Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

» Beveiligingsrichtlijnen voor mobiele apparaten »

Deel 1

»Beveiligingsrichtlijnen voor mobiele apparaten»

Deel 1

Nationaal Cyber Security Centrum
Wilhelmina van Pruisenweg 104 | 2595 AN Den Haag
Postbus 117 | 2501 CC Den Haag

T 070-888 75 55
F 070-888 75 50

E info@ncsc.nl
I www.ncsc.nl

November 2012

Nationaal Cyber Security Centrum
Het Nationaal Cyber Security Centrum (NCSC) draagt via samenwerking tussen bedrijfsleven, overheid en wetenschap bij aan het vergroten van de weerbaarheid van de Nederlandse samenleving in het digitale domein.
Het NCSC ondersteunt de Rijksoverheid en organisaties met een vitale functie in de samenleving met het geven van expertise en advies, response op dreigingen en het versterken van de crisisbeheersing. Daarnaast voorziet het in informatie en advies voor burger, overheid en bedrijfsleven ten behoeve van bewustwording en preventie. Het NCSC is daarmee het centrale meld- en informatiepunt voor ICT-dreigingen en -veiligheidsincidenten.

Deze Beveiligingsrichtlijnen voor mobiele apparaten zijn in 2012 gepubliceerd door het NCSC. Een aantal partijen heeft direct of indirect bijgedragen aan deze Beveiligingsrichtlijnen, waaronder het Nationaal Bureau voor Verbindingsbeveiliging (AIVD/NBV).

INHOUD

HOOFDSTUK 1

Inleiding

1.1 Aanleiding voor de Richtlijnen

Digitale informatie-uitwisseling is essentieel voor het functioneren van de Nederlandse samenleving. Hierbij spelen technologische innovatie, sociale media en de beschikbaarheid van goedkope mobiele apparaten een steeds belangrijkere rol. Betrouwbare digitale communicatie is van wezenlijk belang en vraagt om voortdurende zorg om de beschikbaarheid, integriteit en vertrouwelijkheid, van informatie te garanderen.

De Richtlijnen voor mobiele apparaten (hierna de Richtlijnen genoemd) bestaan uit twee documenten die, na implementatie, bijdragen aan een betere beveiliging van mobiele apparaten van gebruikers bij organisaties en de (Rijks)overheid. Deel 1 (dit document) beschrijft de Richtlijnen voor mobiele apparaten op hoofdlijnen.

1.2 Bring Your Own Device (BYOD)

Bring Your Own Device (BYOD) is een beleid waarin medewerkers, zakelijke partners en andere gebruikers in staat worden gesteld om persoonlijk geselecteerde en gekochte client (computer) apparatuur - zoals smartphones, tablets en laptops - op de werkplek te gebruiken en met het bedrijfsnetwerk te verbinden.

1.3 Consumerization of IT (CoIT)

Consumerization of IT (CoIT) is breder dan BYOD en beschrijft de cyclus van de informatietechnologie (IT) die eerst in de consumentenmarkt wordt gebruikt en later binnen bedrijven en (Rijks)overheidsorganisaties.
CoIT verwijst dan ook niet alleen naar het gebruik van persoonlijk geselecteerde en gekochte client (computer) apparatuur op het werk, maar ook naar onlinediensten, zoals online dataopslag, webgebaseerde e-maildiensten en sociale media of sociale netwerksites.

De aggregatie van onlinediensten die een gebruiker vanaf elke plek, op elk moment met behulp van elk (mobiel) apparaat kan benaderen wordt vaak aangeduid als persoonlijke cloud. Elke persoonlijke cloud kan verschillend zijn, in die zin dat een persoonlijke cloud is samengesteld uit verschillende diensten, maar elke dienst is gecentraliseerd in de cloud, of het nu een uniforme internetbankierapplicatie is of een aanpasbare nieuwsfeed.

1.4 Context/scope

De Richtlijnen richten zich op de beveiliging van mobiele apparaten vanuit het oogpunt van de eindgebruiker. De vraag staat hierbij centraal welke maatregelen de gebruiker van het mobiele apparaat kan instellen via de gebruikersinterface.

De Richtlijnen richten zich niet op de infrastructuur die organisaties en (Rijks)overheid dienen in te richten voor het beheer van mobiele apparaten die toegang hebben tot bedrijfsnetwerken en van welke mobiele (bedrijfs)applicaties deze mobiele apparaten gebruik mogen maken.
Denk hierbij aan:

- Mobile Device Management (MDM): het geautomatiseerd uitrollen en centraal monitoren en beheren van mobiele apparaten;
- Mobile Application Management (MAM): het beheren en controleren van (mobiele) applicaties.

1.5 Doelgroep

Deze Richtlijnen zijn bedoeld voor eindgebruikers en diegenen die bij organisaties en de (Rijks)overheid betrokken zijn bij de beveiliging van mobiele apparaten.

1.6 Doelstelling

De Richtlijnen geven een overzicht van beveiligingsmaatregelen die gebruikers en beheerders van mobiele apparaten moeten nemen om een bepaalde mate van veiligheid te bereiken. De maatregelen hebben niet alleen betrekking op het mobiele apparaat, maar ook op het gebruik en de configuratie van het mobiele besturingssysteem, zoals iOS en Android, en de applicaties (apps) die op het mobiele apparaat zijn geïnstalleerd.

1.7 Toepassing van de Richtlijnen

De Richtlijnen kunnen voor een bepaald toepassingsgebied worden omgezet in een normenkader. In tegenstelling tot de Richtlijnen, die adviserend van aard zijn, is een normenkader dwingend voor het toepassingsgebied. Afhankelijk van de aard en de specifieke kenmerken van het toepassingsgebied kunnen maatregelen worden weggelaten en/of worden opgenomen en kunnen wegingsfactoren van de individuele maatregelen worden aangepast.

1.8 De mate van wenselijkheid

De wenselijkheid van elke beveiligingsmaatregel wordt in algemene zin gewaardeerd volgens classificatieniveau een (1) of twee (2). Deze twee classificatieniveaus vormen twee punten op een schaal van mogelijke waarden waarbij niveau een kan worden gezien als de sterkste mate van wenselijkheid (must have) en niveau twee als een redelijk mate van wenselijkheid maar een niet-noodzakelijke voorwaarde (should have/nice to have).

Voor de maatregelen die zijn geclassificeerd als niveau een kan worden gesteld dat het praktisch en verstandig is om deze te implementeren, ze de beveiliging duidelijk ten goede komen en de functionaliteit en gebruiksvriendelijkheid van het mobiele apparaat niet te veel negatief beïnvloeden. De beveiliging wordt bewerkstelligd door ongeautoriseerde toegang tot het mobiele apparaat te voorkomen en zodoende het mobiele apparaat en de privacygevoelige en vertrouwelijke gegevens die op het mobiele apparaat worden verwerkt te beschermen.

Voor de maatregelen op niveau twee kan worden gesteld dat deze zijn bedoeld voor omgevingen en/of toepassinggebieden waar een hoger beveiligingsniveau wordt geëist. Een andere reden is dat deze maatregelen in de ogen van (sommige) gebruikers de functionaliteit en gebruiksvriendelijkheid van het mobiele apparaat te veel negatief beïnvloeden.

Bij de uiteindelijke afweging van wenselijkheid gaat het niet zozeer om het 'waarom' dan wel om 'de mate waarin' moet worden beveiligd. Het sleutelwoord hierbij is risicoafweging: die kan inzicht geven in wat en in hoeverre beveiligd moet worden. Daarbij wordt gekeken naar de kans op optreden van een dreiging, het te verdedigen belang, de mogelijke impact hiervan op de bedrijfsvoering en gebruiksvriendelijkheid. De Richtlijnen bieden de maatregelen die genomen kunnen worden om de kans op het optreden van dreigingen terug te dringen en/of de impact in geval van optreden van een dreiging te beperken.

1.9 Uitgangspunten

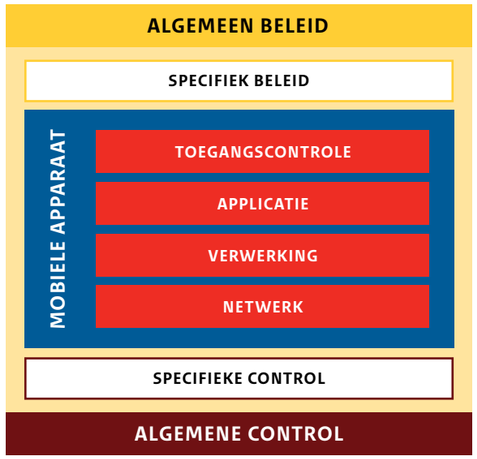
De uitgangspunten voor deze richtlijnen zijn:

- De Richtlijnen zijn generiek van opzet en voor een breed spectrum van mobiele apparaten toepasbaar. In deze versie worden implementatievoorschriften beschreven voor mobiele apparaten die iOS of Android gebruiken.
- De Richtlijnen richten zich op de drie aspecten van informatiebeveiliging: beschikbaarheid, integriteit en vertrouwelijkheid.
- De Richtlijnen hebben betrekking op mobiele apparaten en de omgeving waarin ze worden gebruikt. Dit omvat de hardware van het mobiele apparaat waarop het besturingssysteem en de verschillende apps draaien, het netwerk, de koppelingen tussen componenten en de software die noodzakelijk is om op een veilige manier van het mobiele apparaat en mobiele diensten gebruik te maken.
- De Richtlijnen kunnen als (toetsbare) norm worden gebruikt.

1.10 Opbouw van de documenten

De twee documenten die de Richtlijnen beschrijven zijn op dezelfde manier opgebouwd. De Richtlijnen in deel 1 beschrijven vooral maatregelen op hoofdlijnen die gebruikers en organisaties kunnen nemen om mobiele apparaten veiliger te gebruiken. Deel 2 beschrijft op detailniveau de (deel)maatregelen en hoe deze geïmplementeerd kunnen worden. Dit deel zal door het technische karakter meer aan verandering onderhevig zijn dan deel 1.

De Richtlijnen zijn te vinden in de hoofdstukken 3 tot en met 7 en worden in de onderstaande lagen *(zie fig. 1)*, elk mits van toepassing, in een apart hoofdstuk beschreven. Deze indeling is gebaseerd op het artikel 'Het construeren van referentiekaders: een principle-based aanpak' [1].



Figuur 1

Algemeen en specifiek beleid

Het algemeen beleid bevat randvoorwaarden, zoals hoofdbeleid, strategie, regelgeving en uitgangspunten voor business- en IT-architectuur. De volgende vraag dient hier beantwoord te worden: 'Welke organisatiebrede voorwaarden gelden voor het mobiele apparaat'.

Het specifiek beleid bevat aspecten die van toepassing zijn op mobiele apparaten. Deze specifieke conditionele aspecten zijn gerelateerd aan algemene beleidsaspecten. De volgende vraag dient hier beantwoord te worden: 'Welke specifieke voorwaarden gelden voor het mobiele apparaat'.

Het mobiele apparaat

Het mobiele apparaat bestaat uit de volgende vier lagen:

- Toegangscontrole: Is een gebruikersgeoriënteerd domein en bevat onder andere identiteits- en toegangsbeheer.
- Applicatie: Is een proces- en applicatiegeoriënteerd domein.
- Verwerking: Vertegenwoordigt de verwerkingslaag (databases en platform) en vervult de rol van mediator of integrator.
- Netwerk: Vertegenwoordigt de communicatielaag en bevat onder andere de netwerkinfrastructuur.

De volgende vraag dient hier beantwoord te worden: 'Hoe (waar/wanneer) moet het mobiele apparaat ingericht zijn'.

Specifieke en algemene control

Specifieke control: Vertegenwoordigt een domein dat specifieke control- en evaluatieaspecten ten aanzien van het auditobject bevat. Er wordt nagegaan in hoeverre er

bij de inrichting van het auditobject, zoals de processen en IT-objecten, controle-instrumenten zijn ingebouwd om de inrichting van de processen en IT-objecten te beheersen.

Algemene control: Binnen dit domein worden de noodzakelijke beheersprocessen voor het auditobject vastgesteld en wordt nagegaan hoe deze processen zijn vormgegeven om de inrichting van het betreffende auditobject continu in control te houden, zoals IT-servicesupport en managementprocessen.

De lagen vormen een middel om de Richtlijnen in clusters te beschrijven. Zoals op een aantal plekken zal blijken, zijn de lagen in de praktijk niet volledig van elkaar te scheiden en kunnen sommige Richtlijnen in meer dan één laag beschreven worden. Omwille van de overzichtelijkheid worden de eisen niettemin zoveel mogelijk in één laag beschreven. De beveiligingsmaatregelen worden alle volgens hetzelfde formaat beschreven:

- De nummering in de kolom 'Nr.' is de nummering van Richtlijnen zoals die gelden voor mobiele apparaten.
- De kolom 'Beschrijving van richtlijn' geeft een beschrijving van de richtlijn.

In deel 2 van de Richtlijnen wordt dit uitgebreid:

- De kolom 'Doelstelling' beschrijft de doelstelling die met de richtlijn beoogd wordt.
- De kolom 'Rationale'[1] geeft een toelichting op de richtlijn.
- De kolom 'Niveau'[2] beschrijft de initiële mate van wenselijkheid van de richtlijn. Deze kan in een specifieke situatie aangepast worden als gevolg van een risicoafweging.
- De kolom 'Configureren' geeft informatie hoe de richtlijn geconfigureerd (ingesteld) kan worden.
- De kolom 'Ingevuld door richtlijn' geeft aan door welke richtlijn deze algemene of specifieke beleidsrichtlijn wordt ingevuld. Vaak zijn dit de features/functies van het mobiele apparaat die via de gebruikersinterface kunnen worden geconfigureerd.
- De kolom iOS geeft aan of deze richtlijn (functie/feature/instelling) wordt ondersteund door mobiele apparaten met iOS.
- De kolom Android geeft aan of deze richtlijn (functie/feature/instelling) wordt ondersteund door mobiele apparaten met Android.

1. Definitie Rationale = idee achter een bepaalde handeling, standpuntbepaling, opstelling (Bron: 'Groot woordenboek van de Nederlandse Taal, 14de editie').
2. Met behulp van het classificatiesysteem worden de maatregelen gewaardeerd.

Een overzicht van alle gebruikte afkortingen staat in bijlage A. Voor de Richtlijnen is een aantal literatuurbronnen geraadpleegd. Op plaatsen waar informatie uit de literatuurbronnen verwerkt is, wordt hiernaar verwezen in de vorm van '[x]'. '[x]' verwijst naar een document opgenomen in bijlage B.
Bijlage C bevat een samenvatting van alle Richtlijnen en kan gebruikt worden als checklist voor de Richtlijnen.

Tot slot gebruiken de Richtlijnen ook voetnoten om bepaalde termen of begrippen te verduidelijken. Deze voetnoten herkent u aan een cijfer in superscript (bijvoorbeeld: [3]).

1.11 Onderhoud van de Richtlijnen

Het NCSC is verantwoordelijk voor het opstellen en onderhouden van de Richtlijnen. De Richtlijnen zullen jaarlijks worden geactualiseerd. Indien noodzakelijk zal het NCSC de Richtlijnen eerder aanpassen.

Aanvullingen, opmerkingen of eigen ervaringen ontvangen wij graag via: Richtlijnen@ncsc.nl.

1.12 Relatie met andere documenten

De Richtlijnen zijn afgeleid van verschillende standaarden, normen, raamwerken, best practices en benchmarks die door organisaties zijn opgesteld, zoals:

- Security Configuration Benchmark For Apple iOS 4.3.3 [2]
- Security Configuration Benchmark For Apple iOS 5.0.1 [3]
- iOS Hardening Configuration Guide - For iPod Touch, iPhone and iPad running iOS 5.1 or higher [4]
- Security Configuration Recommendations for Apple iOS 5 Devices [5]
- CIS Google Android 2.3 Benchmark [6]
- CIS Google Android 4 Benchmark [7]

NOOT:
Als dit document de naam van een product, dienst, fabrikant of leverancier noemt, betekent dit niet dat het NCSC deze op enige wijze goedkeurt, afkeurt, aanraadt, afraadt of op een andere manier hiermee verbonden is.

HOOFDSTUK 2

Veilig gebruik van mobiele apparaten

Dit hoofdstuk beschrijft hoe u zowel zakelijk als privé op een verstandige manier met de beveiligingsrisico's van mobiele apparaten kunt omgaan en mogelijke schade kan voorkomen of beperken.

De belangrijkste beveiligingsmogelijkheden van het mobiele apparaat zijn: authenticatie van de gebruiker, versleuteling van de opgeslagen gegevens, versleuteling van het netwerkverkeer en het op commando wissen van de opgeslagen gegevens (eventueel op afstand).

Apps op mobiele apparaten verwerken in meer of mindere mate privacygevoelige of vertrouwelijke informatie of wisselen deze uit. Het mobiele apparaat is de mobiele frontend voor centraal opgeslagen informatie. Denk hierbij aan uw contacten, e-mails, agenda-afspraken en documenten. Dit brengt beveiligingsrisico's met zich mee.

2.1 Uw mobiele apparaat kwijt of gestolen

Neem maatregelen zodat bij verlies of diefstal geen (privacygevoelige of vertrouwelijke) informatie op straat komt te liggen:

- Beveilig de toegang tot uw mobiele apparaat door middel van een toegangscode die door derden niet makkelijk te raden is (zie richtlijn B1-04 en B1-05). Selecteer altijd de methode die de sterkste beveiliging biedt en wijzig regelmatig uw toegangscode (zie richtlijn B1-02 en B0-03). De SIM-kaart heeft een eigen toegangscode (zie richtlijn B1-07). Wij adviseren om ook deze toegangscode regelmatig te wijzigen.
  Let op: Op het moment dat een kwaadwillende de verwijderbare media uit uw mobiele apparaat neemt, heeft hij toegang tot alle onversleutelde gegevens die hierop zijn opgeslagen. De toegangscode beveiligt alleen het mobiele apparaat en niet de verwijderbare media zoals de (micro-)SD-kaart. Het advies is dan ook om naast deze maatregel alle informatie op het mobiele apparaat te versleutelen (zie richtlijn B1-01).

- Stel uw mobiele apparaat zo in dat na een ingestelde tijdsperiode (bijvoorbeeld tussen de vijf en vijftien minuten) het mobiele apparaat automatisch wordt vergrendeld (zie richtlijn B1-08). Deze maatregel is effectief in combinatie met een toegangscode (zie richtlijn B1-04 en B1-05).

- Activeer de functionaliteit waarmee informatie op uw mobiele apparaat standaard versleuteld opgeslagen wordt (zie richtlijn B1-01).

- Stel uw mobiele apparaat zo in dat na een aantal mislukte inlogpogingen (bijvoorbeeld tien) het mobiele apparaat wordt gereset naar de standaard fabrieksinstellingen en uw informatie op het mobiele apparaat wordt gewist (zie richtlijn B1-06). Het advies is om naast deze maatregel regelmatig een reservekopie te maken van de gegevens op uw mobiele apparaat (zie richtlijn B0-06).

- Maak gebruik van volgsoftware die het beheren van uw mobiele apparaat op afstand ondersteunt, zodat u bij vermissing controle houdt over uw mobiele apparaat (zie richtlijn B1-13).
  Let op: Deze functionaliteit werkt niet op het moment dat het mobiele apparaat uitgeschakeld is, in vliegtuigmodus staat of de SIM-kaart is verwijderd of verwisseld.
  Beveiligingstoepassingen van derden[3] bieden de functionaliteit om een SMS te versturen als de SIM-kaart in uw mobiele apparaat wordt verwisseld door een andere SIM-kaart. Op deze manier kunt u uw mobiele apparaat toch lokaliseren en de erop opgeslagen gegevens wissen.

- Maak regelmatig een reservekopie/back-up van uw mobiele apparaat zodat u bij vermissing of een defect niet uw informatie kwijt bent. Voor het maken van een reservekopie/back-up hebt u een beheertoepassing nodig die is geïnstalleerd op uw computer (zie richtlijn B0-06). Zie ook paragraaf 2.6 'Wees voorzichtig bij onlineopslag'.

- Bewaar de International Mobile Equipment Identity (IMEI)-code[4] op een veilige plek en gescheiden van uw mobiele apparaat. De IMEI-code is een 15-cijferig nummer en is de unieke identificatie (serienummer) van uw mobiele apparaat. Deze IMEI-code heeft u nodig om bij verlies of diefstal aangifte te doen bij de politie.

- Doe altijd aangifte bij de politie als u merkt dat uw mobiele apparaat is verdwenen. Wanneer u uw mobiele apparaat gebruikt voor werk, meldt het dan ook bij de hiervoor aangewezen instantie binnen uw organisatie (bijvoorbeeld beveiliging of facilitaire zaken).

2.2 Lever uw mobiele apparaat 'schoon' in

Op het moment dat u uw mobiele apparaat verkoopt, weggeeft aan iemand anders of bij reparatie adviseren wij de fabrieksinstellingen te herstellen en alle informatie te wissen (zie richtlijn B2-07). Denk hierbij aan uw contactgegevens, sms'jes, e-mails of de door u geïnstalleerde apps en instellingen. Het wissen voorkomt dat de nieuwe eigenaar toegang heeft tot achtergebleven informatie op het mobiele apparaat.

3. http://www.av-comparatives.org/images/stories/test/mobile/mobile2011_english.pdf en http://mobile-security-software-review.toptenreviews.com/
4. U vindt het IMEI-nummer van uw mobiele telefoon door *#06# in te toetsen.

2.3 Voorkom een virusinfectie op uw mobiele apparaat

Kwaadwillenden maken misbruik van kwetsbaarheden op uw mobiele apparaat, bijvoorbeeld als u een 'onschuldig' lijkende app downloadt, die zonder dat u dat merkt geheime, kwaadaardige functies (een Trojaans paard) bevat. Als uw mobiele apparaat is geïnfecteerd met kwaadaardige software (malware), kunnen kwaadwillenden bijvoorbeeld:

- Zien wat u intypt om zo gebruikersnamen, wachtwoorden of andere (vertrouwelijke) informatie te achterhalen (zie kwetsbaarheid K1-5 'Spyware' in deel 2 van de Richtlijnen).
- Informatie verzamelen en verzenden naar een centrale server (zie kwetsbaarheid K1-5 'Spyware' in deel 2 van de Richtlijnen).
- SMS'jes versturen naar (dure) servicenummers of een abonnement afsluiten zonder dat u daarvan op de hoogte bent (zie kwetsbaarheid K1-7 'Diallerware' in deel 2 van de Richtlijnen).

Wij adviseren u om terughoudend te zijn met het installeren van onbekende apps op uw mobiele apparaat (zie richtlijn B2-01 en B2-02). Schaf nieuwe apps voor uw mobiele apparaat altijd aan via officiële distributiekanalen van leveranciers, de zogenaamde 'appstores' (zie richtlijn B2-08). Controleer vooraf de betrouwbaarheid van zowel de app als de makers. Bronnen die hierbij geraadpleegd kunnen worden zijn reviews van de app in de 'appstore', of de ICT-afdeling van uw organisatie. Installeer alleen apps op het moment dat het initiatief voor installatie van de app bij u ligt of deze wordt gedistribueerd via de ICT-afdeling van uw organisatie. Ga bewust om met beveiligingsinstellingen van de apps (zie richtlijn B2-03), controleer altijd of deze in lijn zijn met de Richtlijnen van uw organisatie. Geef alleen toestemming (rechten) aan apps op het moment dat u zeker bent van de impact en risico's (zie richtlijn B0-02). Voorzie uw mobiele apparaat, inclusief apps, altijd van de laatste beveiligingsupdates en softwareversies (zie richtlijn B2-05).

2.4 Laat uw mobiele apparaat niet afluisteren

Mobiele apparaten ondersteunen een breed scala aan typen draadloze netwerken, zoals Wi-Fi en Bluetooth. Deze draadloze netwerken zijn in meer of mindere mate kwetsbaar voor afluisteren, waardoor informatie kan worden onderschept. Daarnaast kan gevoelige informatie langs andere weg uitlekken. Door zwakheden in de beveiliging van gsm-communicatie kunnen bijvoorbeeld telefoongesprekken en sms-berichten worden afgeluisterd. Ook is gebleken dat voicemails door derden af te luisteren kunnen zijn.

Wij adviseren u om de volgende maatregelen in acht te nemen:

- Schakel Wi-Fi, Bluetooth en andere netwerktypen uit wanneer u daar geen gebruik van maakt (zie richtlijn B3-02 t/m B3-06, B3-11 en B3-12).
- Wees bewust en kritisch waar en wanneer u van een publiek (onversleuteld) Wi-Fi-netwerk gebruik maakt. Het is af te raden om op openbare plaatsen van een publiek Wi-Fi-netwerk gebruik te maken. Als u dat toch doet, onderneem dan geen activiteiten die met uw werk of financiën te maken hebben. Stel daarnaast uw mobiele apparaat zo in dat het niet automatisch verbinding maakt met een Wi-Fi-netwerk (zie richtlijn B3-07 t/m B3-09).
- Maak zoveel mogelijk gebruik van Virtual Private Network (VPN) verbindingen, zodat het dataverkeer wordt versleuteld over deze VPN-verbinding (zie richtlijn B3-10).

2.5 Geef geen informatie via uw mobiele apparaat vrij

Sommige apps voor mobiele apparaten verzamelen data van individuele gebruikers (bijvoorbeeld persoons- en locatiegegevens) en sturen deze op de achtergrond naar derden (bijvoorbeeld externe servers, ontwikkelaars of adverteerders), zonder de gebruiker te informeren. In veel gevallen gaat het om de volgende gegevens: toestel-id, telefoonnummers en contactpersonenlijst. Apps worden door gebruikers geïnstalleerd, vaak zonder dat ze weten wie de ontwikkelaar is en wat de exacte werking van de applicatie is. Hierbij geeft de gebruiker soms toestemming voor toegang tot informatie op zijn mobiele apparaat zonder te weten wat hiermee wordt gedaan (zie richtlijnen B0-01 t/m B0-03, B2-02 en B2-03).

Ook hebben steeds meer apps de mogelijkheid om locatiegegevens toe te voegen aan tweets, foto's of video's (geotagging). Uw 'volgers' kunnen zo precies zien waar u was op het moment van het maken van een foto of het plaatsen van een bericht. Dit is natuurlijk ook de doelstelling van de op locatie gebaseerde diensten (zie kwetsbaarheid K1-3 'Onbedoeld lekken van gegevens' in deel 2 van de Richtlijnen en richtlijn B2-06).

Om onbewust vrijgeven van informatie te voorkomen of dit zoveel mogelijk te beperken adviseren wij u het volgende:

- Lees het factsheet "Veilig op sociale netwerken"[5] aandachtig door. Hierin wordt een overzicht gegeven van de beveiliging- en privacyrisico's verbonden aan deelname aan sociale netwerken. Daarnaast wordt een drietal veel voorkomende aanvalsmethoden, evenals enkele maatregelen voor veilig(er) gebruik van sociale netwerken beschreven.

5. http://www.govcert.nl/dienstverlening/Kennis+en+publicaties/factsheets/factsheet-over-het-gebruik-van-sociale-netwerken-voorwerknemers.html

- Kijk kritisch naar de standaardinstellingen van uw mobiele apparaat ten aanzien van beveiliging, privacy en connectiviteit. Beperk het delen van of de toegang tot informatie (zoals locatiegegevens) wanneer het delen ervan niet nodig is (zie richtlijn B2-03 en B2-06).
- Lees voordat u een app installeert de voorwaarden en privacybeleid door van de aanbieder, zodat u op de hoogte bent hoe er met uw gegevens wordt omgegaan. Als er geen voorwaarden of privacybeleid bestaat, probeer dan op een andere manier deze informatie boven water te krijgen. Bronnen die hierbij geraadpleegd kunnen worden zijn reviews van de app of aanbieder in de 'appstore', onafhankelijke testrapporten van de app of de ICT-afdeling van uw organisatie (zie richtlijn B2-02 en B2-08).

2.6 Wees voorzichtig bij onlineopslag

Er zijn veel leveranciers die onlineopslag van foto's, documenten of back-ups aanbieden. Deze onlineopslag vindt meestal in de 'cloud'[6] plaats. De beveiliging van dergelijke diensten heeft u niet zelf in de hand en is niet altijd afdoende, wees dus voorzichtig bij onlineopslag vanaf uw mobiele apparaat. U moet altijd voorzichtig zijn met het online opslaan van uw vertrouwelijke gegevens. De onlinebestanden zijn direct toegankelijk voor iedereen die uw inloggegevens (vaak gebaseerd op e-mailadres en wachtwoord) weet te achterhalen (zie richtlijn B1-02).
Een ander aandachtspunt bij clouddiensten is het risico dat de dienst niet bereikbaar is. Dit kan komen doordat de clouddienst 'uit de lucht is' of omdat u geen internetverbinding tot u beschikking heeft.

Om op een veilige manier gebruik te maken van onlineopslag adviseren wij u het volgende:

- Maak bij het synchroniseren van u gegevens met de onlineopslag gebruik van een versleutelde verbinding (zie richtlijn B3-01 en B3-10). Informeer bij de dienstverlener van de onlineopslag of dit wordt ondersteund.
- Versleutel uw bestanden voordat deze online worden geplaatst (zie richtlijn B1-01).

2.7 Overige tips

- Informeer binnen uw organisatie of er beleid, Richtlijnen en/of standaarden zijn met betrekking tot het gebruik van mobiele apparaten (zie richtlijn B0-01).
- Wees u bewust dat u extra risico loopt als u uw mobiele apparaat 'jailbreakt', omdat uw mobiele apparaat dan niet meer wordt beschermd door de beveiligingsmaatregelen die de leverancier heeft ingebouwd (zie richtlijn B0-07).
- Maak gebruik van verschillende toegangscodes voor het mobiele apparaat, de verschillende diensten en apps (zie richtlijn B1-02).
- Wijzig regelmatig uw toegangscode (zie richtlijn B1-03).
- Schrijf uw inloggegevens niet op. Als u dat toch doet, bewaar uw inloggegevens dan op een veilige plek en gescheiden van uw mobiele apparaat.

6. https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/whitepaper-cloud-computing.html

HOOFDSTUK 3

Algemeen en specifiek beleid

In dit hoofdstuk worden generieke maatregelen beschreven die niet tot een specifieke categorie behoren, maar generiek zijn voor de beveiliging van mobiele apparaten.

Het algemeen beleid bevat randvoorwaarden, zoals hoofdbeleid, strategie, regelgeving en uitgangspunten voor business- en IT-architectuur. Welke organisatiebrede voorwaarden gelden voor het mobiele apparaat?

Het specifiek beleid bevat conditionele aspecten die van toepassing zijn op mobiele apparaten. Deze specifieke conditionele aspecten zijn gerelateerd aan algemene beleidsaspecten. Welke specifieke voorwaarden gelden voor het mobiele apparaat?

Nr.	Beschrijving van richtlijn	Niveau
B0-01	Er dienen maatregelen genomen te worden die gebruikers bewust en bekwaam maken	1
B0-02	Er dient inzichtelijk te zijn welke privacygevoelige en vertrouwelijke gegevens worden verwerkt	1
B0-03	Er dienen maatregelen genomen te worden die de privacygevoelige en vertrouwelijke gegevens afdoende beschermen	1
B0-04	Er dienen maatregelen genomen te worden die het aantal kwetsbaarheden tot een minimum beperken	1
B0-05	Er dient zoveel mogelijk gebruik gemaakt te worden van bestaande beveiligingsfuncties (features)	1
B0-06	• Maak regelmatig een back-up • Test regelmatig of de back-up ook teruggezet kan worden	1
B0-07	Jailbreak of root nooit het mobiele apparaat	1

HOOFDSTUK 4

Toegangscontrole

Dit hoofdstuk besteedt aandacht aan de maatregelen om identiteits en toegangsbeheer voor mobiele apparaten in te richten.

Nr.	Beschrijving van richtlijn	Niveau
B1-01	Versleutel opgeslagen gegevens waar mogelijk	1
B1-02	Maak gebruik van verschillende toegangscodes voor het mobiele apparaat, de verschillende diensten en apps	1
B1-03	Wijzig regelmatig de toegangscode van het mobiele apparaat, de verschillende diensten en apps	1
B1-04	Stel een toegangscode in om het mobiele apparaat te ontgrendelen	1
B1-05	Stel een toegangscode in om het mobiele apparaat te ontgrendelen die bestaat uit een combinatie van alfabetische, numerieke en niet-alfanumerieke tekens	2
B1-06	Stel het maximaal aantal toegestane mislukte aanmeldingspogingen in	1
B1-07	Schakel SIM-kaartvergrendeling in	1
B1-08	Stel automatische vergrendeling in waardoor het mobiele apparaat na een bepaalde periode wordt vergrendeld	1
B1-09	Sta apps niet toe om de gecodeerde opslag van certificaten, toegangscodes en andere credentials te benaderen.	2
B1-10	Schakel het tonen van de toegangscode tijdens het invoeren uit	2
B1-11	Schakel voorvertoning van berichten (voor Android alleen SMS-berichten) op het beginscherm uit	2
B1-12	Schakel de functies die ondersteuning bieden bij het ontwikkelen van apps - zoals USB-foutopsporing[7] - uit	1
B1-13	Maak gebruik van volgsoftware[8]	1

7. Deze optie machtigt foutopsporingsprogramma's op een computer om via een USB-verbinding met het mobiele apparaat te communiceren.
8. Voorbeelden van dergelijke applicaties zijn Find My iPhone (Zoek mijn iPhone) voor iOS <https://itunes.apple.com/nl/app/zoek-mijn-iphone/id376101648?mt=8> en Lookout, Prey of Samsung Dive voor Android <https://play.google.com/store/apps/details?id=com.alienmanfc6.wheresmyandroid&hl=nl>.

HOOFDSTUK 5

Applicatie

Dit hoofdstuk besteedt aandacht aan maatregelen om apps op het mobiele apparaat te beveiligen.

Nr.	Beschrijving van richtlijn	Niveau
B2-01	Het aantal geïnstalleerde apps dient te worden beperkt	1
B2-02	Installeer alleen apps op het moment dat bekend is wie deze app heeft gemaakt en de maker van deze app wordt vertrouwd	1
B2-03	Beperk de rechten van geïnstalleerde apps tot een absoluut minimum	1
B2-04	Configureer de browser zodanig dat het noodzakelijke beveiligingsniveau wordt gegarandeerd	1
B2-05	Voorzie tijdig alle software van de laatste versies/patches	1
B2-06	Locatievoorzieningen dienen zoveel mogelijk te zijn uitgeschakeld	1
B2-07	Het mobiele apparaat dient ‘schoon’ in te worden geleverd	1
B2-08	Installeer alleen apps als de bron bekend is	1
B2-09	Schakel JavaScript uit	2
B2-10	Schakel fraudemeldingen in	1
B2-11	Schakel automatisch vullen van webformulieren uit	2
B2-12	Schakel Privémodus (Incognitomodus) in	1
B2-13	Schakel cookies accepteren uit	1
B2-14	Schakel beveiligingswaarschuwingen weergeven in	1

HOOFDSTUK 6

Verwerking

Dit hoofdstuk is niet verder uitgewerkt omdat de infrastructuur die organisaties en (Rijks)overheid dienen in te richten voor het beheer van mobiele apparaten geen onderdeel uitmaakt van deze Richtlijnen (zie ook paragraaf 1.4).
Denk hierbij aan het geautomatiseerd uitrollen en centraal monitoren en beheren van mobiele apparaten die toegang hebben tot bedrijfsnetwerken (MDM) en het beheren en controleren van mobiele (bedrijfs)applicaties die de mobiele apparaten mogen gebruiken (MAM).

HOOFDSTUK 7

Netwerk

Dit hoofdstuk besteedt aandacht aan maatregelen om communicatie- en netwerkbeveiliging voor mobiele apparaten in te richten.

Nr.	Beschrijving van richtlijn	Niveau
B3-01	Versleutel verzonden gegevens waar mogelijk	1
B3-02	Schakel netwerkverbindingen zoveel mogelijk uit wanneer deze niet worden gebruikt	1
B3-03	Schakel de mobiele internetverbinding (mobiele data) uit als hier geen gebruik van wordt gemaakt[9]	2
B3-04	Schakel dataroaming[10] uit als hier geen gebruik van wordt gemaakt	1
B3-05	Schakel Persoonlijke hotspot[11] uit als hier geen gebruik van wordt gemaakt	1
B3-06	Schakel Wi-Fi uit als hier geen gebruik van wordt gemaakt[12]	2
B3-07	Stel het mobiele apparaat zo in dat Wi-Fi-netwerken, waar eerder verbinding mee is gemaakt, worden vergeten	1
B3-08	Stel het mobiele apparaat zo in dat er niet wordt gevraagd om een verbinding te maken met een Wi-Fi-netwerk	1
B3-09	Stel het mobiele apparaat zo in dat er niet automatisch met een Wi-Fi-netwerk wordt verbonden	1
B3-10	Maak zoveel mogelijk gebruik van een VPN-verbinding	1
B3-11	Schakel Bluetooth uit als hier geen gebruik van wordt gemaakt	1
B3-12	Schakel Near Field Communication (NFC) uit als hier geen gebruik van wordt gemaakt	1
B3-13	Schakel vliegtuigmodus in[13, 14, 15] als geen draadloze netwerkverbindingen en voorzieningen nodig zijn	2

9. Dit is een ongebruikelijke (ongewone) instelling voor een mobiel apparaat en beperkt de functionaliteit van het mobiele apparaat aanzienlijk.
10. Het automatisch overschakelen van het mobiele apparaat op het netwerk van een telecomaanbieder waar men geen contract mee heeft zodat een bepaalde dienst wordt voortgezet, met name met een mobiele telefoon in het buitenland van een buitenlandse provider.
11. Ook vaak aangeduid met tetheren en betekent dat de mobiele internetverbinding van het mobiele apparaat wordt gedeeld met een laptop of tablet.
12. Dit is een ongebruikelijke (ongewone) instelling voor een mobiel apparaat en beperkt de functionaliteit van het mobiele apparaat aanzienlijk.
13. In de vliegtuigmodus worden de draadloze verbindingen en voorzieningen van het mobiele apparaat uitgeschakeld om aan de voorschriften van luchtvaartmaatschappijen te voldoen. Denk hierbij aan de volgende draadloze functies: mobiele telefonie (spraak en gegevens), Wi-Fi, Bluetooth, GPS en locatievoorzieningen.
14. Dit is een ongebruikelijke (ongewone) instelling voor een mobiel apparaat en beperkt de functionaliteit van het mobiele apparaat aanzienlijk.
15. In vliegtuigmodus kunnen Wi-Fi en Bluetooth opnieuw worden ingeschakeld http://support.apple.com/kb/ht1355?viewlocale=nl_NL

BIJLAGE A » AFKORTINGEN

BYOD	Bring Your Own Device
CoIT	Consumerization of IT
GSM	Global System for Mobile Communications, officieel Groupe Spécial Mobile
ICT	Informatie- en communicatietechnologie
IMEI	International Mobile Equipment Identity
IT	Informatietechnologie
MAM	Mobile Application Management
MDM	Mobile Device Management
NCSC	Nationaal Cyber Security Centrum
NFC	Near field communication
SIM	Subscriber Identity Module
SMS	Short Message Service
USB	Universele Seriële Bus
VPN	Virtual Private Network
Wi-Fi	Wireless Fidelity

BIJLAGE B » LITERATUURLIJST

[1] De Richtlijnen worden beschreven volgens de lagen uit het artikel 'Het construeren van referentiekaders: een principle-based aanpak' van dr. Wiekram B.Tewarie RE, Prof.dr.ir. Ronald Paans RE en dr. Joris Hulstijn, uit de IT-Auditor, nummer 2 van jaargang 2011. http://www.norea.nl/readfile.aspx?ContentID=68278&ObjectID=940136&Type=1&File=0000036004_Referentiekaders.pdf

[2] 'Security Configuration Benchmark For Apple iOS 4.3.3', d.d. juni 2011. https://benchmarks.cisecurity.org/en-us/?route=downloads.show.single.iphone.130

[3] 'Security Configuration Benchmark For Apple iOS 5.0.1', d.d. december 2011. http://benchmarks.cisecurity.org/en-us/?route=downloads.show.single.iphone.140

[4] 'iOS Hardening Configuration Guide - For iPod Touch, iPhone and iPad running iOS 5.1 or higher', d.d. maart 2012. http://www.dsd.gov.au/publications/iOS5_Hardening_Guide.pdf

[5] 'Security Configuration Recommendations for Apple iOS 5 Devices', d.d. maart 2012. http://www.nsa.gov/ia/_files/os/applemac/Apple_iOS_5_Guide.pdf

[6] 'CIS Google Android 2.3 Benchmark', d.d. juli 2012. http://benchmarks.cisecurity.org/en-us/?route=downloads.show.single.android.110

[7] 'CIS Google Android 4 Benchmark', d.d. oktober 2012. http://benchmarks.cisecurity.org/en-us/?route=downloads.show.single.android4.100

BIJLAGE C » SAMENVATTING RICHTLIJNEN

Algemeen en specifiek beleid		
Nr.	**Beschrijving van richtlijn**	**Niveau**
B0-01	Er dienen maatregelen genomen te worden die gebruikers bewust en bekwaam maken	1
B0-02	Er dient inzichtelijk te zijn welke privacygevoelige en vertrouwelijke gegevens worden verwerkt	1
B0-03	Er dienen maatregelen genomen te worden die de privacygevoelige en vertrouwelijke gegevens afdoende beschermen	1
B0-04	Er dienen maatregelen genomen te worden die het aantal kwetsbaarheden tot een minimum beperken	1
B0-05	Er dient zoveel mogelijk gebruik gemaakt te worden van bestaande beveiligingsfuncties (features)	1
B0-06	• Maak regelmatig een back-up • Test regelmatig of de back-up ook teruggezet kan worden	1
B0-07	Jailbreak of root nooit het mobiele apparaat	1

Toegangscontrole		
Nr.	**Beschrijving van richtlijn**	**Niveau**
B1-01	Versleutel opgeslagen gegevens waar mogelijk	1
B1-02	Maak gebruik van verschillende toegangscodes voor het mobiele apparaat, de verschillende diensten en apps	1
B1-03	Wijzig regelmatig de toegangscode van het mobiele apparaat, de verschillende diensten en apps	1
B1-04	Stel een toegangscode in om het mobiele apparaat te ontgrendelen	1
B1-05	Stel een toegangscode in om het mobiele apparaat te ontgrendelen die bestaat uit een combinatie van alfabetische, numerieke en niet-alfanumerieke tekens	2
B1-06	Stel het maximaal aantal toegestane mislukte aanmeldingspogingen in	1
B1-07	Schakel SIM-kaartvergrendeling in	1
B1-08	Stel automatische vergrendeling in waardoor het mobiele apparaat na een bepaalde periode wordt vergrendeld	1
B1-09	Sta apps niet toe om de gecodeerde opslag van certificaten, toegangscodes en andere credentials te benaderen	2
B1-10	Schakel het tonen van de toegangscode tijdens het invoeren uit	2
B1-11	Schakel voorvertoning van berichten (voor Android alleen SMS-berichten) op het begin-scherm uit	2
B1-12	Schakel de functies die ondersteuning bieden bij het ontwikkelen van apps - zoals USB-foutopsporing - uit	1
B1-13	Maak gebruik van volgsoftware	1

Applicatie		
Nr.	**Beschrijving van richtlijn**	**Niveau**
B2-01	Het aantal geïnstalleerde apps dient te worden beperkt	1
B2-02	Installeer alleen apps op het moment dat bekend is wie deze app heeft gemaakt en de maker van deze app wordt vertrouwd	1
B2-03	Beperk de rechten van geïnstalleerde apps tot een absoluut minimum	1
B2-04	Configureer de browser zodanig dat het noodzakelijke beveiligingsniveau wordt gegarandeerd	1
B2-05	Voorzie tijdig alle software van de laatste versies/patches	1
B2-06	Locatievoorzieningen dienen zoveel mogelijk te zijn uitgeschakeld	1
B2-07	Het mobiele apparaat dient ‘schoon’ in te worden geleverd	1
B2-08	Installeer alleen apps als de bron bekend is	1
B2-09	Schakel JavaScript uit	2
B2-10	Schakel fraudemeldingen in	1
B2-11	Schakel automatisch vullen van webformulieren uit	2
B2-12	Schakel Privémodus (Incognitomodus) in	1
B2-13	Schakel cookies accepteren uit	1
B2-14	Schakel beveiligingswaarschuwingen weergeven in	1

Netwerk		
Nr.	**Beschrijving van richtlijn**	**Niveau**
B3-01	Versleutel verzonden gegevens waar mogelijk	1
B3-02	Schakel netwerkverbindingen zoveel mogelijk uit wanneer deze niet worden gebruikt	1
B3-03	Schakel de mobiele internetverbinding (mobiele data) uit als hier geen gebruik van wordt gemaakt	2
B3-04	Schakel dataroaming uit als hier geen gebruik van wordt gemaakt	1
B3-05	Schakel Persoonlijke hotspot uit als hier geen gebruik van wordt gemaakt	1
B3-06	Schakel Wi-Fi uit als hier geen gebruik van wordt gemaakt	2
B3-07	Stel het mobiele apparaat zo in dat Wi-Fi-netwerken waar eerder verbinding mee is gemaakt worden vergeten	1
B3-08	Stel het mobiele apparaat zo in dat er niet wordt gevraagd om een verbinding te maken met een Wi-Fi-netwerk	1
B3-09	Stel het mobiele apparaat zo in dat er niet automatisch met een Wi-Fi-netwerk wordt verbonden	1
B3-10	Maak zoveel mogelijk gebruik van een VPN-verbinding	1
B3-11	Schakel Bluetooth uit als hier geen gebruik van wordt gemaakt	1
B3-12	Schakel Near Field Communication (NFC) uit als hier geen gebruik van wordt gemaakt	1
B3-13	Schakel vliegtuigmodus in als geen draadloze netwerkverbindingen en voorzieningen nodig zijn	2

Colofon

Uitgave
Nationaal Cyber Security Centrum, Den Haag | November 2012

Wilhelmina van Pruisenweg 104 | 2595 AN Den Haag
Postbus 117 | 2501 CC Den Haag

T 070-888 75 55
F 070-888 75 50

E info@ncsc.nl
I www.ncsc.nl

Nationaal Cyber Security Centrum

Het Nationaal Cyber Security Centrum (NCSC) draagt via samenwerking tussen bedrijfsleven, overheid en wetenschap bij aan het vergroten van de weerbaarheid van de Nederlandse samenleving in het digitale domein.

Het NCSC ondersteunt de Rijksoverheid en organisaties met een vitale functie in de samenleving met expertise en advies, respons op dreigingen en het versterken van de crisisbeheersing. Daarnaast voorziet het in informatie en advies voor burger, overheid en bedrijfsleven ten behoeve van bewustwording en preventie. Het NCSC is daarmee het centrale meld- en informatiepunt voor ICT-dreigingen en -veiligheidsincidenten.

Nationaal Cyber Security Centrum
Wilhelmina van Pruisenweg 104 | 2595 AN Den Haag
Postbus 117 | 2501 CC Den Haag

T 070-888 75 55
F 070-888 75 50

E info@ncsc.nl
I www.ncsc.nl

November 2012