanaged* omgeving.

Aan de andere kant zullen instanties met een hoog dreigingsprofiel blijven vasthouden aan een *Managed* omgeving. Op die manier kan de IT-afdeling de end-to-end verantwoordelijkheid optimaal borgen.

Bij het kiezen van Managed devices zullen bedrijven vooral uitgaan van leveranciers die ook centrale device management toepassingen bieden, zoals bij de BlackBerry. Inmiddels is er ook device management software van Apple beschikbaar voor het centraal beheren van iPhones en iPads.

### 5.2 Managed bij zwaar dreigingsprofiel

Organisaties uit de sector Openbare Orde en Veiligheid (OOV) kiezen vooral voor centraal beheerde devices (Managed). Via deze devices kunnen gebruikers toegang krijgen tot vertrouwelijke en/of geheime informatie. Deze devices worden uitsluitend zakelijk ingezet.

### 5.3 Unmanaged (BYO) bij lichter dreigingsprofiel

Bij organisaties met een lichter dreigingsprofiel is het eerder toegestaan om eigen apparatuur in te zetten (Unmanaged). De gebruiker is dan ook zelf verantwoordelijk voor het juiste gebruik van het device. Het is wel verstandig de gebruiker een overeenkomst te laten tekenen. Hiermee wordt een eerste stap gezet in het verhogen van het bewustzijn van de gebruiker.

Om te voorkomen dat er toch lastige ondersteuningsvragen bij de helpdesk terecht komen, overwegen veel organisaties wel om het aantal type devices of operating systemen (bijvoorbeeld iOS 4+ en Android 2.2+) te beperken. Hiermee bereikt men niet een zuivere vorm van BYO (any device), maar wel een vorm die beter haalbaar en beter beheerbaar is.

Daarnaast is het aanbieden van applicaties in een browser of via desktopvirtualisatie een manier om vragen bij de helpdesk terug te dringen.



## **6. CONCLUSIE 4: NU IS HET MOMENT OM BEWUSTWORDING EXTRA AANDACHT TE GEVEN**

### **6.1 Herhaal bewustwording regelmatig**

Het toestaan van het gebruik van een smart device voor zakelijke toepassingen wordt als zeer wenselijk gezien om uiteenlopende redenen. Denk daarbij aan flexibiliteit, imago, plezier, etc.

Uit deze whitepaper blijkt dat de beveiliging van een smart device voor een groot deel afhankelijk is van hoe de gebruiker ermee omgaat. Het volledig technisch beveiligen van een smart device is namelijk onhaalbaar en onwenselijk. De drive van medewerkers en bestuurders voor het gebruik van smart devices biedt daarmee een uitgelezen kans voor bewustwording. 'In ruil' voor het toestaan van de smart device voor zakelijk gebruik wordt van de medewerker verwacht aandacht te besteden aan het verhogen van bewustwording rond informatiebeveiligingsrisico's. Die bewustwording moet zich dan niet beperken tot het gebruik van het smart device, maar breder, omwille van de kwaliteit van de beveiliging. Daarbij dient gezorgd te worden voor regelmatige herhaling van de bewustwording door middel van training, zodat de opgedane kennis actueel blijft.

### **6.2 Gedragscode maakt gebruiker medeverantwoordelijk**

Er dient een gedragscode te worden opgesteld voor gebruikers die met hun eigen devices (BYO) toegang krijgen tot bedrijfsinformatie en applicaties. Daarmee krijgen de gebruikers meer vrijheid in hun keuzes, in ruil voor meer verantwoordelijkheid. Een gedragscode is vrijblijvend, maar geeft wel aan wat een organisatie van haar medewerkers verwacht.

### **6.3 Aansluitvoorwaarden vormen sluitstuk**

Het laten ondertekenen van aansluitvoorwaarden is een manier om in concrete vorm daadwerkelijke verantwoordelijkheden af te dwingen bij de gebruiker. Voordat gebruik wordt gemaakt van toegangsmogelijkheden met de mobiele devices dient de gebruiker de voorwaarden te hebben ondertekend. Eventueel kan in de aansluitvoorwaarden worden opgenomen dat de gebruiker (regelmatig) deelneemt aan bewustwordingstrainingen.



## 7. CONTACT

Wilt u meer informatie omtrent het beveiligen van smart devices binnen uw organisatie? Dan kunt u contact opnemen met:

Arnold Jessurun  
Managing Consultant bij onafhankelijk ICT adviesbureau Strict  
Afdeling Strict Security Management

06-27085902  
[a.jessurun@strict.nl](mailto:a.jessurun@strict.nl)

[www.strict.nl](http://www.strict.nl)