# Informatiebeveiliging
## iPhones en iPads

Mobile Internet Devices (MID) zijn enorm in opkomst. Ze worden tegenwoordig steeds vaker gebruikt voor zakelijke toepassingen. Dit brengt veel voordelen met zich mee en het ligt geheel in lijn met de trend die ook wel Het Nieuwe Werken wordt genoemd. Naast voordelen brengt het gebruik van MID voor zakelijke toepassingen voor organisaties ook nieuwe uitdagingen met zich mee op het gebied van informatiebeveiliging. Op welke wijze kan informatiebeveiliging gewaarborgd worden wanneer MID toegang hebben tot bedrijfsinformatie? Dit artikel richt zich op de behandeling van dit vraagstuk en wel specifiek op de Apple-toestellen iPhones en iPads. De hiermee samenhangende informatiebeveiligingsrisico's en de mogelijkheden om deze te behandelen, hebben wij in kaart gebracht aan de hand van literatuurstudie, vier interviews en een survey.

CHEE-KEAN CHOW EN MICHEL KRUL

Het zakelijk gebruik van Mobile Internet Devices (MID) is in opkomst en deze groei zal zich naar verwachting voortzetten vanwege de vele mogelijkheden die deze toestellen bieden. De mogelijkheid om (kantoor)applicaties te installeren, e-mails te lezen en het snelle mobiele internet maken de MID handig voor onderweg en hebben bijgedragen aan de populariteit van deze toestellen.

Het zakelijk gebruik van MID leidt echter ook tot nieuwe risico's of een toename van bestaande risico's op het gebied van informatiebeveiliging. Verlies en diefstal van MID zijn voorbeelden van dergelijke risico's. Hierdoor kan bedrijfsgevoelige informatie op straat komen te liggen. Ook de vermenging van zakelijk en privégebruik op hetzelfde toestel kan leiden tot extra risico's op het gebied van informatiebeveiliging. Zo haalt Whatsapp standaard alle personen uit de contactenlijst binnen [REIJ13]. Deze kan ook zakelijke contactgegevens bevatten.

Een grote uitdaging op het gebied van informatiebeveiliging bij de implementatie van MID is de diversiteit van de mobiele platforms, zoals bijvoorbeeld Android, iOS, Windows Phone en Blackberry. Deze platforms onderscheiden zich onder andere in de beveiligingsmaatregelen die zij ondersteunen. Hierdoor bestaan er verschillen tussen de verschillende soorten toestellen/platforms voor wat betreft de inrichting van (aanvullende) beveiligingsmaatregelen die de organisatie dient te nemen. Vanwege deze diversiteit is er voor gekozen om dit artikel toe te spitsen op één platform, namelijk iOS, het besturingssysteem dat draait op Apple iPhones en iPads. Dit onderzoek richt zich op het besturingssysteem iOS 5, omdat bij aanvang van het onderzoek dit besturingssysteem de meest recente versie was. De huidige versie, iOS 6, bevat ten opzichte van iOS 5 geen significante veranderingen op het gebied van informatiebeveiliging. Derhalve zijn de in dit artikel gepresenteerde beheersmaatregelen ook voor iOS 6 van toepassing.

Er is gekozen voor de Apple-toestellen omdat deze populair zijn in de zakelijke wereld en Apple tevens pretendeert dat iOS geschikt is voor zakelijk gebruik. Waar in het vervolg van dit artikel gesproken wordt over MID, wordt bedoeld iPhones en iPads.

Met dit artikel willen we bijdragen aan de bewustwording ten aanzien van extra beveiligingsrisico's die de uitgifte van MID voor zakelijk gebruik met zich meebrengen. Tevens willen we bijdragen aan de bewustwording van het feit dat de toepassing van nieuwe technieken, nieuwe beveiligingsrisico's met zich

meebrengt, en dus gepaard dient te gaan met een herbeoordeling van het informatiebeveiligingsframework.

## RISICO'S

Bij de vaststelling van de MID-gerelateerde risico's is uitgegaan van de volgende definiëring: 'De informatiebeveiligingsincidenten die zich als gevolg van het zakelijk gebruik van MID (iPhones of iPads) kunnen voordoen, of waarvoor geldt dat de kans dat deze zich voordoen als gevolg van het zakelijk gebruik van MID toeneemt, en die kunnen leiden tot aantasting van de vertrouwelijkheid, integriteit en/of beschikbaarheid van informatie.'

Uitgaande van deze definitie zijn tijdens het onderzoek de volgende MID-gerelateerde risico's geïdentificeerd:

### Verlies en diefstal

Door het kwijtraken van het toestel of diefstal kunnen het toestel en de opgeslagen data in handen van onbevoegden terechtkomen. Indien het toestel tevens toegang verleent tot het bedrijfsnetwerk kan verlies en diefstal leiden tot ongeautoriseerde toegang tot het bedrijfsnetwerk.

### Kwaadaardige apps

Er wordt een applicatie, of app, op het toestel geïnstalleerd, die doelbewust de vertrouwelijkheid, integriteit of beschikbaarheid van data probeert aan te tasten.

### Onbeveiligde gegevensuitwisseling

De mobiliteit van het toestel brengt met zich mee dat gebruikers het

vaak onderweg bij zich hebben. Wanneer op sommige locaties een slechte (3G-)verbinding is of wanneer grote bestanden verstuurd moeten worden, dan kan dit een aanleiding zijn om gebruik te maken van een openbare wifi-hotspot. Het risico bestaat dat een hacker het communicatieverkeer tussen het toestel en de wifi-hotspot onderschept (man-in-the-middle attack). Dit risico wordt groter wanneer er gebruik gemaakt wordt van een onbeveiligde wifi-hotspot.

### Onbewuste gegevensverstrekking

De gebruiker verstrekt onbewust gegevens. Dit gebeurt wanneer apps of andere personen meekijken, zonder dat de gebruiker zich hiervan bewust is. In het geval van meekijken door apps gaat het hier niet om kwaadaardige apps, maar om apps die informatie verzamelen om bepaalde diensten te kunnen aanbieden (bijvoorbeeld navigatiediensten). Gevolg kan onder andere zijn dat anderen inzicht hebben in de locatie waar de gebruiker zich bevindt.
Naast apps kunnen ook andere personen al dan niet ongemerkt meekijken naar de activiteiten die op het scherm van de MID plaatsvinden. De gebruiker kan hierdoor onbedoeld derden inzicht geven in bedrijfsgegevens. Deze laatste situatie speelt meer bij iPads omdat iPads een groter beeldscherm hebben.

### Ongecontroleerde externe opslag

Het gebruik van MID stimuleert gebruikers om gegevens op externe locaties, zoals bepaalde clouddiensten, op te slaan. Wanneer bedrijfsgegevens eveneens buiten het bedrijfsnetwerk worden opgeslagen, dan heeft de organisatie geen grip meer op de desbetreffende bedrijfsgegevens.

### Onzorgvuldige buitengebruikstelling

Wanneer een toestel buiten gebruik gesteld moet worden, dan mag het toestel vanaf dat moment geen bedrijfsgegevens meer bevatten en/of toegang meer hebben tot het bedrijfsnetwerk. Dit zou voor alle hardware moeten gelden, echter, voor iPhones en iPads is de kans groot dat men zich er minder van bewust is dat hierop ook bedrijfsdata zijn opgeslagen, waardoor een zorgvuldige buitengebruikstelling minder vanzelfsprekend is [HOGB10].

### Modificatie

Apple voert een restrictief beleid ten aanzien van het toestaan van modificaties aan de basisfunctionaliteit die de iPhone en iPad bieden. Deze restricties beperken het gebruik van het toestel tot toepassingen die door Apple geautoriseerd zijn. Als gevolg hiervan kunnen apps uitsluitend vanuit de door Apple gecontroleerde App Store geïnstalleerd worden. Wanneer er een softwarematige modificatie ten aanzien van het besturingssysteem op het toestel wordt uitgevoerd (*jailbreak*), dan kunnen deze technische restricties en beveiligingsmaatregelen omzeild worden. Gebruikers kunnen hiermee verhoogde rechten verkrijgen op het toestel (root rechten) waarmee ze toegang hebben tot het complete bestandssysteem en commandoregels, waardoor zij elk bestand kunnen wijzigen, wissen of toevoegen. Tevens ontstaat hierdoor de mogelijkheid om apps die niet door Apple zijn geautoriseerd, te installeren. Dit laatste vergroot het risico van het installeren van kwaadaardige apps.
Hoewel jailbreaken op zichzelf nog niet de vertrouwelijkheid, integriteit en beschikbaarheid van gegevens aantast, vergroot dit wel de kans dat de overige risico's die in dit artikel worden genoemd zich voordoen.

### Bezoek aan een malafide website

Vanuit bezochte (malafide) websites kunnen zogenaamde *browser based attacks* plaatsvinden. De bezochte website veroorzaakt een verbinding tussen het toestel en een hacker. De hacker stuurt commando's waarbij gebruikgemaakt wordt van beveiligingslekken in de browser. Hierdoor kan de hacker toegang krijgen tot niet afgeschermde data op het toestel [JUNI12], [NACH11].
Wij beschouwen dit als een MID-specifiek risico omdat er een aantal factoren zijn die dit risico vergroten. Het kleinere scherm kan ertoe leiden dat bepaalde kenmerken waaruit de beveiliging van een website blijkt (zoals de 's' van https) minder snel opvallen [HOGB10]. Daarnaast zijn gebruikers zich vaak minder bewust van de informatiebeveiligingsrisico's bij het gebruik van de MID.

### Reageren op phishing-bericht

Door het reageren op valse sms' en of e-mailberichten kunnen de toegangsgegevens van gebruikers worden onderschept. Dit wordt eveneens in de hand gewerkt vanwege het kleinere scherm waarop betrouwbaarheidskenmerken minder snel opvallen [HOGB10] en doordat de gebruikers zich vaak minder bewust zijn van de informatiebeveiligingsrisico's bij het gebruik van de MID.

### Delen toestel

De combinatie van zakelijk en privé gebruik vergroot de kans dat het toestel wordt gedeeld met anderen, zoals vrienden en/of familieleden. Het gebruik door vrienden of familieleden vergroot de kans op ongeautoriseerde toegang tot bedrijfsdata. Dit risico is vooral van toepassing op iPads vanwege de aard (groter beeldscherm, toegankelijkheid, e.d.) van het toestel. Daarnaast is een iPhone veel persoonlijker dan een iPad, waardoor een iPhone minder snel wordt gedeeld.

## OMGANG MET RISICO'S

Er zijn verschillende mogelijkheden om met risico's om te gaan. Het proces van identificeren en beoordelen van risico's en het vaststellen en maken van een keuze uit de verschillende mogelijkheden, vindt plaats binnen de planfase van het

Plan-Do-Check-Act model van het ISO 27000-normenkader.

Het ISO 27000-normenkader noemt de volgende mogelijkheden om met risico's om te gaan:

- Het risico mitigeren - de mogelijkheden hiertoe worden in dit artikel nader beschreven.
- Het aanvaarden van risico's - aan de hand van de criteria voor de aanvaarding van risico's, die voortvloeien uit het beleid van de organisatie, kan de directie besluiten bepaalde (rest)risico's te aanvaarden.
- Risico's vermijden - hierbij kan gedacht worden aan het beperken van de mate waarin bedrijfsfunctionaliteiten op MID beschikbaar gesteld worden.
- De risico's overdragen aan derden - hier wordt in dit artikel niet nader op ingegaan. Reden hiervoor is dat het onderzoek zich met name richt op de vraag hóe risico's beheerst kunnen worden, en niet op de vraag wáár risico's beheerst kunnen worden.

De organisatie kan een keuze maken uit deze mogelijkheden. Deze keuze hangt voor een groot deel af van het bestaande informatiebeveiligingsbeleid, de cultuur van de organisatie en de doelstellingen die de organisatie met het uitrollen van MID beoogt.

## GEÏNTEGREERDE BEHEERSMAATREGELEN IOS

Dit artikel zal nader ingaan op de mitigerende maatregelen. Apple heeft een aantal maatregelen binnen het iOS-platform geïntegreerd. Deze maatregelen, waar je als organisatie geen invloed op hebt, worden in deze paragraaf beschreven. In de paragraaf Overige mitigerende maatregelen zal nader worden ingegaan op mogelijke aanvullende mitigerende maatregelen.

### Hardware encryptie

In elk Apple-toestel bevindt zich een hardware module, ofwel de crypto engine, die voor de encryptie van alle gegevens op het toestel zorgt. Deze crypto engine houdt zich bezig met het versleutelen en ontsleutelen van gegevens op momenten dat deze gegevens benaderd moeten worden door applicaties op het toestel. De crypto engine maakt hierbij gebruik van een uniek nummer, waarmee elk Apple-toestel is uitgerust.
Voordeel van hardware encryptie vanuit beveiligingsoogpunt is dat de gegevens in het geheugen van het toestel niet door andere apparaten ontsleuteld kunnen worden, zonder het unieke nummer van het apparaat dat deze encrypt heeft [APPL12]. De beperking van hardware encryptie is dat wanneer een onbevoegde zichzelf toegang tot het toestel weet te verschaffen, bijvoorbeeld als gevolg van een jailbreak, deze onbevoegde meteen toegang tot de data op het toestel heeft. Dit komt omdat de crypto engine de aangeroepen data automatisch ontsleutelt, zonder dat hier een toegangscode voor ingegeven hoeft te worden.
Apple heeft de hardware encryptie ingebouwd om onder meer een snelle uitvoering van *remote wipe* (zie verderop) mogelijk te maken, omdat hierbij alleen de decryptie key vervangen hoeft te worden, waarna de met de oude encryptie key versleutelde data niet meer teruggelezen kunnen worden [HOLL12].

### Dataprotectie

Dataprotectie is een aanvullende encryptielaag bovenop hardware encryptie.
Het doel van dataprotectie is om het toestel te laten reageren bij bepaalde gebeurtenissen, zoals een binnenkomend gesprek, sms en/of email, zonder dat bepaalde gevoelige gegevens ontsleuteld worden. De aan gegevens toegekende beveiligings-class bepaalt in welke situaties deze gegevens benaderd mogen worden. De gegevens worden aan een beveiligingsclass gekoppeld door de app die de gegevens beheert. Afhankelijk van de beveiligingsclass vindt extra versleuteling plaats met behulp van het gebruikerswachtwoord [APPL12].
Apps die gebruik willen maken van de faciliteiten die dataprotectie biedt, dienen de daarvoor vereiste API's te gebruiken die Apple voorschrijft. *Van third party apps* waarbij bedrijfsdata wordt gebruikt, dient dus eerst vastgesteld te worden of zij de vereiste API's aanroepen om dataprotectie effectief te gebruiken [HOLL12].

### Remote wipe

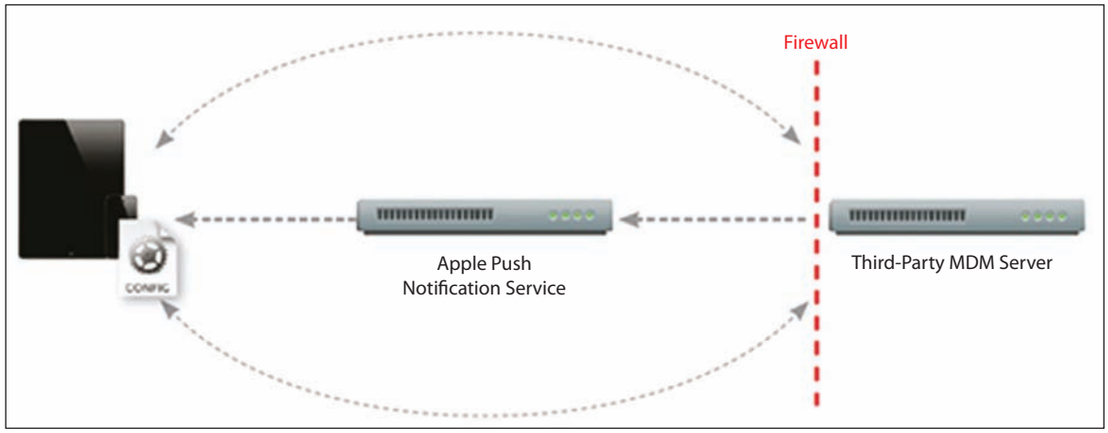
Als een apparaat is verloren of gestolen, dan kan de beheerder of de eigenaar van het apparaat een remote wipe commando geven. Dit leidt ertoe dat op afstand de decryptie key vervangen wordt, waardoor de met de oude encryptie key versleutelde gegevens op het toestel onleesbaar worden. Voor een succesvolle uitvoering is wel een connectie van het toestel met het internet vereist.

### Sandboxing

*Sandboxing* is een techniek voor het creëren van afgeschermde omgevingen. Een sandbox is een container die ervoor zorgt dat verschillende applicaties van elkaar gescheiden blijven. De apps kunnen hierdoor niet rechtstreeks data benaderen die door een andere app beheerd worden. Raadplegen van gegevens van andere apps is uitsluitend mogelijk met behulp van speciaal hiervoor ontwikkelde API's. In dat geval heeft de ontwikkelaar van de app bewust de keuze gemaakt om deze gegevens inzichtelijk te maken. Een aantal functionaliteiten is standaard benaderbaar voor apps, en wordt derhalve niet door sandboxing afgeschermd, zoals de contactpersonen, de kalender, de fotogalerij, de browsehistorie, de microfoon en de videocamera [NACH11].

### Verplichte code signing

Code signing is een cryptografische techniek waarmee de integriteit en authenticiteit van programmatuur ▶




*Figuur 1: Illustratie van de werking van de Apple Push Notification Service*

kan worden gewaarborgd. Dit wordt zowel op de besturingssoftware als op apps toegepast. Met behulp van deze techniek wordt programmatuur door de ontwikkelaar voorzien van een digitale handtekening, gebaseerd op een door Apple verstrekt certificaat. Deze handtekening maakt onderdeel uit van het bestand dat de programmacode bevat.
Alle apps in de App Store moeten zijn voorzien van deze digitale handtekening. Bovendien voert Apple ook controles uit op de apps in de App Store met als doel om kwaadaardige apps buiten de deur te houden.

### Versleutelde digitale sleutelhanger (keychain)

IPads en iPhones zijn voorzien van een (met encryptie) beveiligde digitale sleutelhanger (keychain) voor het bewaren van usernames en passwords. De in de keychain opgeslagen gegevens zijn van elkaar gescheiden. De toegangsgegevens die door een app zijn opgeslagen, kunnen hierdoor niet worden benaderd door andere apps [APPL12].

## OVERIGE MITIGERENDE MAATREGELEN

Naast de in het iOS-platform geïntegreerde beheersmaatregelen, biedt Apple ook de mogelijkheid om aanvullende mitigerende beheersmaatregelen in te richten. Bij het maken van keuzes uit aanvullende beheersmaatregelen dient de organisatie te bepalen in hoeverre de MID gerelateerde risico's verder gemitigeerd moeten worden om deze tot een voor de organisatie aanvaardbaar niveau terug te brengen. De mogelijkheden voor het nemen van aanvullende mitigerende maatregelen worden hierna beschreven.

### iPhone configuration utility

De iPhone configuration utility is een applicatie waarmee configuratie profielen vanuit de organisatie aangemaakt en beheerd kunnen worden. Met behulp van deze configuratieprofielen kunnen per afzonderlijk toestel meer soorten instellingen afgedwongen worden, waaronder wachtwoordvereisten en beperkingen in de functionaliteiten van het toestel. De aangemaakte (updates van) configuratieprofielen kunnen vanuit de organisatie op drie verschillende manieren naar het toestel worden gedistribueerd, namelijk met een USB-kabel, per e-mail of door het configuratieprofiel beschikbaar te stellen op een website. Beperking van de laatste twee mogelijkheden is dat het configuratieprofiel nog wel actief door de gebruiker geïnstalleerd moet worden. Wanneer gebruikers weigeren om een configuratieprofiel te installeren, dan voldoet het toestel niet aan de beveiligingsstandaarden van de organisatie. De iPhone configuration utility biedt geen mogelijkheden om dit op afstand te controleren.

### Mobile Device management Services (MDM)

Wanneer aanvullend gebruik wordt gemaakt van MDM-oplossingen, is het wel mogelijk om updates van configuratieprofielen op toestellen te installeren zonder actieve goedkeuring van de gebruikers. MDM-oplossingen bieden de mogelijkheid om de in omloop zijnde toestellen op afstand te beheren. Er zijn meer leveranciers die MDM-oplossingen bieden, die vaak meer platforms kunnen ondersteunen. Apple faciliteert het gebruik van MDM-oplossingen met behulp van de Apple Push Notification Service, waarmee aan een beheerd toestel een wake-upcall gegeven kan worden, waarna het toestel zelf contact opneemt met de MDM-server [APPL11-2]. In figuur 1 wordt de werking van de Apple Push Notification Service geïllustreerd.

MDM-oplossingen bieden tevens de mogelijkheid om bepaalde *queries* ten aanzien van de beheerde toestellen te draaien en op afstand apps te installeren of verwijderen. Verder kunnen MDM-oplossingen functionaliteit bieden om op afstand te controleren of er een jailbreak op een beheerd toestel heeft plaatsgevonden.

### Beveiliging communicatie

De iPhone en iPad ondersteunen de mogelijkheid om een beveiligde Virtual Private Network (VPN)

verbinding in te richten. Ook het gebruik van certificaten en het gebruik van multifactor authenticatie, wordt ondersteund [APPL11-1].

### Secure container

De secure container is een beveiligingsconcept waarbij een scheiding tussen privé en zakelijke data op het toestel wordt aangebracht. Dit wordt bewerkstelligd met behulp van een speciaal hiervoor ontwikkelde app, bijvoorbeeld de Good app. Dit werkt als een beveiligde container voor de zakelijke data. Wanneer een gebruiker voor privégebruik een back-up maakt, dan worden de zakelijke gegevens hierbij niet meegenomen. Alleen vanuit de secure container kan een verbinding met het netwerk van de organisatie gemaakt worden, waarbij gegevens worden gesynchroniseerd.

### Remote desktop

Remote desktop is een beveiligingsconcept waarbij de MID op afstand op de bedrijfscomputer kunnen inloggen. Gegevens op het bedrijfsnetwerk kunnen vervolgens geraadpleegd en eventueel bewerkt worden. Gegevens worden niet op het toestel opgeslagen. Een voorbeeld hiervan is het inloggen op een Citrix omgeving met de iPad voor het benaderen van de bedrijfsdata.

### Specifieke apps ten behoeve van beveiliging

Er bestaan apps in de App Store die extra beveiligingsmogelijkheden bieden. Zo zijn er apps beschikbaar waarmee e-mail en sms-berichten met een wachtwoord kunnen worden beveiligd, zoals de app SMS Secret Coder. Een ander voorbeeld betreft de app Private Folder waarmee een met een wachtwoord beveiligde folder op de MID kan worden aangemaakt. Indien de gebruiker een iPad deelt met familieleden of vrienden, dan kunnen de zakelijke gegevens in deze private folder worden opgeslagen. De private folder is met een wachtwoord beveiligd.

Daarnaast bestaat de mogelijkheid om eigen apps te ontwikkelen voor aanvullende beveiligingsdoeleinden, bijvoorbeeld een app ten behoeve van biometrische verificatie.

### Fysieke beveiligingsmaatregelen

Ter voorkoming van diefstal van een iPad zijn er bepaalde fysieke beheersmaatregelen voorhanden. Bij een iPad zal zich, vergeleken met een iPhone, sneller de situatie voordoen dat deze noodgedwongen tijdelijk onbeheerd achtergelaten moet worden. Een iPhone kan je nu eenmaal makkelijker meenemen in je binnenzak. Om te voorkomen dat een iPad op zulke momenten ontvreemd wordt, zijn er fysieke beveiligingssloten beschikbaar waarmee de iPad aan ieder willekeurig immobiel voorwerp kan worden vastgemaakt.

Een ander voorbeeld van een fysieke beheersmaatregel is de privacybeschermer voor de iPad. Dit betreft een soort folie die over het scherm van de iPad kan worden aangebracht. De folie belet het meekijken door anderen doordat het scherm alleen goed zichtbaar is wanneer de gebruiker er recht voor zit.

### Procedurele maatregelen en bewustzijn gebruiker

Naast de technische maatregelen blijven alertheid van gebruikers op mogelijke risico's en een verantwoordelijke manier waarop de gebruikers met hun toestel omgaan heel belangrijk.
Zo is het van belang dat de gebruiker de toegangscode van zijn toestel niet aan anderen prijsgeeft en bij het ingeven van de toegangscode niet te gemakkelijk anderen op het scherm laat meekijken.
Gebruikers dienen bij het aanroepen van kritische data alert te zijn op het beveiligd zijn van de verbinding. Tevens is het van belang dat de gebruiker op de juiste manier handelt bij vermissing van het toestel en bij situaties waarbij een toestel gerepareerd dient te worden. Verder dienen de juiste handelingen te worden verricht met betrekking tot de data op het toestel bij uitdiensttreding van de gebruiker of bij buiten gebruikstelling van het toestel.

Organisaties waarbij de MID bij de uitoefening van de bedrijfsactiviteiten wordt gebruikt, dienen een beleid te hebben dat erin voorziet dat het gebruikersbewustzijn in dit kader op een voldoende niveau aanwezig is.

## CONCLUSIE

Gedurende het literatuuronderzoek en het praktijkonderzoek zijn in totaal tien MID-specifieke beveiligingsrisico's geïdentificeerd, die ontstaan of toenemen bij het zakelijk gebruik van MID. Op basis hiervan hebben we vastgesteld dat een introductie van MID voor zakelijk gebruik gevolgen heeft voor het informatiebeveilgingsframework van de organisatie.
Uit het onderzoek is gebleken dat er voldoende mogelijkheden aanwezig zijn om de geïdentificeerde risico's in vergaande mate te mitigeren.
Voor wat betreft het risico van modificatie geldt echter wel dat dit moeilijk te beheersen is. Modificatie leidt ertoe dat de beveiligingsmaatregelen die geïntegreerd zijn in de architectuur van Apple, wegvallen. Dit vergroot de kans dat andere risico's zich voordoen.
Om die reden wordt aanbevolen om gebruik te maken van jailbreakdetectie. Dit kan gerealiseerd worden door gebruik te maken van MDM-oplossingen. Daarnaast bieden de leveranciers van de secure container en remote desktop oplossingen ook jailbreak-detectiemogelijkheden.

Echter, hoe sterk de technische beheersmaatregelen ook zijn, een belangrijke randvoorwaarde is uiteindelijk ook het beveiligingsbewustzijn van gebruikers en de wijze waarop gebruikers met hun verantwoordelijkheden (en hun toestellen) omgaan. Technische beheersmaatregelen kunnen veilig gedrag wel ondersteunen, maar niet vervangen. Beleid ten

| Beheersmaat-regelen / Risico's | | Verlies en diefstal | Kwaadaar-dige apps | Onbeveiligde gegevens-uitwisseling | Onbewuste gegevens-verstrekking | Externe opslag | Onzorgvuldige buiten gebruik stelling | Modificatie | Malafide website | Phishing bericht | Delen toestel |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Geïntegreerde beheersmaatregelen | Hardware encryptie | x | | | | | | | | | |
| | Data protectie | x | | | | | | | | | |
| | Remote wipe | x | | | | | x | | | | |
| | Sandboxing | | x | | x | | | | x | | |
| | Verplichte code signing | | x | | | | | | | | |
| | Keychain | | | | | | | | x | x | |
| Overige mitigerende maatregelen | Mobile Device Management oplossingen (MDM) | x | x | | x | x | x | x | x | | |
| | iPhone Configuration Utility (o.a. wachtwoordinstellingen, Toestelbeperkingen, Local wipe) | x | x | | x | x | x | | x | | |
| | Beveiliging communicatie | | | x | | | | | | x | x |
| | Secure container | x | | | x | x | x | | x | | x |
| | Remote desktop | x | | | x | x | x | | x | | x |
| | Specifieke apps ten behoeve van beveiliging | x | | x | x | | | | x | | x |
| | Fysieke beveiligings- maatregelen | x | | | x | | | | | | |
| | Procedurele maatregelen en bewustzijn gebruikers | x | x | x | x | x | x | x | x | x | x |

*Figuur 2: geeft de geïdentificeerde risico's weer plus de maatregelen waarmee dit risico gemitigeerd kan worden.*

behoeve van dit bewustzijn onder de gebruikers is daarom van belang.

## TOT SLOT

Ontwikkelingen op het gebied van MID gaan op dit moment zeer snel. Dat geldt zowel voor de beveiliging als voor de bedreigingen. Het informatiebeveiligingsframework dient voor wat betreft de beheersing van MID gerelateerde risico's regelmatig gereviewed en geactualiseerd te worden.

Gedurende het praktijkonderzoek zijn nog een aantal algemene aandachtspunten naar voren gekomen die van belang zijn voor een succesvolle introductie van MID.

- De introductie van MID dient mede gezien de vele keuzes die dit met zich meebrengt, als een project te worden ingericht. Met inbegrip van een project initiatiedocument, een risicoanalyse en een testtraject.
- Naast de uitgangssituatie van dit onderzoek, waarbij de organisatie de toestellen verstrekt aan medewerkers, kan het zijn dat er binnen dezelfde organisatie ook sprake is van een BYOD (Bring your own device) of CYOD (Choose your own device) traject. In dat geval is bij de keuze van maatregelen, samenhang tussen deze trajecten van belang.
- Het te ver doorvoeren van technische maatregelen kan averechts werken. Wanneer dit er toe leidt dat gebruikers in te grote mate beperkt worden, dan leidt dit ertoe dat gebruikers 'andere wegen gaan bewandelen', waardoor de risico's alsnog blijven bestaan. Bij de inrichting van maatregelen dient hiermee rekening te worden gehouden. ■

**C. (Chee-Kean) Chow MSc EMITA** is werkzaam als Senior IT-auditor bij Ernst & Young. In 2012 heeft Chee-Kean de postinitiële opleiding IT-Auditing & Advisory aan de Erasmus School of Accounting & Assurance (ESAA) in Rotterdam afgerond.

**M. (Michel) Krul EMITA** is sinds mei 2011 werkzaam als Internal Auditor bij Hof Hoorneman Bankiers. In 2012 heeft Michel de postinitiële opleiding IT-Auditing & Advisory bij de Erasmus Universiteit Rotterdam afgerond.

**Literatuur**

[APPL11-1] Apple, *iPad in business*, 2011.
[APPL11-2] Apple, *Deploying iPhone and iPad*, 2011.
[APPL12] Apple, *iOS Security*, mei 2012.
[HOGB10] ENISA European Network and Information Security Agency , Dr Giles Hogben, Dr Marnix Dekker, Smartphones - *Information security risks, opportunities and recommendations for users*, december 2010.
[HOLL12] Jesse Hollington, *iOS Encryption and Data Protection*, augustus 2012. Zie http://www.ilounge.com/index.php/articles/comments/ios-encryption-and-data-protection/.
[JUNI12] Juniper, 2011 *Mobile Threaths Report*, februari 2012.
[NACH11] Symantec, Carey Nachenberg, *A window into mobile device security*, juni 2011.
[NENI05] NEN-ISO/IEC 27001, *Informatietechnologie-Beveiligingstechnieken-Managementsystemen voor informatiebeveiliging- Eisen*, november 2005.
[REIJ13] Dimitri Reijerman, CBP: *WhatsApp schend privacy op diverse punten*, januari 2013. Zie http://tweakers.net/nieuws/86914/cbp-whatsapp-schendt-privacy-op-diverse-punten.html.