Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

» Beveiligingsrichtlijnen voor mobiele apparaten »

Deel 2

»Beveiligingsrichtlijnen voor mobiele apparaten»

Deel 2

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 beschrijft de Richtlijnen voor mobiele apparaten op hoofdlijnen. Dit document vormt een ondersteunend document en beschrijft de maatregelen op detailniveau. Met deze maatregelen kan worden voldaan aan de richtlijnen uit deel 1.

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

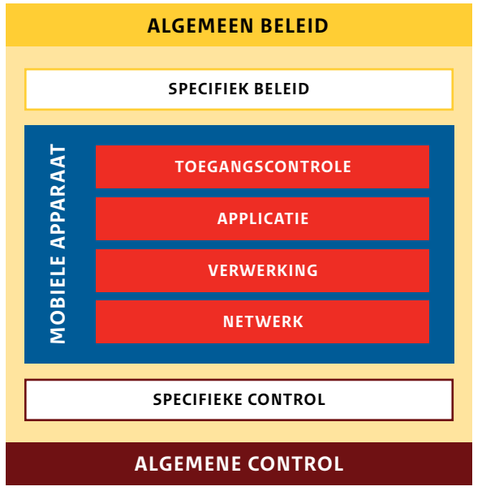
De uitgangspunten voor deze richtlijnen zijn:

- 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.

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.

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.

HOOFDSTUK 2

Mobiele risico's

Nr.	Beveiligingslaag	Risico
K1-1	• Applicatie • Verwerking • Netwerk	Lekken van gegevens

Toelichting

Om een adequate beveiliging van de gegevens op het mobiele apparaat te garanderen is men voor een groot deel afhankelijk van de betrouwbaarheid van de apps die de gegevens opslaan en/of verwerken.
De beveiliging die standaard wordt geboden door het mobiele apparaat is toereikend voor de meeste gegevens. Als strengere eisen worden gestelt aan de, vaak zakelijke, gegevens moet extra beveiliging worden ingebouwd in de app die deze gegevens verwerkt.

Zonder twijfel is het grootste risico een verloren of gestolen mobiel apparaat. Een gestolen of verloren mobiel apparaat met onbeveiligde gegevens in het geheugen of op verwisselbare opslagmedia geeft een aanvaller de mogelijkheid om toegang te krijgen tot de gegevens die erop zijn opgeslagen.

Het mobiele apparaat wordt verkocht of overgedragen aan een andere gebruiker of ter reparatie aangeboden zonder dat gegevens worden verwijderd, of het mobiele apparaat wordt op een onjuiste manier buiten gebruik gesteld. Hierdoor kan een aanvaller toegang krijgen tot de gegevens die erop zijn opgeslagen.

Kwetsbaarheden

- Kwetsbaarheden in het mobiele besturingssysteem of de geïnstalleerde apps
- Zwakheden in de toegepaste encryptiemethode voor gegevensopslag
- Onveilige gegevensopslag
- Verlies of diefstal van het mobiele apparaat
- Op onjuiste manier buiten gebruik stellen van het mobiele apparaat
- Gebrek aan bewustwording bij gebruikers
- Gebrek aan vaardigheid bij gebruikers

Nr.	Beveiligingslaag	Risico
K1-2	Netwerk	Afluisteren of modificeren van netwerkverkeer

Toelichting

Om een adequate beveiliging van de gegevens tijdens transport te garanderen is men voor een groot deel afhankelijk van de beveiliging die door netwerkverbindingen wordt geboden. Bij niet afdoende beveiliging kunnen gegevens tijdens transport worden onderschept of gewijzigd.

Een aanvaller zet bijvoorbeeld een kwaadaardig draadloos accesspoint op (Wi-Fi of GSM) waar gebruikers verbinding mee maken. De aanvaller onderschept of wijzigt vervolgens de communicatie van de gebruikers om verdere aanvallen uit te voeren, zoals bijvoorbeeld phishing.

Opmerking: Ga uit van het feit dat apps zullen worden gebruikt op het meest open Wi-Fi-netwerk dat je maar kunt bedenken. Maak dus gebruik van apps die SSL- of TLS-versleuteling gebruiken bij het verzenden of ontvangen van alle gegevens die moeten worden beveiligd. Een andere eis is dat de app de hostname op de SSL-certificaten controleert en alleen gevalideerde SSL-certificaten en geen nagemaakte of zelfondertekende certificaten accepteert.

Kwetsbaarheden

- Zwakheden in de toegepaste encryptiemethode bij netwerkverbinding
- Onveilige of onvoldoende beveiligde netwerkverbinding
- Gebrek aan bewustwording bij gebruikers
- Gebrek aan vaardigheid bij gebruikers

Nr.	Beveiligingslaag	Risico
K1-3	Applicatie	Onbedoeld lekken van gegevens

Toelichting

Gebruikers onthullen onbedoeld gegevens die op het mobiele apparaat zijn opgeslagen. Veel gebruikers zijn zich niet bewust dat apps op het mobiele apparaat gegevens kunnen lekken en dat deze worden verzonden naar derden. De meeste apps beschikken over privacyinstellingen maar gebruikers zijn zich vaak niet bewust dat apps over deze instellingen beschikken om het delen van gegevens te voorkomen.
Bij dit risico worden gegevens vrijgegeven door onbewust of onbekwaam handelen van de gebruiker (bijvoorbeeld onnodige rechten geven aan apps, locatiegegevens koppelen aan foto's en deze in de cloud plaatsen).

Kwetsbaarheden

- Moeilijk (lastig) voor gebruiker om inzicht te krijgen in de vereiste (en toegekende) gebruikersrechten
- Er zijn geen privacy 'best practices' beschikbaar
- Gebrek aan bewustwording bij gebruikers
- Gebrek aan vaardigheid bij gebruikers
- Covert channels[3] (verscholen kanaal)
- Zwakke implementatie van sandboxing[4]

Nr.	Beveiligingslaag	Risico
K1-4	Algemeen beleid	Phishing[5]

Toelichting

Een aanvaller verzamelt gebruikersgegevens (zoals wachtwoorden en creditcardnummers) met behulp van malafide apps of berichten (zoals SMS, e-mail) die betrouwbaar lijken.

Kwetsbaarheden

- Zwakke authenticatiemechanismen bij appdistributie
- Gebrek aan bewustwording bij gebruikers
- Gebrek aan vaardigheid bij gebruikers

3. http://en.wikipedia.org/wiki/Covert_channel
4. http://nl.wikipedia.org/wiki/Sandbox_%28software%29
5. http://www.waarschuwingsdienst.nl/Risicos/Misbruik+van+je+gegevens/Wat+is+phishing.html

Nr.	Beveiligingslaag	Risico
K1-5	Verwerking	Spyware[6]

Toelichting

Op het mobiele apparaat is spyware geïnstalleerd waardoor een aanvaller toegang heeft tot persoonsgegevens of deze kan afleiden. Als spyware wordt een kwaadaardige app bedoeld die allerlei gegevens verzameld die op het mobiele apparaat worden verwerkt.

De hoeveelheid persoonsgegevens, gevoelige documenten en toegangsrechten die is opgeslagen en wordt verwerkt door mobiele apparaten maakt deze een interessant doelwit voor spyware. Mobiele apparaten hebben covert channels (verscholen kanalen) die door een app kunnen worden gebruikt om onbedoeld gegevens te verstrekken aan een aanvaller.

Kwetsbaarheden

- Zwakke authenticatiemechanismen bij appdistributie
- Kwetsbaarheden waardoor malware geïnstalleerd kan worden
- Kwetsbaarheden in reputatiesystemen
- Covert channels (verscholen kanaal)
- Zwakke implementatie van sandboxing
- Moeilijk voor gebruiker om inzicht te krijgen in de vereiste (en toegekende) gebruikersrechten
- Gebrek aan bewustwording bij gebruikers
- Gebrek aan vaardigheid bij gebruikers

Nr.	Beveiligingslaag	Risico
K1-6	Verwerking	Surveillance (bewaken, toezicht)

Toelichting

Een aanvaller bespioneert (controleert) een specifieke gebruiker via het mobiele apparaat van deze gebruiker.

Mobiele apparaten bevatten meerdere sensoren zoals een microfoon, camera, versnellingsmeter en GPS. Dit, gecombineerd met de mogelijkheid om software van derden te installeren en het feit dat een mobiel apparaat nauw verbonden is met een individu, maakt het een nuttig spionagehulpmiddel.

Kwetsbaarheden

- Zwakke authenticatiemechanismen bij appdistributie
- Kwetsbaarheden waardoor malware kan worden geïnstalleerd
- Covert channels (verscholen kanaal)
- Zwakke implementatie van sandboxing
- Moeilijk (lastig) voor gebruiker om inzicht te krijgen in de vereiste (en toegekende) gebruikersrechten
- Gebrek aan bewustwording bij gebruikers
- Gebrek aan vaardigheid bij gebruikers

6. http://www.waarschuwingsdienst.nl/Risicos/Inbreuk+op+je+privacy/Spyware+spion.html

Nr.	Beveiligingslaag	Risico
K1-7	Verwerking	Diallerware

Toelichting

Een aanvaller steelt geld van de gebruiker door middel van malware die op de achtergrond gebruikmaakt van betaalde SMS-diensten of telefoonnummers.

Een aanvaller kan geld stelen via het mobiele apparaat van een slachtoffer als hij in staat is om een app te installeren op het apparaat en deze app het recht heeft om gebruik te maken van betaalde diensten.

Kwetsbaarheden

- Zwakke authenticatiemechanismen bij appdistributie
- Kwetsbaarheden waardoor malware kan worden geïnstalleerd
- Covert channels (verscholen kanaal)
- Zwakke implementatie van sandboxing
- Moeilijk (lastig) voor gebruiker om inzicht te krijgen in de vereiste (en toegekende) gebruikersrechten
- Gebrek aan bewustwording bij gebruikers
- Gebrek aan vaardigheid bij gebruikers

Nr.	Beveiligingslaag	Risico
K1-8	Verwerking	Financiële malware

Toelichting

Het mobiele apparaat is geïnfecteerd met malware die speciaal is ontworpen voor het stelen van creditcard-nummers, online bankgegevens, et cetera.

Financiële malware heeft veel verschijningsvormen: het kan een keylogger zijn die creditcardnummers verzamelt, of een app die SMS-authenticatiecodes onderschept om internetbankierapps aan te vallen. Een andere manier is om een malafide app te plaatsen in de appstore, die zich voordoet als een echte internetbankierapp. Als gebruikers deze app downloaden en gebruiken, kan de aanvaller een man-in-the-middleaanval opzetten om banktransacties uit te voeren.

Kwetsbaarheden

- Zwakke authenticatiemechanismen voor appdistributie
- Kwetsbaarheden waardoor malware kan worden geïnstalleerd
- Covert channels (verscholen kanaal)
- Zwakke implementatie van sandboxing
- Moeilijk voor gebruiker om inzicht te krijgen in de vereiste (en toegekende) gebruikersrechten
- Gebrek aan bewustwording bij gebruikers
- Gebrek aan vaardigheid bij gebruikers

HOOFDSTUK 2 » MOBIELE RISICO'S

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.

Nr.	Beveiligingslaag	Beschrijving van richtlijn
B0-01	Algemeen beleid	Er dienen maatregelen genomen te worden die gebruikers bewust en bekwaam maken

Doelstelling

Waarborgen dat gebruikers zich bewust zijn van de bedreigingen en risico's die het gebruik van mobiele apparaten met zich meebrengt en dat gebruikers worden getraind in het omgaan met de beveiligingsprocedures en het correcte gebruik van mobiele apparaten, om eventuele beveiligingsrisico's te minimaliseren.

Rationale

Gebruikers van mobiele apparaten binnen de organisatie en - indien van toepassing - externe gebruikers, dienen een passende training en regelmatige nascholing te krijgen betreffende het beleid en de procedures van de organisatie met betrekking tot het gebruik van mobiele apparaten. Hieronder vallen de beveiligings-eisen, wettelijke verplichtingen en bedrijfsmaatregelen, alsmede de training in het correct gebruik van de mobiele apparaten, bijvoorbeeld inlogprocedures, het gebruik van apps, et cetera, voordat zij toegang krijgen tot deze voorzieningen.

Niveau 1

Ingevuld door richtlijn (functie / feature van het mobiele apparaat)

Niet van toepassing, maar is de verantwoordelijkheid van de gebruiker

iOS	Android
Ja	Ja

Nr.	Beveiligingslaag	Beschrijving van richtlijn
B0-02	Algemeen beleid	Er dient inzichtelijk te zijn welke privacygevoelige en vertrouwelijke gegevens worden verwerkt

Doelstelling

Het kunnen maken van een bewuste en weloverwogen afweging tussen de gebruiksvriendelijkheid en de beveiliging van de gegevens die worden verwerkt.

Rationale

Denk hierbij aan contactgegevens, e-mails, persoonlijke gegevens zoals foto's en video's, et cetera.

Denk na, voor ingebruikname, welke privacygevoelige en vertrouwelijke gegevens worden verwerkt.

Niveau 1

Ingevuld door richtlijn (functie / feature van het mobiele apparaat)

Niet van toepassing, maar is de verantwoordelijkheid van de gebruiker

iOS	Android
Ja	Ja

Nr.	Beveiligingslaag	Beschrijving van richtlijn
B0-03	Algemeen beleid	Er dienen maatregelen genomen te worden die de privacygevoelige en vertrouwelijke gegevens afdoende beschermen

Doelstelling

Het afdoende beschermen van de privacygevoelige en vertrouwelijke gegevens.

Rationale

Op basis van de inventarisatie van de privacygevoelige en vertrouwelijke gegevens uit richtlijn B0-02 kan de gebruiker een bewuste en weloverwogen beslissing nemen welke maatregelen geïmplementeerd dienen te worden om deze privacygevoelige en vertrouwelijke gegevens afdoende te beschermen.

Niveau 1

Ingevuld door richtlijn (functie / feature van het mobiele apparaat)

B1-01 Versleutel opgeslagen gegevens waar mogelijk.
B1-02 Maak gebruik van verschillende toegangscodes voor het mobiele apparaat, de verschillende diensten en apps.
B1-03 Wijzig regelmatig de toegangscode van het mobiele apparaat, de verschillende diensten en apps.
B1-04 Stel een toegangscode in om het mobiele apparaat te ontgrendelen.
B1-05 Stel een toegangscode in om het mobiele apparaat te ontgrendelen die bestaat uit een combinatie van alfabetische, numerieke en niet-alfanumerieke tekens.
B1-06 Stel het maximaal aantal toegestane mislukte aanmeldingspogingen in.
B1-07 Schakel SIM-kaartvergrendeling in
B1-08 Stel automatische vergrendeling in waardoor het mobiele apparaat na een bepaalde periode wordt vergrendeld.
B1-09 Sta apps niet toe om de gecodeerde opslag van certificaten, toegangscodes en andere credentials te benaderen.
B1-10 Schakel het tonen van de toegangscode tijdens het invoeren uit.
B1-11 chakel voorvertoning van berichten (voor Android alleen SMS-berichten) op het beginscherm uit.
B1-12 Schakel de functies die ondersteuning bieden bij het ontwikkelen van apps, zoals USB-fout-opsporing, uit.
B1-13 Maak gebruik van volgsoftware.
B2-03 Beperk de rechten van geïnstalleerde apps tot een absoluut minimum.
B2-04 Configureer de browser zodanig dat het noodzakelijke beveiligingsniveau wordt gegarandeerd.
Deze richtlijn wordt ingevuld door:
B2-09 - Schakel JavaScript uit.
B2-10 - Schakel fraudemeldingen in.
B2-11 - Schakel automatisch vullen van webformulieren uit.
B2-12 - Schakel Privémodus (Incognitomodus) in.
B2-13 - Schakel cookies accepteren uit.
B2-14 - Schakel beveiligingswaarschuwingen weergeven in.
B2-06 Locatievoorzieningen dienen zoveel mogelijk te zijn uitgeschakeld.
B2-07 Het mobiele apparaat dient ‘schoon’ in te worden geleverd.
B3-01 Versleutel verzonden gegevens waar mogelijk.

B0-03 Vervolg invulling door richtlijn (functie / feature van het mobiele apparaat)

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

iOS	Android
Ja	Ja

Nr.	Beveiligingslaag	Beschrijving van richtlijn
B0-04	Algemeen beleid	Er dienen maatregelen genomen te worden die het aantal kwetsbaarheden tot een minimum beperken

Doelstelling

- Het mobiele apparaat en de privacygevoelige en vertrouwelijke gegevens die op het mobiele apparaat worden verwerkt afdoende te beschermen en mogelijk misbruik door het vrijgeven van deze gegevens tot een minimum te beperken.
- Het aantal kwetsbaarheden op het mobiele apparaat tot een minimum te beperken en mogelijke uitbuiting van kwetsbaarheden voor te zijn.

Rationale

Het is een utopie om te geloven dat mobiele besturingssystemen en apps geen kwetsbaarheden bevatten. Het streven moet wel zijn om het aantal kwetsbaarheden te beperken door bewust om te gaan welke apps worden geïnstalleerd. Als er kwetsbaarheden in software worden gevonden die op het mobiele apparaat draaien is het raadzaam om het beveiligingsadvies van de leverancier of een onafhankelijke partij zoals het NCSC zo snel mogelijk te installeren. Dit zorgt ervoor dat het misbruik van de kwetsbaarheid tot een minimum wordt beperkt.

Niveau 1

Ingevuld door richtlijn (functie / feature van het mobiele apparaat)

B1-12 Schakel de functies die ondersteuning bieden bij het ontwikkelen van apps, zoals USB-fout-opsporing, uit.
B2-01 Het aantal geïnstalleerde apps dient te worden beperkt.
B2-02 Installeer alleen apps op het moment dat bekend is wie deze app heeft gemaakt en de maker van deze app wordt vertrouwd.
Deze richtlijn wordt ingevuld door:
B2-08 - Installeer alleen apps als de bron bekend is.
B2-03 Beperk de rechten van geïnstalleerde apps tot een absoluut minimum.
B2-04 Configureer de browser zodanig dat het noodzakelijke beveiligingsniveau wordt gegarandeerd.
Deze richtlijn wordt ingevuld door:
B2-09 - Schakel JavaScript uit.
B2-10 - Schakel fraudemeldingen in.
B2-14 - Schakel beveiligingswaarschuwingen weergeven in.
B2-05 Voorzie tijdig alle software van de laatste versies/patches.
B3-02 Schakel netwerkverbindingen zoveel mogelijk uit wanneer deze niet worden gebruikt.
Deze richtlijn wordt ingevuld door:
B3-03 - Schakel de mobiele internetverbinding (mobiele data) uit als hier geen gebruik van wordt gemaakt.
B3-04 - Schakel dataroaming uit als hier geen gebruik van wordt gemaakt.
B3-05 - Schakel Persoonlijke hotspot uit als hier geen gebruik van wordt gemaakt.
B3-06 - Schakel Wi-Fi uit als hier geen gebruik van wordt gemaakt.
B3-11 - Schakel Bluetooth uit als hier geen gebruik van wordt gemaakt.
B3-12 - Schakel Near Field Communication (NFC) uit als hier geen gebruik van wordt gemaakt.
B3-13 - Schakel vliegtuigmodus in als geen draadloze netwerkverbindingen en voorzieningen nodig zijn.

iOS	Android
Ja	Ja

Nr.	Beveiligingslaag	Beschrijving van richtlijn
B0-05	Algemeen beleid	Er dient zoveel mogelijk gebruik gemaakt te worden van bestaande beveiligings-functies (features)

Doelstelling

Het mobiele apparaat, de privacygevoelige en vertrouwelijke gegevens die op het mobiele apparaat worden verwerkt afdoende te beschermen en mogelijk misbruik door het vrijgeven van deze gegevens tot een minimum te beperken.

Rationale

Beveiligingsfuncties moeten effectief worden ingezet zodat de weerstand (robuustheid) tegen aanvallen wordt vergroot. Denk voor het uitzetten van beveiligingsfuncties na over waarom deze betreffende beveiligingsfunctie uitgezet dient te worden en wat de consequenties hiervan zijn, zodat het een bewuste en weloverwogen beslissing is.

Niveau 1

iOS	Android
Ja	Ja

Nr.	Beveiligingslaag	Beschrijving van richtlijn
B0-06	Algemeen beleid	• Maak regelmatig een back-up van het mobiele apparaat • Test regelmatig of de back-up ook teruggezet kan worden

Doelstelling

Het waarborgen van de integriteit en beschikbaarheid van het mobiele apparaat en de informatieverwerkende apps inclusief bijbehorende gegevens.

Rationale

Er moeten regelmatig back-ups (reservekopieën) worden gemaakt van het mobiele apparaat, de informatieverwerkende apps inclusief bijbehorende gegevens. Hiervoor moeten voorzieningen beschikbaar zijn, zodat alle essentiële gegevens en systemen tijdig hersteld kunnen worden na een incident.

Het is aan te raden om back-ups te versleutelen. Valt een back-up onverhoopt in handen van een kwaadwillende, dan kan deze in dit geval geen toegang krijgen tot de informatie in de back-up.

Tot slot is het van belang om regelmatig te testen of de gemaakte back-ups de mogelijkheid bieden om een verloren, gestolen of defect geraakt mobiel apparaat opnieuw in te richten.

Android Android biedt de mogelijkheid om een back-up van de persoonlijke gegevens te maken in het gekoppelde Google-account op de servers van Google. Als het mobiele apparaat wordt vervangen, kunnen de gegevens worden hersteld als weer voor de eerste keer wordt aangemeld op het Google-account. Er worden veel verschillende persoonlijke gegevens in de back-up opgenomen, waaronder Wi-Fi-wachtwoorden, browserbladwijzers, een lijst met de apps die zijn geïnstalleerd, de woorden die u aan het woordenboek van het schermtoetsenbord heeft toegevoegd en de meeste instellingen die u via de toepassing Instellingen heeft geconfigureerd. Ook kunnen apps van derden gebruik maken van deze functionaliteit, de gegevens kunnen dan worden hersteld als een app opnieuw wordt geïnstalleerd.
Let op: Als deze optie wordt/is uitgeschakeld, wordt er geen back-up van de gegevens in het gekoppelde Google-account meer gemaakt en worden bestaande back-ups van de Google-servers verwijderd.

iOS **Een reservekopie maken met iTunes**
Met iTunes kunnen reservekopieën van de instellingen, gedownloade apps en bijbehorende gegevens en andere informatie op het mobiele apparaat worden gemaakt. iTunes maakt bij de volgende bewerkingen een reservekopie van het mobiele apparaat[7]:

- *Synchroniseren met iTunes:* Elke keer dat het mobiele apparaat wordt aangesloten op de computer, wordt het mobiele apparaat gesynchroniseerd. iTunes maakt niet automatisch een reservekopie van een mobiel apparaat waarvoor niet is ingesteld dat het mobiele apparaat met de computer moet worden gesynchroniseerd. Het mobiele apparaat kan ook handmatig worden gesynchroniseerd met behulp van iTunes.
- *Het mobiele apparaat bijwerken of herstellen:* iTunes maakt automatisch een reservekopie van het mobiele apparaat voordat het wordt bijgewerkt en hersteld.

Tip: iTunes kan reservekopieën van het mobiele apparaat ook versleutelen om uw gegevens te beveiligen (Zie hiervoor de gebruikershandleiding van iTunes[8]).

Een reservekopie terugzetten met iTunes
Met iTunes kunnen de gegevens van een reservekopie worden terugzetten op het mobiele apparaat, of de reservekopie kan worden gebruikt om de gegevens naar een andere mobiel apparaat te kopiëren.

Let op: Als een 'oude' reservekopie wordt terugzet, is het mogelijk dat appgegevens worden vervangen door gegevens die niet meer actueel zijn.

B0-06 Vervolg rationale

iOS **Met betrekking tot iOS 5.1**

Een reservekopie maken met iCloud
Met iCloud[9] kan (dagelijks) automatisch een reservekopie worden gemaakt van het mobiele apparaat via Wi-Fi, mits het apparaat is aangesloten op een voedingsbron en is vergrendeld.
iCloud maakt een reservekopie van:

- Aangeschafte muziek, tv-programma's, apps en boeken
- Foto's en video's in de Filmrol
- Instellingen van het mobiele apparaat
- Appgegevens
- Beginscherm en de ordening van de apps
- Berichten (iMessage-berichten, sms'jes en mms-berichten)
- Beltonen

Let op: Als automatisch een reservekopie wordt gemaakt met iCloud, kan niet tevens automatisch een reservekopie op de computer worden gemaakt met iTunes. Er kan dan wel handmatig met iTunes een reservekopie op de computer worden gemaakt.

Een reservekopie terugzetten met iCloud[10]
Met iCloud kunnen de gegevens van een reservekopie worden teruggezet op het mobiele apparaat.

Configureren

Deze functionaliteit/feature is handmatig te configureren via de gebruikersinterface van het mobiele apparaat. Zie hiervoor de gebruikershandleiding van het mobiele apparaat of het betreffende besturingssysteem.

Niveau 1	
iOS	**Android**
Ja	Ja

7. Ga voor meer informatie over reservekopieën, waaronder de instellingen en de gegevens die in een reservekopie worden bewaard naar support.apple.com/kb/HT1766?viewlocale=nl_NL.
8. http://www.apple.com/nl/itunes/how-to/
9. iCloud is beschikbaar op iOS 5-apparaten, op Macs met OS X Lion versie 10.7.2 of hoger en op pc's met het iCloud-configuratiescherm voor Windows (hiervoor is Windows Vista Service Pack 2 of Windows 7 vereist)
10. Ga voor meer informatie over het bijwerken en herstellen van de iPhone-software naar support.apple.com/kb/HT1414?viewlocale=nl_NL.

Nr.	Beveiligingslaag	Beschrijving van richtlijn
B0-07	Algemeen beleid	Jailbreak of root nooit het mobiele apparaat

Doelstelling

Het mobiele apparaat en de privacygevoelige en vertrouwelijke gegevens die op het mobiele apparaat worden verwerkt afdoende te beschermen en mogelijk misbruik door het vrijgeven van deze gegevens tot een minimum te beperken.

Rationale

Uw mobiele apparaat wordt niet meer beschermd door de beveiligingsmaatregelen die de leverancier heeft ingebouwd. Dankzij een jailbreak of root krijgt een gebruiker onbeperkt toegang tot het besturingssysteem. Hierdoor kunnen bezitters van het mobiele apparaat apps downloaden die niet in de officiële appstore te vinden zijn. Dit is niet in lijn met richtlijn B2-02 en B2-08.
De kans is dan ook aanwezig dat apps worden gedownload die malware bevatten en op deze manier het mobiele apparaat besmetten. Door de bescherming die in het besturingssysteem zit te omzeilen, is het systeem dus kwetsbaar voor allerlei soorten malware. Het advies is dan ook om het mobiele apparaat niet te jailbreaken of rooten.

Niveau 1

Ingevuld door richtlijn (functie / feature van het mobiele apparaat)

Niet van toepassing, maar is de verantwoordelijkheid van de gebruiker.

iOS	Android
Ja	Ja

HOOFDSTUK 3 » ALGEMEEN EN SPECIFIEK BELEID

HOOFDSTUK 4

Toegangscontrole

Nr.	Beveiligingslaag	Beschrijving van richtlijn
B1-01	Toegangscontrole	Versleutel opgeslagen gegevens waar mogelijk
	Doelstelling	
	Privacygevoelige en vertrouwelijke gegevens die op het mobiele apparaat worden verwerkt afdoende te beschermen en mogelijk misbruik door het vrijgeven van deze gegevens tot een minimum te beperken.	
	Rationale	
	Deze maatregel beschermt de privacygevoelige en vertrouwelijke gegevens bij verlies, diefstal of het onbeheerd achterlaten van het mobiele apparaat en voorkomt dat ongeautoriseerde apps deze gegevens kunnen lezen.	
	Niveau 1	
	Ingevuld door richtlijn (functie / feature van het mobiele apparaat)	
	Niet van toepassing, maar is de verantwoordelijkheid van de gebruiker.	
	iOS	**Android**
	Ja	Ja

Nr.	Beveiligingslaag	Beschrijving van richtlijn
B1-02	Toegangscontrole	Maak gebruik van verschillende toegangscodes voor het mobiele apparaat, de verschillende diensten en apps
	Doelstelling	
	• Het voorkomen van ongeautoriseerde toegang tot het mobiele apparaat, de verschillende diensten en apps. • Het mobiele apparaat, de privacygevoelige en vertrouwelijke gegevens die op het mobiele apparaat worden verwerkt afdoende te beschermen en het vrijgeven van deze gegevens tot een minimum te beperken. • De kans op misbruik van deze gegevens te minimaliseren en de schade bij misbruik zo beperkt mogelijk te houden.	
	Rationale	
	Veel mensen gebruiken vaak dezelfde toegangscode, het is echter verstandig om voor verschillende websites, diensten en apps verschillende toegangscodes te gebruiken. Je gebruikt tenslotte voor je huis, je auto en je kluisje ook niet dezelfde sleutel.[11] Door gebruik te maken van verschillende toegangscodes wordt de situatie voorkomen dat een kwaadwillende die één toegangscode heeft achterhaald bij alle accounts en gegevens kan, van bijvoorbeeld het mobiele apparaat, diensten en apps.	
	Niveau 1	
	Ingevuld door richtlijn (functie / feature van het mobiele apparaat)	
	Niet van toepassing, maar is de verantwoordelijkheid van de gebruiker.	
	iOS	**Android**
	Ja	Ja

11. Bron: digibewust.nl, http://www.digibewust.nl/onderwerpen/wachtwoorden

Nr.	Beveiligingslaag	Beschrijving van richtlijn
B1-03	Toegangscontrole	Wijzig regelmatig de toegangscode van het mobiele apparaat, de verschillende diensten en apps

Doelstelling

- Het voorkomen van ongeautoriseerde toegang tot het mobiele apparaat, de verschillende diensten en apps.
- Het mobiele apparaat, de privacygevoelige en vertrouwelijke gegevens die op het mobiele apparaat worden verwerkt afdoende te beschermen en het vrijgeven van deze gegevens tot een minimum te beperken.
- De kans op misbruik van deze gegevens te minimaliseren en de schade bij misbruik zo beperkt mogelijk te houden.

Rationale

Het is verstandig om regelmatig (bijvoorbeeld om de maand, of om de drie maanden) de toegangscodes te wijzigen en ervoor te zorgen dat deze niet te voorspelbaar worden bij het kiezen van een nieuwe toegangscode. Kies bijvoorbeeld geen opeenvolgende toegangscodes.

Bij verlies of diefstal van het mobiele apparaat is een toegangscode geen garantie voor vertrouwelijkheid en integriteit met betrekking tot de gegevens op het mobiele apparaat, maar het is wel de eerste drempel en vereist een extra inspanning van de kwaadwillende om het mobiele apparaat te compromitteren.[12]

Configureren

Deze functionaliteit/feature is handmatig te configureren via de gebruikersinterface van het mobiele apparaat, zie hiervoor de gebruikershandleiding van het mobiele apparaat of het betreffende besturingssysteem.

Niveau 1

Ingevuld door richtlijn (functie / feature van het mobiele apparaat)

Niet van toepassing, maar is de verantwoordelijkheid van de gebruiker.

iOS	Android
Ja	Ja

12. Lees meer informatie over het gebruik van (sterke) wachtwoorden op waarschuwingsdienst.nl: http://www.waarschuwingsdienst.nl/Computer+beveiligen/Wachtwoorden/Moelijke+wachtwoorden+op+een+makkelijke+manier.html, http://www.waarschuwingsdienst.nl/Computer+beveiligen/Wachtwoorden/Over+wachtwoorden+en+wachtwoorden+achterhalen.html; en, digibewust.nl http://www.digibewust.nl/onderwerpen/wachtwoorden.

Nr.	Beveiligingslaag	Beschrijving van richtlijn
B1-04	Toegangscontrole	Stel een toegangscode in om het mobiele apparaat te ontgrendelen

Doelstelling

- Het voorkomen van ongeautoriseerde toegang tot het mobiele apparaat.
- Het mobiele apparaat, de privacygevoelige en vertrouwelijke gegevens die op het mobiele apparaat worden verwerkt afdoende te beschermen en het vrijgeven van deze gegevens tot een minimum te beperken.
- De kans op misbruik van deze gegevens te minimaliseren en de schade bij misbruik zo beperkt mogelijk te houden.

Rationale

Het mobiele apparaat moet zo worden geconfigureerd dat een toegangscode wordt vereist voordat toegang wordt verkregen tot het mobiele apparaat.

Bij verlies of diefstal van het mobiele apparaat is een toegangscode geen garantie voor vertrouwelijkheid en integriteit van de gegevens op het mobiele apparaat, maar het is wel de eerste drempel en vereist een extra inspanning van de kwaadwillende om het mobiele apparaat te compromitteren.

Deze richtlijn alleen is vaak niet afdoende maar kan worden aangevuld met onder andere richtlijnen B1-01, B1-06, et cetera om het de kwaadwillende moeilijker te maken om het mobiele apparaat te compromitteren.

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 losse 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).

Configureren

Deze functionaliteit/feature is handmatig te configureren via de gebruikersinterface van het mobiele apparaat, zie hiervoor de gebruikershandleiding van het mobiele apparaat of het betreffende besturingssysteem.

Niveau 1

iOS	Android
Ja	Ja

Nr.	Beveiligingslaag	Beschrijving van richtlijn
B1-05	Toegangscontrole	Stel een toegangscode in om het mobiele apparaat te ontgrendelen die bestaat uit een combinatie van alfabetische, numerieke en niet-alfanumerieke tekens

Doelstelling

- Het voorkomen van ongeautoriseerde toegang tot het mobiele apparaat.
- Het mobiele apparaat, de privacygevoelige en vertrouwelijke gegevens die op het mobiele apparaat worden verwerkt afdoende te beschermen en het vrijgeven van deze gegevens tot een minimum te beperken.
- De kans op misbruik van deze gegevens te minimaliseren en de schade bij misbruik zo beperkt mogelijk te houden.

Rationale

Een mobiel apparaat kan zo worden geconfigureerd dat er wordt vereist dat een toegangscode uit numerieke, alfabetische en niet-alfanumerieke karakters moet bestaan.
Door een mix van alfabetische, numerieke en niet-alfanumerieke tekens wordt de complexiteit van de toegangscode verhoogd waardoor het voor een potentiële aanvaller lastiger wordt om via een brute-force-aanval toegang tot het mobiele apparaat te krijgen.

Configureren

Deze functionaliteit/feature is handmatig te configureren via de gebruikersinterface van het mobiele apparaat, zie hiervoor de gebruikershandleiding van het mobiele apparaat of het betreffende besturingssysteem.

Niveau 2

iOS	Android
Ja	Ja

Nr.	Beveiligingslaag	Beschrijving van richtlijn
B1-06	Toegangscontrole	Stel het maximaal aantal toegestane mislukte aanmeldingspogingen in

Doelstelling

- Het voorkomen van ongeautoriseerde toegang tot informatie op het (verloren of gestolen) mobiele apparaat
- Het mobiele apparaat, de privacygevoelige en vertrouwelijke gegevens die op het mobiele apparaat worden verwerkt afdoende te beschermen en het vrijgeven van deze gegevens tot een minimum te beperken.
- De kans op misbruik van deze gegevens te minimaliseren en de schade bij misbruik zo beperkt mogelijk te houden.

Rationale

Een mobiel apparaat kan zo worden geconfigureerd dat na x (bijvoorbeeld tien) mislukte pogingen om de toegangscode in te voeren, alle instellingen worden hersteld naar de standaardwaarden en al de gegevens en mediabestanden worden gewist door de coderingssleutel voor de gegevens te verwijderen.
Het veelvuldig fout invoeren van de toegangscode wijst over het algemeen op het feit dat het mobiele apparaat niet meer in het bezit is van de eigenaar maar in het bezit is van een kwaadwillende die probeert toegang te krijgen tot het mobiele apparaat.

Configureren

Deze functionaliteit/feature is handmatig te configureren via de gebruikersinterface van het mobiele apparaat, zie hiervoor de gebruikershandleiding van het mobiele apparaat of het betreffende besturingssysteem.

Niveau 1

iOS	Android
Ja	Ja

Nr.	Beveiligingslaag	Beschrijving van richtlijn
B1-07	Toegangscontrole	Schakel SIM-kaartvergrendeling in

Doelstelling

- Het voorkomen van ongeautoriseerde toegang tot de informatie op de SIM-kaart
- Het mobiele apparaat, de privacygevoelige en vertrouwelijke gegevens die op het mobiele apparaat (SIM-kaart) worden verwerkt afdoende te beschermen en het vrijgeven van deze gegevens tot een minimum te beperken.
- De kans op misbruik van deze gegevens te minimaliseren en schade bij misbruik zo beperkt mogelijk te houden.

Rationale

SIM-kaarten bevatten vaak contactgegevens en andere persoonlijke informatie waarvan de vertrouwelijkheid en integriteit moeten worden gegarandeerd. Deze instelling vergrendelt de SIM-kaart, zodat een pincode wordt gevraagd om toegang te krijgen tot de informatie op de SIM-kaart.
Partijen die niet in het bezit zijn van de pincode, mogen niet in staat zijn om de gegevens op de SIM-kaart te bekijken. Ze mogen ook niet in staat zijn om de SIM-kaart in een ander mobiel apparaat te gebruiken.

Configureren

Deze functionaliteit/feature is handmatig te configureren via de gebruikersinterface van het mobiele apparaat, zie hiervoor de gebruikershandleiding van het mobiele apparaat of het betreffende besturingssysteem.

Niveau 1

iOS	Android
Ja	Ja

Nr.	Beveiligingslaag	Beschrijving van richtlijn
B1-08	Toegangscontrole	Stel automatische vergrendeling in waardoor het mobiele apparaat na een bepaalde periode wordt vergrendeld.

Doelstelling

- Het voorkomen van ongeautoriseerde toegang tot het mobiele apparaat.
- Het mobiele apparaat, de privacygevoelige en vertrouwelijke gegevens die op het mobiele apparaat worden verwerkt afdoende te beschermen en het vrijgeven van deze gegevens tot een minimum te beperken.
- De kans op misbruik van deze gegevens te minimaliseren en schade bij misbruik zo beperkt mogelijk te houden.

Rationale

Een mobiel apparaat kan zo worden geconfigureerd dat het automatisch wordt vergrendeld na een vooraf bepaalde periode van inactiviteit.
Als richtlijn kan worden aangehouden dat een time-out van 5 minuten moet worden ingesteld als het mobiele apparaat wordt gebruikt voor reguliere werkzaamheden en een time-out van 1 à 2 minuten moet worden ingesteld als het mobiele apparaat wordt gebruikt bij werkzaamheden waarbij een verhoogd beveiligingsniveau gehanteerd dient te worden.

Let op: Hoe groter de periode voordat het mobiele apparaat automatisch wordt vergrendeld, hoe groter het risico dat een kwaadwillende het mobiele apparaat in een ontgrendelde toestand aantreft.

Configureren

Deze functionaliteit/feature is handmatig te configureren via de gebruikersinterface van het mobiele apparaat, zie hiervoor de gebruikershandleiding van het mobiele apparaat of het betreffende besturingssysteem.

Niveau 1

iOS	Android
Ja	Ja

Nr.	Beveiligingslaag	Beschrijving van richtlijn
B1-09	Toegangscontrole	Sta apps niet toe om de gecodeerde opslag van certificaten, toegangscodes en andere credentials te benaderen

Doelstelling

- Het voorkomen van ongeautoriseerde toegang tot de informatie die in de referentieopslag wordt bewaard
- Het mobiele apparaat (referentieopslag), de privacygevoelige en vertrouwelijke gegevens die op het mobiele apparaat worden verwerkt afdoende te beschermen en het vrijgeven van deze gegevens tot een minimum te beperken.
- De kans op misbruik van deze gegevens te minimaliseren en schade bij misbruik zo beperkt mogelijk te houden.

Rationale

Deze optie geeft apps toestemming om de gecodeerde opslag van beveiligde certificaten, verwante wachtwoorden en andere referenties op het mobiele apparaat te openen. De referentieopslag wordt gebruikt om bepaalde VPN- en Wi-Fi-verbindingen tot stand te brengen.

Mobiele apparaten bevatten niet alleen informatie, maar ook wachtwoorden en andere referenties die een aanvaller de gelegenheid geven om vertrouwelijke gegevens uit andere bronnen te achterhalen waar het mobiele apparaat gegevens mee uitwisselt.

Het versleutelen van de referentieopslag en het verhinderen van toegang van apps tot de gecodeerde opslag van certificaten, toegangscodes en andere credentials beperkt de blootstelling van persoonsgegevens uitsluitend tot het mobiele apparaat zelf. Kwaadwillenden kunnen hierdoor geen gebruik maken van de credentials die in de versleutelde referentieopslag worden bewaard.

Configureren

Deze functionaliteit/feature is handmatig te configureren via de gebruikersinterface van het mobiele apparaat, zie hiervoor de gebruikershandleiding van het mobiele apparaat of het betreffende besturingssysteem.

Niveau 2

iOS	Android
iOS bevat deze instelling niet	Ja

Nr.	Beveiligingslaag	Beschrijving van richtlijn
B1-10	Toegangscontrole	Schakel het tonen van de toegangscode tijdens het invoeren uit

Doelstelling

- Het voorkomen van ongeautoriseerde toegang tot het mobiele apparaat.
- Het mobiele apparaat, de privacygevoelige en vertrouwelijke gegevens die op het mobiele apparaat worden verwerkt afdoende te beschermen en het vrijgeven van deze gegevens tot een minimum te beperken.
- De kans op misbruik van deze gegevens te minimaliseren en de schade bij misbruik zo beperkt mogelijk te houden.
- Het voorkomen dat derden via meekijken de toegangscode weten te achterhalen.

Rationale

Het weergeven van wachtwoorden als deze worden ingetypt minimaliseert de kans op fouten tijdens het invoeren.
Zelfs als maar een karakter per keer getoond wordt, stelt dit een kwaadwillende in staat door mee te kijken/observeren (schoudersurfen) de toegangscode te achterhalen. Het wordt aanbevolen om deze functie uit te schakelen.

Configureren

Deze functionaliteit/feature is handmatig te configureren via de gebruikersinterface van het mobiele apparaat, zie hiervoor de gebruikershandleiding van het mobiele apparaat of het betreffende besturingssysteem.

Niveau 2

iOS	Android
iOS bevat deze instelling niet	Ja

Nr.	Beveiligingslaag	Beschrijving van richtlijn
B1-11	Toegangscontrole	Schakel voorvertoning van berichten (voor Android alleen SMS-berichten) op het beginscherm uit.

Doelstelling

- Het voorkomen dat ongeautoriseerde personen berichten (voor Android alleen SMS-berichten) kunnen lezen
- De privacygevoelige en vertrouwelijke gegevens die op het mobiele apparaat worden verwerkt afdoende te beschermen en het vrijgeven van deze gegevens tot een minimum te beperken.
- De kans op misbruik van deze gegevens te minimaliseren en de schade bij misbruik zo beperkt mogelijk te houden.

Rationale

Als een mobiel apparaat is vergrendeld en er is een toegangscode nodig om het mobiele apparaat te ontgrendelen, bestaat de mogelijkheid om deze berichten (SMS-berichten voor Android) toch te tonen op het beginscherm.
Het wordt aanbevolen om de voorvertoning van berichten (SMS-berichten voor Android) op het beginscherm uit te schakelen voor alle apps waarbij privacy en vertrouwelijkheid met betrekking tot de berichtgeving moet worden gegarandeerd.

Configureren

Deze functionaliteit/feature is handmatig te configureren via de gebruikersinterface van het mobiele apparaat, zie hiervoor de gebruikershandleiding van het mobiele apparaat of het betreffende besturingssysteem.

Niveau 2

iOS	Android
Ja	Ja

Nr.	Beveiligingslaag	Beschrijving van richtlijn
B1-12	Toegangscontrole	Schakel de functies die ondersteuning bieden bij het ontwikkelen van apps - zoals USB-foutopsporing[13] - uit

Doelstelling

- Het voorkomen van ongeautoriseerde toegang tot het mobiele apparaat.
- Het mobiele apparaat, de privacygevoelige en vertrouwelijke gegevens die op het mobiele apparaat worden verwerkt afdoende te beschermen en het vrijgeven van deze gegevens tot een minimum te beperken.
- De kans op misbruik van deze gegevens te minimaliseren en de schade bij misbruik zo beperkt mogelijk te houden.

Rationale

Het besturingssysteem stelt ontwikkelaars onder andere in staat om foutopsporingsprogramma's op een computer te machtigen om via een USB-verbinding met het mobiele apparaat te communiceren (USB-foutopsporing). Deze USB-poort wordt ook gebruikt om het mobiele apparaat op te laden. Er moet worden voorkomen dat het opladen van het mobiele apparaat een kwaadwillende de gelegenheid biedt om op deze manier het mobiele apparaat aan te vallen.

Configureren

Deze functionaliteit/feature is handmatig te configureren via de gebruikersinterface van het mobiele apparaat, zie hiervoor de gebruikershandleiding van het mobiele apparaat of het betreffende besturingssysteem.

Niveau 2

iOS	Android
Deze functie wordt niet ondersteund door iOS en vormt dus geen risico voor iOS	Ja

13. Deze optie machtigt foutopsporingsprogramma's op een computer om via een USB-verbinding met het mobiele apparaat te communiceren.

Nr.	Beveiligingslaag	Beschrijving van richtlijn
B1-13	Toegangscontrole	Maak gebruik van volgsoftware[14]

Doelstelling

- Zorgdragen dat een verloren of gestolen mobiel apparaat terug wordt gevonden en ongeautoriseerde toegang tot het mobiele apparaat wordt voorkomen.
- Het mobiele apparaat, de privacygevoelige en vertrouwelijke gegevens die op het mobiele apparaat worden verwerkt afdoende te beschermen en het vrijgeven van deze gegevens tot een minimum te beperken.
- De kans op misbruik van deze gegevens te minimaliseren en de schade bij misbruik zo beperkt mogelijk te houden.

Rationale

Installeer volgsoftware op het mobiele apparaat. Voorbeelden van dergelijke applicaties zijn Zoek mijn iPhone voor iOS en Lookout, Prey of Samsung Dive voor Android.[15]

Let op: Deze functionaliteit werkt niet op het moment dat het mobiele apparaat uit staat, in vliegtuigmodus staat of de SIM-kaart is verwijderd of verwisseld.
Beveiligingstoepassingen van derden[16] 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 wissen.

iOS Voor iOS geldt dat dit standaardfunctionaliteit is die via de optie 'Zoek mijn iPhone' wordt aangeboden. Zoek mijn iPhone biedt de volgende functies: de iPhone op een kaart tonen, een bericht op het mobiele apparaat weergeven, een geluid op het mobiele apparaat laten afspelen, het scherm laten vergrendelen of de gegevens extern wissen.

iOS maakt hierbij gebruik van de clouddienst iCloud. Net zoals aangegeven bij richtlijn B0-02, dient inzichtelijk te zijn welke privacygevoelige en vertrouwelijke gegevens men wil toevertrouwen aan een clouddienst, gebaseerd op een bewuste en weloverwogen afweging.[17]

Configureren

iOS
- Instellen van de iCloud omgeving (onder andere 'Zoek mijn iPhone' inschakelen).
- Deze functionaliteit/feature is handmatig te configureren via de gebruikersinterface van het mobiele apparaat, zie hiervoor de gebruikershandleiding van het mobiele apparaat of het betreffende besturingssysteem.

Niveau 1

iOS	Android
Ja	Ja

14. 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.
15. http://www.rijksoverheid.nl/nieuws/2012/10/09/start-straatroofcampagnes-straatroof-is-triest-en-hier-waak-ik.html
16. http://www.av-comparatives.org/images/stories/test/mobile/mobile2011_english.pdf en http://mobile-security-software-review.toptenreviews.com/
17. https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/whitepaper-cloud-computing.html

HOOFDSTUK 5

Applicatie

Nr.	Beveiligingslaag	Beschrijving van richtlijn
B2-01	Applicatie	Het aantal geïnstalleerde apps dient te worden beperkt.

Doelstelling

- Het aantal kwetsbaarheden op het mobiele apparaat tot een minimum te beperken
- Het mobiele apparaat, de privacygevoelige en vertrouwelijke gegevens die op het mobiele apparaat worden verwerkt afdoende te beschermen en het vrijgeven van deze gegevens tot een minimum te beperken
- De kans op misbruik van deze gegevens te minimaliseren en de schade bij misbruik zo beperkt mogelijk te houden.

Rationale

De eenvoudigste manier om kwetsbaarheden door gebruik van bepaalde apps te voorkomen is door apps überhaupt niet te installeren.

Opmerking: Controleer ook de voorgeïnstalleerde apps voordat het mobiele apparaat in gebruik wordt genomen, bij twijfel over deze apps is het advies om deze te de-installeren.

Niveau 1

Ingevuld door richtlijn (functie / feature van het mobiele apparaat)

Niet van toepassing, maar is de verantwoordelijkheid van de gebruiker.

iOS	Android
Ja	Ja

Nr.	Beveiligingslaag	Beschrijving van richtlijn
B2-02	Applicatie	Installeer alleen apps op het moment dat bekend is wie deze app heeft gemaakt en de maker van deze app wordt vertrouwd.

Doelstelling

- Het aantal kwetsbaarheden op het mobiele apparaat tot een minimum te beperken
- Het mobiele apparaat, de privacygevoelige en vertrouwelijke gegevens die op het mobiele apparaat worden verwerkt afdoende te beschermen en het vrijgeven van deze gegevens tot een minimum te beperken
- De kans op misbruik van deze gegevens te minimaliseren en schade bij misbruik zo beperkt mogelijk te houden.

Rationale

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.

Opmerking: Ga echter niet blindelings uit van het feit dat de ontwikkelaars van apps zich ook altijd houden aan de geldende voorwaarden en het privacybeleid.

Niveau 1

Ingevuld door richtlijn (functie / feature van het mobiele apparaat)

B2-08 Installeer alleen apps als de bron bekend is.

iOS	Android
Ja	Ja

Nr.	Beveiligingslaag	Beschrijving van richtlijn
B2-03	Applicatie	Beperk de rechten van geïnstalleerde apps tot een absoluut minimum

Doelstelling

Privacygevoelige en vertrouwelijke gegevens die op het mobiele apparaat worden verwerkt afdoende te beschermen en mogelijk misbruik door het vrijgeven van deze gegevens tot een minimum te beperken.

Rationale

Aan apps dienen de (absoluut) minimale bevoegdheden te worden toegekend die vereist zijn om aan hen toegewezen taken uit te voeren. Hoe meer bevoegdheden (of mogelijkheden) een app heeft, hoe meer mogelijkheden de app heeft om een kwetsbaarheid te vormen.

Niveau 1

Ingevuld door richtlijn (functie / feature van het mobiele apparaat)

Niet van toepassing, maar is de verantwoordelijkheid van de gebruiker.

iOS	Android
Ja	Ja

Nr.	Beveiligingslaag	Beschrijving van richtlijn
B2-04	Applicatie	Configureer de browser zodanig dat het noodzakelijke beveiligingsniveau wordt gegarandeerd

Doelstelling

- Het voorkomen van ongeautoriseerde toegang tot het mobiele apparaat.
- Het mobiele apparaat, de privacygevoelige en vertrouwelijke gegevens die op het mobiele apparaat worden verwerkt afdoende te beschermen en het vrijgeven van deze gegevens tot een minimum te beperken.
- De kans op misbruik van deze gegevens te minimaliseren en schade bij misbruik zo beperkt mogelijk te houden.

Rationale

De browser biedt een aantal instellingen die zorg dragen voor het noodzakelijke beveiligingsniveau. Het is verstandig om deze aandachtig te bestuderen en op basis van bewuste afweging een bepaalde instelling wel of juist niet te configureren.

Niveau 1

Ingevuld door richtlijn (functie / feature van het mobiele apparaat)

B2-09 Schakel JavaScript uit.
B2-10 Schakel fraudemeldingen in.
B2-11 Schakel automatisch vullen van webformulieren uit.
B2-12 Schakel Privémodus (Incognitomodus) in.
B2-13 Schakel cookies accepteren uit.
B2-14 Schakel beveiligingswaarschuwingen weergeven in.

iOS	Android
Ja	Ja

Nr.	Beveiligingslaag	Beschrijving van richtlijn
B2-05	Applicatie	Voorzie tijdig alle software van de laatste versies/patches

Doelstelling

Het aantal kwetsbaarheden op het mobiele apparaat tot een minimum te beperken en mogelijke uitbuiting van kwetsbaarheden voor te zijn.

Rationale

Denk hierbij aan zowel het mobiele besturingssysteem (firmware) als de apps die op het mobiele apparaat zijn geïnstalleerd.
Op het moment dat een mobiel apparaat wordt aangeschaft beschikt het over de softwareversies die 'geldig' waren op het moment dat het mobiele apparaat werd gefabriceerd. Het is dan ook niet ondenkbaar dat er updates beschikbaar zijn gekomen sinds die tijd. Het wordt aanbevolen om de software op het mobiele apparaat voor gebruik bij te werken naar de laatste versies en deze software in de toekomst ook actueel te houden.
Software-updates bevatten naast nieuwe functionaliteiten en bugfixes[18] vaak ook beveiligingsupdates.

Android **Apps bijwerken**

Nadat apps zijn gedownload en geïnstalleerd, kunnen deze zo worden geconfigureerd dat de apps zichzelf automatisch bijwerken. Ga naar Google Play, de appstore van Android die eerder bekend-stond als Android Market, en navigeer naar Mijn apps. Hier staan de apps die momenteel op het mobiele apparaat zijn geïnstalleerd. Onder het kopje Handmatige updates wordt weergegeven welke apps aan een update toe zijn. Iedere app kan afzonderlijk worden bijgewerkt of alle apps kunnen in één keer worden bijgewerkt.
Als u apps automatisch wilt laten voorzien van de updates, moet u dit per app aangeven. In het detailscherm van de app moet de functie Automatisch bijwerken toestaan ingeschakeld worden.

Android-besturingssysteem bijwerken

Het Android-besturingssysteem wordt op het mobiele apparaat van meerdere fabrikanten gebruikt. Het resultaat is dat een nieuwe versie van het Android-besturingssysteem aangepast moet worden voor de verschillende typen mobiele apparaten die Android als besturingssysteem gebruiken. Als de software is aangepast wordt deze via de telecomproviders van de verschillende landen gedistribueerd. Wanneer en of het mobiele apparaat kan worden voorzien van de laatste versie van het Android-besturingssysteem is dus afhankelijk van de fabrikant: is deze bereid om het Android-besturingssysteem aan te passen aan het betreffende type mobiele apparaat.

iOS **Apps bijwerken**

Zodra de App Store wordt bezocht, wordt gecontroleerd of er updates beschikbaar zijn voor de geïnstalleerde apps. De App Store controleert bovendien elke week automatisch of er updates beschikbaar zijn.

iOS-besturingssysteem bijwerken

- iOS 4.2/4.3: Het iOS-besturingssysteem kan worden bijgewerkt met iTunes op de computer.
- Vanaf iOS 5.1: Het iOS-besturingssysteem kan worden bijgewerkt via Over-the-Air of met iTunes op de computer. Het bijwerken van het mobiele apparaat via Over-the-Air kan zowel via Wi-Fi als via het mobiele datanetwerk. Niet alle iOS-updates kunnen via het mobiele datanetwerk worden gedownload in verband met de grootte van de update. Soms wordt het downloaden via het mobiele datanetwerk niet ondersteund door de telecomprovider, die eist dat gebruikers een Wi-Fi-netwerk gebruiken.

18. 'bug' is de naam die wordt gebruikt om een fout in een sotwareprogramma aan te duiden. Bugfixes zijn oplossingen voor deze fouten. Het zijn meestal kleine programma's die geschreven zijn om een fout in een sotwareprogramma op te lossen.

B2-05	**Vervolg rationale**

Tip: Zorg ervoor dat een reservekopie van het mobiele apparaat is gemaakt voordat de update wordt uitgevoerd om eventueel verlies van gegevens te voorkomen, mocht het bijwerken van het besturingssysteem mislukken. Als specifieke software wordt gebruikt om het besturingssysteem bij te werken, zoals iTunes voor het iOS-besturingssysteem, kan het zijn dat er automatisch een reservekopie van het mobiele apparaat wordt gemaakt voordat het besturingssysteem wordt bijgewerkt (zie ook B0-06).

Tip: Om het Android mobiele apparaat en persoonlijke gegevens te beschermen, moet het downloaden van apps alleen worden toegestaan van vertrouwde bronnen (zie ook B2-08).

Configureren

Deze functionaliteit/feature is handmatig te configureren via de gebruikersinterface van het mobiele apparaat, zie hiervoor de gebruikershandleiding van het mobiele apparaat of het betreffende besturingssysteem.

Niveau 1	
iOS	**Android**
Ja	Ja

Nr.	Beveiligingslaag	Beschrijving van richtlijn
B2-06	Applicatie	Locatievoorzieningen dienen zoveel mogelijk te zijn uitgeschakeld

Doelstelling

Het beschermen van locatiegegevens en mogelijk misbruik door het vrijgeven van deze gegevens tot een minimum te beperken.

Rationale

Voorkom dat locatiegegevens onbedoeld gekoppeld worden aan foto's, video's, berichten, et cetera en dat deze hierdoor misbruikt kunnen worden. Het gebruik van locatiegegevens kan over het algemeen totaal worden uitgezet of per app worden bepaald.

De locatie van het mobiele apparaat, en dus indirect van de gebruiker, wordt bepaald aan de hand van de volgende informatiebronnen:
- Beschikbare informatie van mobiele datanetwerken
- Lokale Wi-Fi-netwerken (als Wi-Fi is ingeschakeld)
- Global Positioning System (GPS) (mits beschikbaar)

Android Er kan bij Android niet per app worden aangegeven of deze gebruik mag maken van locatiegegevens: het is in feite alles of niets. Iedere app kan locatiegegevens versturen als deze locatiegegevens beschikbaar zijn op het mobiele apparaat.
Het is echter wel mogelijk om locatievoorzieningen in of uit te schakelen voor websites. Het is hierdoor mogelijk om websites met locatiespecifieke inhoud toe te staan om de gebruiker te vragen of de locatie gedeeld mag worden op basis van de locatiegegevens van het mobiele apparaat. Hiervoor moet het delen van de locatie wel zijn ingeschakeld.

iOS Voor iOS kan het delen van locatiegegevens in of uit worden geschakeld. Op het moment dat dit is ingeschakeld kan per iOS app worden ingesteld of deze gebruik mag maken van deze locatiegegevens.

Tip: Als apps gebruikmaken van locatievoorzieningen, is het aan te raden eerst de voorwaarden en het privacybeleid van de fabrikant/leverancier van de app te lezen, zodat inzichtelijk wordt hoe de app in kwestie de locatiegegevens gebruikt.

Configureren

Deze functionaliteit/feature is handmatig te configureren via de gebruikersinterface van het mobiele apparaat, zie hiervoor de gebruikershandleiding van het mobiele apparaat of het betreffende besturingssysteem.

Niveau 1	
iOS	**Android**
Ja	Ja

Nr.	Beveiligingslaag	Beschrijving van richtlijn
B2-07	Applicatie	Het mobiele apparaat dient 'schoon' in te worden geleverd

Doelstelling

- Privacygevoelige en vertrouwelijke gegevens die op het mobiele apparaat worden verwerkt afdoende te beschermen en mogelijk misbruik door het vrijgeven van deze gegevens tot een minimum te beperken.
- Waarborgen dat geen gegevens kunnen worden achterhaald op het moment dat het mobiele apparaat is ingeleverd, verkocht of wordt gerepareerd.

Rationale

Het wissen van de gegevens op het mobiele apparaat en het herstellen naar de fabrieksinstellingen vermindert de kans dat een aanvaller in staat is om gevoelige informatie te achterhalen van het mobiele apparaat.

Bij normaal gebruik maakt zowel een mobiel apparaat met iOS als een met Android geen gebruik van een beveiligde wisfunctie om gegevens van de schijf te wissen, waardoor de verwijderde gegevens kunnen worden hersteld. Daarom moet de schijf worden overschreven via de optie 'Wis alle inhoud en instellingen' voor iOS en de optie 'Fabrieksinstellingen terugzetten' voor Android voordat het mobiele apparaat niet meer onder controle is van de gebruiker. Denk hierbij aan de volgende situaties:

- Het mobiele apparaat is verkocht
- Het mobiele apparaat is defect en moet worden gerepareerd
- Het mobiele apparaat is afgeschreven en wordt afgevoerd/weggegooid
- Het mobiele apparaat wordt overhandigd aan een andere gebruiker

Let op: De volgende situatie heeft nogal wat juridische consequenties: Een gebruiker heeft een mobiel apparaat in privé-eigendom maar gebruikt het mobiele apparaat ook voor zakelijke doeleinden. Mag de werkgever de gegevens op het mobiele apparaat wissen op het moment dat bijvoorbeeld de medewerker uit dienst gaat?[19]

Om te controleren of de gegevens ook van het mobiele apparaat zijn verwijderd, zowel van lokale opslag als van verwijderbare opslagmedia, is het noodzakelijk om een forensische toolkit te installeren.
Opmerking: Om deze forensische toolkits te kunnen gebruiken dient men over specialistische kennis te beschikken. Dit is niet aan te raden voor beginners of onervaren gebruikers.

iOS

Apps verwijderen
Nadat een app is verwijderd, zijn de bijbehorende gegevens niet meer toegankelijk via de gebruikersinterface van het mobiele apparaat. De gegevens zijn echter nog niet van het mobiele apparaat verwijderd. Zie 'Wis alle inhoud en instellingen' om alle inhoud en instellingen te verwijderen.

Wis alle inhoud en instellingen
Via de optie 'Wis alle inhoud en instellingen' worden alle instellingen hersteld naar de standaardwaarden en worden al de gegevens en mediabestanden gewist door de coderingssleutel te verwijderen.

Android

Via de optie 'Fabrieksinstellingen terugzetten' worden alle persoonlijke gegevens uit het interne geheugen gewist, inclusief informatie over het gekoppelde Google-account, andere accounts, de instellingen van het systeem en apps en eventueel gedownloade apps. Als het mobiele apparaat opnieuw wordt ingesteld, worden eventuele systeemupdates die zijn gedownload niet gewist.

Tip: Vergeet niet om ook de gegevens van de USB-opslag of de SD-kaart (afhankelijk van het model mobiele apparaat) te verwijderen. Deze kunnen bestanden bevatten die zijn gedownload of gekopieerd.

19. Factsheet Bring your own device juridisch bekeken: http://ictrecht.nl/factsheets/byod-bring-your-own-device-juridisch-bekeken/

B2-07 **Vervolg configureren**

Deze functionaliteit/feature is handmatig te configureren via de gebruikersinterface van het mobiele apparaat, zie hiervoor de gebruikershandleiding van het mobiele apparaat of het betreffende besturingssysteem.

Niveau 1

iOS	Android
Ja	Ja

Nr.	Beveiligingslaag	Beschrijving van richtlijn
B2-08	Applicatie	Installeer alleen apps als de bron bekend is

Doelstelling

- Het aantal kwetsbaarheden op het mobiele apparaat tot een minimum te beperken en mogelijke uitbuiting van kwetsbaarheden voor te zijn.
- Het voorkomen dat apps geïnstalleerd kunnen worden via niet-vertrouwde distributiekanalen.

Rationale

Apps die zijn gedownload van internet kunnen afkomstig zijn van onbekende bronnen. Om het mobiele apparaat en persoonlijke gegevens te beschermen, is het het beste om alleen apps te downloaden van vertrouwde bronnen, zoals Google Play (voorheen Android Market) of de Apple App Store.

Android Android biedt de mogelijkheid om apps te installeren die zijn gedownload van het internet of die zijn ontvangen via e-mail waarvan de bron onbekend is. Via deze instelling kan aangegeven worden dat apps alleen gedownload kunnen worden van vertrouwde bronnen zoals Google Play.

iOS Voor iOS geldt dat apps alleen gedownload kunnen worden van de App Store.

Als u een gegeven app zoekt, zorgt het blokkeren van installatie van apps uit niet-vertrouwde distributiekanalen ervoor dat de kans groter is dat de gezochte app ook degene is die u hebt gedownload.

Opmerking: Google vereist dat de applicatieontwikkelaars hun apps digitaal ondertekenen en deze via de appstore van Android, Google Play, distribueren.

Configureren

Deze functionaliteit/feature is handmatig te configureren via de gebruikersinterface van het mobiele apparaat, zie hiervoor de gebruikershandleiding van het mobiele apparaat of het betreffende besturingssysteem.

Niveau 1

iOS	Android
Voor iOS geldt dat het niet mogelijk is om van deze richtlijn af te wijken.	Ja

Nr.	Beveiligingslaag	Beschrijving van richtlijn
B2-09	Applicatie	Schakel JavaScript uit

Doelstelling

- Het voorkomen van ongeautoriseerde toegang tot het mobiele apparaat, doordat de kans wordt verlaagd dat het mobiele apparaat via kwetsbaarheden in JavaScript wordt aangevallen.
- Het mobiele apparaat, de privacygevoelige en vertrouwelijke gegevens die op het mobiele apparaat worden verwerkt afdoende te beschermen en het vrijgeven van deze gegevens tot een minimum te beperken.
- De kans op misbruik van deze gegevens te minimaliseren en de schade bij misbruik zo beperkt mogelijk te houden.

Rationale

JavaScript is een scripttaal die veel gebruikt wordt om webpagina's interactief te maken en webapplicaties te ontwikkelen. Ook kunnen onderdelen op de pagina worden bestuurd, zoals het weergeven van de huidige datum en tijd of het openen van een gekoppelde pagina in een pop-upvenster. Het wordt aanbevolen dat JavaScript en plug-ins zijn uitgeschakeld in omgevingen waar veiligheid voorop staat.

Let op: Deze maatregel kan tot gevolg hebben dat een webpagina niet voor de volle 100% functioneert zoals deze is ontworpen en ontwikkeld.

Als door omstandigheden toch gebruik moet worden gemaakt van JavaScript, zet dit dan alleen aan voor vertrouwde websites op basis van een whitelist.

Configureren

Deze functionaliteit/feature is handmatig te configureren via de gebruikersinterface van het mobiele apparaat, zie hiervoor de gebruikershandleiding van het mobiele apparaat of het betreffende besturingssysteem.

Niveau 2

iOS	Android
Ja	Ja

Nr.	Beveiligingslaag	Beschrijving van richtlijn
B2-10	Applicatie	Schakel fraudemeldingen in

Doelstelling

- Het voorkomen van ongeautoriseerde toegang tot het mobiele apparaat, doordat de kans wordt verlaagd dat het mobiele apparaat wordt besmet via fraudeleuze websites.
- Het mobiele apparaat, de privacygevoelige en vertrouwelijke gegevens die op het mobiele apparaat worden verwerkt afdoende te beschermen en het vrijgeven van deze gegevens tot een minimum te beperken.
- De kans op misbruik van deze gegevens te minimaliseren en de schade bij misbruik zo beperkt mogelijk te houden.

Rationale

Deze voorziening biedt bescherming tegen potentieel frauduleuze internetsites. Als een verdachte site wordt bezocht, verschijnt er een waarschuwing in Safari en wordt de pagina niet geladen. Het wordt aanbevolen om fraudemeldingen in te schakelen. Door het inschakelen van deze functie kan worden voorkomen dat per ongeluk een bekende phishingsite of andere fraudeleuze site wordt bezocht die wordt herkend door deze functionaliteit.

Let op: Het is wel belangrijk dat de gebruiker ook alert blijft bij het surfen: niet alle fraudeleuze sites worden als zodanig herkend door de functionaliteit.

Configureren

Deze functionaliteit/feature is handmatig te configureren via de gebruikersinterface van het mobiele apparaat, zie hiervoor de gebruikershandleiding van het mobiele apparaat of het betreffende besturingssysteem.

Niveau 1

iOS	Android
Ja	Android bevat deze instelling niet

Nr.	Beveiligingslaag	Beschrijving van richtlijn
B2-11	Applicatie	Schakel automatisch vullen van webformulieren uit

Doelstelling

- Vertrouwelijke gegevens van de gebruiker beschermen.
- Privacygevoelige en vertrouwelijke gegevens die op het mobiele apparaat worden verwerkt afdoende te beschermen en het vrijgeven van deze gegevens tot een minimum te beperken.
- De kans op misbruik van deze gegevens te minimaliseren en de schade bij misbruik zo beperkt mogelijk te houden.

Rationale

De browser heeft een functie om informatie te onthouden die in webformulieren is ingevuld zodat deze informatie kan worden gebruikt om later nieuwe webformulieren automatisch in te vullen. Informatie die automatisch wordt ingevuld kan onder andere persoonlijke gegevens zoals contacten, namen en wachtwoorden bevatten.

Het wordt aanbevolen om de iOS optie 'Automatisch vullen' uit te schakelen.
Het wordt aanbevolen om de Android optie 'Onthoud formuliergegevens' uit te schakelen.

Het uitschakelen van deze functionaliteit zorgt ervoor dat referenties niet lokaal worden opgeslagen op het mobiele apparaat en verlaagt ook de kans dat automatisch ongeautoriseerde toegang wordt verkregen tot een website in het geval ongeautoriseerde toegang tot het mobiele apparaat is verkregen.

iOS Als de optie Gebruik contactinfo is ingeschakeld (deze functionaliteit is standaard uitgeschakeld) en contactgegevens zijn geselecteerd, dan zal Safari de geselecteerde informatie uit Contacten gebruiken om de contactvelden in te vullen op web formulier.
Als Namen en wachtwoorden is ingeschakeld, dan zal Safari de namen en wachtwoorden onthouden die zijn ingevuld van bezochte websites en deze automatisch invullen als de website opnieuw wordt bezocht.

Configureren

Deze functionaliteit/feature is handmatig te configureren via de gebruikersinterface van het mobiele apparaat, zie hiervoor de gebruikershandleiding van het mobiele apparaat of het betreffende besturingssysteem.

Niveau 2

iOS	Android
Ja	Ja

Nr.	Beveiligingslaag	Beschrijving van richtlijn
B2-12	Applicatie	Schakel Privémodus (Incognitomodus) in

Doelstelling

- Vertrouwelijke gegevens (surfgedrag) van de gebruiker beschermen.
- De privacygevoelige en vertrouwelijke gegevens die op het mobiele apparaat worden verwerkt afdoende te beschermen en het vrijgeven van deze gegevens tot een minimum te beperken.
- De kans op misbruik van deze gegevens te minimaliseren en de schade bij misbruik zo beperkt mogelijk te houden.

Rationale

De browser houdt een geschiedenis bij van bezochte webpagina's, uitgevoerde zoekopdrachten en bepaalde informatie uit ingevulde webformulieren(zie richtlijn B2-11). Het volgen van deze informatie kan worden voorkomen door Privémodus (Incognitomodus) in te schakelen. Om er voor te zorgen dat er nog meer privacy wordt geboden en het voor derden nog moeilijker wordt om het surfgedrag van de gebruiker te volgen, wordt aanbevolen om het accepteren van cookies ook uit te schakelen (zie richtlijn B2-13).

Het inschakelen van Privémodus (Incognitomodus) beschermt bepaalde privé-informatie en blokkeert dat bepaalde websites het gedrag bijhouden van de gebruiker binnen deze browsersessie. Zo zullen de bezochte webpagina's, zoekgeschiedenis en informatie uit ingevulde webformulieren niet worden vastgelegd.

Opmerking: Deze Privémodus (Incognitomodus) voorkomt niet dat websites het IP-adres zien, zal niet voorkomen dat van websites cookies worden verzameld (zie richtlijn B2-13) en zal ook geen keyloggers of spyware tegenhouden. Hiervoor zullen aanvullende maatregelen genomen dienen te worden (zie richtlijn B0-04).

Configureren

Deze functionaliteit/feature is handmatig te configureren via de gebruikersinterface van het mobiele apparaat, zie hiervoor de gebruikershandleiding van het mobiele apparaat of het betreffende besturingssysteem.

Niveau 1

iOS	Android
Ja	Ja

Nr.	Beveiligingslaag	Beschrijving van richtlijn
B2-13	Applicatie	Schakel cookies accepteren uit

Doelstelling

- Vertrouwelijke gegevens (surfgedrag) van de gebruiker beschermen.
- De privacygevoelige en vertrouwelijke gegevens die op het mobiele apparaat worden verwerkt afdoende te beschermen en het vrijgeven van deze gegevens tot een minimum te beperken.
- De kans op misbruik van deze gegevens te minimaliseren en de schade bij misbruik zo beperkt mogelijk te houden.

Rationale

Cookies houden informatie bij over het bezoek aan websites. Maar betekent dit nu ook een bedreiging voor uw privacy op het internet?[20]

Voor uw gemak maken websites gebruik van cookies om bepaalde gegevens van het bezoek aan de site vast te leggen. Zo worden bijvoorbeeld voor sommige sites die met een wachtwoord zijn beveiligd, cookies gebruikt zodat deze niet bij elk bezoek opnieuw ingetypt hoeven te worden. Websites zoals Facebook, Gmail of Twitter, gebruiken cookies om logininformatie te bewaren zodat niet telkens opnieuw de gebruikersnaam en wachtwoord hoeven te worden opgegeven. Als een kwaadwillende deze cookies kan bemachtigen, kan hij zich als u voordoen en toegang verkrijgen tot privacygevoelige en vertrouwelijke gegevens binnen de betreffende site of onlinedienst.
Andere sites gebruiken cookies om voorkeuren te onthouden. De webpagina's worden dan bijvoorbeeld aangepast op basis van de informatie die eerder is verstrekt. De webserver van die website plaatst een cookie op het mobiele apparaat. Als u nu de volgende keer diezelfde website bezoekt, hoeft u bijvoorbeeld niet nogmaals aan te geven of u een voorkeur heeft voor de Nederlandstalige of de Engelstalige versie. Het cookie voor die specifieke website houdt uw voorkeur bij.

De enige functie van een cookie is het verstrekken van informatie aan derden. Cookies vormen dus geen gevaar voor het mobiele apparaat: ze installeren geen virussen of spyware en kunnen het mobiele apparaat niet aanpassen of laten crashen.

Soorten cookies
Er bestaan verschillende soorten cookies. We kunnen op twee manieren een onderscheid maken:
- Permanente versus tijdelijke cookies:
  - Permanente cookies blijven op het mobiele apparaat staan, ook nadat de browser is afgesloten.
  - Tijdelijke cookies worden verwijderd wanneer de browser afgesloten wordt. Deze cookies gelden enkel voor de lopende sessie en worden dus ook wel sessiecookies genoemd.
- Directe versus indirecte cookies:
  - Directe cookies (first-partycookies) zijn gemaakt door, of worden verzonden naar de website die wordt bezocht (bijvoorbeeld: de website http://www.vertrouwdewebsite.nl wordt bezocht, en vertrouwdewebsite.nl plaatst een cookie).
  - Indirecte cookies (third-partycookies) zijn gemaakt door, of worden verzonden naar een andere website dan degene die wordt bezocht (bijvoorbeeld de website http://www.vertrouwdewebsite.nl wordt bezocht, en een adverteerder op deze website plaatst een cookie)

Cookiewet[21]
Sinds 5 juni 2012 moeten op grond van de Telecommunicatiewet websites u informeren als zij cookies willen plaatsen die bijvoorbeeld uw surfgedrag bijhouden. Zij mogen deze alleen plaatsen als u hiervoor toestemming geeft.

Websites hebben uw toestemming niet nodig voor cookies die noodzakelijk zijn om een dienst of webshop te laten functioneren. Dit zijn bijvoorbeeld bestanden die bijhouden wat u in uw virtuele winkelwagentje heeft.

B2-13 Vervolg configureren

Deze functionaliteit/feature is handmatig te configureren via de gebruikersinterface van het mobiele apparaat, zie hiervoor de gebruikershandleiding van het mobiele apparaat of het betreffende besturingssysteem.

Niveau 1	
iOS	**Android**
Ja	Ja

Nr.	Beveiligingslaag	Beschrijving van richtlijn
B2-14	Applicatie	Schakel beveiligingswaarschuwingen weergeven in

Doelstelling

- Het voorkomen van ongeautoriseerde toegang tot het mobiele apparaat, doordat wordt gewaarschuwd op het moment dat (mogelijk) fraudeleuze websites worden bezocht.
- Het mobiele apparaat, de privacygevoelige en vertrouwelijke gegevens die op het mobiele apparaat worden verwerkt afdoende te beschermen en het vrijgeven van deze gegevens tot een minimum te beperken.
- De kans op misbruik van deze gegevens te minimaliseren en de schade bij misbruik zo beperkt mogelijk te houden.

Rationale

De browser ondersteund een aantal veiligheidscontroles waaronder de controle of een aangeboden SSL-certificaat[22] verlopen is en of het vermelde domein overeenkomt met de bezochte site.
Het wordt aanbevolen om beveiligingswaarschuwingen weergeven in te schakelen, er wordt dan door de browser gewaarschuwd voor websites met algemene beveiligingsproblemen, zoals verouderde of ongeldige certificaten.

Opmerking: Deze instelling zorgt er niet voor dat apps deze SSL-certificaten controleren, deze verantwoordelijkheid ligt bij de appontwikkelaars (zie ook richtlijn B2-08). Als SSL niet op de juiste manier in een app is geïmplementeerd, is deze app mogelijk kwetsbaar voor man-in-the-middleaanvallen omdat de SSL-certificaten niet of niet voldoende worden gecontroleerd.

Configureren

Deze functionaliteit/feature is handmatig te configureren via de gebruikersinterface van het mobiele apparaat, zie hiervoor de gebruikershandleiding van het mobiele apparaat of het betreffende besturingssysteem.

Niveau 1	
iOS	**Android**
iOS bevat deze instelling niet	Ja

20. Zie voor meer informatie het artikel 'Cookies: een bedreiging voor uw privacy?' op Waarschuwingsdienst.nl: http://www.waarschuwingsdienst.nl/Risicos/Inbreuk+op+je+privacy/Cookies-+een+bedreiging+voor+uw+privacy.html
21. Zie voor meer informatie met betrekking tot de cookiewet: http://www.rijksoverheid.nl/documenten-en-publicaties/persberichten/2012/06/01/nieuwe-telecommunicatiewet-treedt-5-juni-2012-in-werking.html en http://www.rijksoverheid.nl/onderwerpen/ict/veilig-online-en-e-privacy/internet-bezoek-volgen-met-cookies
22. SSL is de afkorting voor Secure Sockets Layer.

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

Nr.	Beveiligingslaag	Beschrijving van richtlijn
B3-01	Netwerk	Versleutel verzonden gegevens waar mogelijk

Doelstelling

Privacygevoelige en vertrouwelijke gegevens die op het mobiele apparaat worden verwerkt afdoende te beschermen en mogelijk misbruik door het vrijgeven van deze gegevens tot een minimum te beperken.

Rationale

Denk hierbij aan gegevensoverdracht tussen het mobiele apparaat en bijvoorbeeld:
- Onlineback-updiensten (zie ook richtlijn B0-05)
- Clouddiensten
- Bedrijfsnetwerken

Niveau 1

Ingevuld door richtlijn (functie / feature van het mobiele apparaat)

B3-10 Maak zoveel mogelijk gebruik van een VPN-verbinding.

iOS	Android
Ja	Ja

Nr.	Beveiligingslaag	Beschrijving van richtlijn
B3-02	Netwerk	Schakel netwerkverbindingen zoveel mogelijk uit wanneer deze niet worden gebruikt

Doelstelling

- Misbruik van deze netwerkverbindingen tot een minimum te beperken.
- De privacygevoelige en vertrouwelijke gegevens die via deze netwerkverbindingen worden verstuurd afdoende te beschermen en het vrijgeven van deze gegevens tot een minimum te beperken.
- De mogelijkheid dat het mobiele apparaat via het netwerk (op afstand) wordt aangevallen te verlagen en zo ongeautoriseerde toegang tot het mobiele apparaat te voorkomen.
- Het mobiele apparaat, de privacygevoelige en vertrouwelijke gegevens die op het mobiele apparaat worden verwerkt afdoende te beschermen en het vrijgeven van deze gegevens tot een minimum te beperken.
- De kans op misbruik van deze gegevens te minimaliseren en de schade bij misbruik zo beperkt mogelijk te houden.

Rationale

Op het moment dat netwerkverbindingen worden uitgeschakeld kan hier niet op een of andere manier misbruik van worden gemaakt.

Niveau 1

Ingevuld door richtlijn (functie / feature van het mobiele apparaat)

B3-03 Schakel de mobiele internetverbinding (mobiele data) uit als hier geen gebruik van wordt gemaakt.
B3-04 Schakel dataroaming uit als hier geen gebruik van wordt gemaakt
B3-05 Schakel Persoonlijke hotspot uit als hier geen gebruik van wordt gemaakt.
B3-06 Schakel Wi-Fi uit als hier geen gebruik van wordt gemaakt.
B3-07 Stel het mobiele apparaat zo in dat Wi-Fi-netwerken, waar eerder verbinding mee is gemaakt, worden vergeten.
B3-08 Stel het mobiele apparaat zo in dat er niet wordt gevraagd om een verbinding te maken met een Wi-Fi-netwerk.

B3-02	Vervolg ingevuld door richtlijn (functie / feature van het mobiele apparaat)	
	B3-09 Stel het mobiele apparaat zo in dat er niet automatisch met een Wi-Fi-netwerk wordt verbonden. B3-11 Schakel Bluetooth uit als hier geen gebruik van wordt gemaakt. B3-12 Schakel Near Field Communication (NFC) uit als hier geen gebruik van wordt gemaakt. B3-13 Schakel vliegtuigmodus in als geen draadloze netwerkverbindingen en voorzieningen nodig zijn.	
	iOS	**Android**
	Ja	Ja

Nr.	Beveiligingslaag	Beschrijving van richtlijn
B3-03	Netwerk	Schakel de mobiele internetverbinding (mobiele data) uit als hier geen gebruik van wordt gemaakt[23]

Doelstelling

- Misbruik van deze netwerkverbindingen tot een minimum te beperken.
- De privacygevoelige en vertrouwelijke gegevens die via deze netwerkverbindingen worden verstuurd afdoende te beschermen en het vrijgeven van deze gegevens tot een minimum te beperken.
- De mogelijkheid dat het mobiele apparaat via het netwerk (op afstand) wordt aangevallen te verlagen en zo ongeautoriseerde toegang tot het mobiele apparaat te voorkomen.
- Het mobiele apparaat, de privacygevoelige en vertrouwelijke gegevens die op het mobiele apparaat worden verwerkt afdoende te beschermen en het vrijgeven van deze gegevens tot een minimum te beperken.
- De kans op misbruik van deze gegevens te minimaliseren en de schade bij misbruik zo beperkt mogelijk te houden.

Rationale

Als de mobiele internetverbinding (mobiel data) is uitgeschakeld, kunnen geen gegevens via het mobiele netwerk worden verstuurd. Apps waarvoor een internetverbinding is vereist, werken niet tenzij het mobiele apparaat via Wi-Fi toegang heeft tot het internet.

Configureren

Deze functionaliteit/feature is handmatig te configureren via de gebruikersinterface van het mobiele apparaat, zie hiervoor de gebruikershandleiding van het mobiele apparaat of het betreffende besturingssysteem.

Niveau 2

iOS	Android
Ja	Ja

23. Dit is een ongebruikelijke (ongewone) instelling voor een mobiel apparaat en beperkt de functionaliteit van het mobiele apparaat aanzienlijk.

Nr.	Beveiligingslaag	Beschrijving van richtlijn
B3-04	Netwerk	Schakel dataroaming[24] uit als hier geen gebruik van wordt gemaakt

Doelstelling

- Misbruik van deze netwerkverbindingen tot een minimum te beperken.
- De privacygevoelige en vertrouwelijke gegevens die via deze netwerkverbindingen worden verstuurd afdoende te beschermen en het vrijgeven van deze gegevens tot een minimum te beperken.
- De mogelijkheid dat het mobiele apparaat via het netwerk (op afstand) wordt aangevallen te verlagen en zo ongeautoriseerde toegang tot het mobiele apparaat te voorkomen.
- Het mobiele apparaat, de privacygevoelige en vertrouwelijke gegevens die op het mobiele apparaat worden verwerkt afdoende te beschermen en het vrijgeven van deze gegevens tot een minimum te beperken.
- De kans op misbruik van deze gegevens te minimaliseren en de schade bij misbruik zo beperkt mogelijk te houden.

Rationale

Als dataroaming is uitgeschakeld, kunnen geen gegevens via het mobiele netwerk worden verstuurd. Apps waarvoor een internetverbinding is vereist, werken niet tenzij het mobiele apparaat via Wi-Fi toegang heeft tot het internet.

Er zijn twee belangrijke risico's verbonden aan dataroaming:

- Wat zijn de juridische consequenties bij internationaal dataroamen? Hoe wordt bijvoorbeeld de privacy beschermd in het land waar de netwerkverbinding wordt opgezet? Welke wet- en regelgeving geldt er daar met betrekking tot het afluisteren en analyseren van het netwerkverkeer?
- Als een mobiel apparaat geen netwerkverbinding meer heeft, dan wordt de gegevensbeveiliging op het mobiele apparaat bepaald door hoe het mobiele apparaat de bescherming van gegevens lokaal heeft geïmplementeerd. Het mobiele apparaat kan namelijk niet het beveiligingsbeleid van een server ophalen en het wissen op afstand werkt ook niet als er geen netwerkverbinding aanwezig is.

Het uitschakelen van dataroaming reduceert de mogelijkheid van een externe aanval op het mobiele apparaat.

Configureren

Deze functionaliteit/feature is handmatig te configureren via de gebruikersinterface van het mobiele apparaat, zie hiervoor de gebruikershandleiding van het mobiele apparaat of het betreffende besturingssysteem.

Niveau 1

iOS	Android
Ja	Ja

24. 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.

Nr.	Beveiligingslaag	Beschrijving van richtlijn
B3-05	Netwerk	Schakel Persoonlijke hotspot[25] uit als hier geen gebruik van wordt gemaakt

Doelstelling

- Misbruik van deze netwerkverbindingen tot een minimum te beperken.
- De privacygevoelige en vertrouwelijke gegevens die via deze netwerkverbindingen worden verstuurd afdoende te beschermen en het vrijgeven van deze gegevens tot een minimum te beperken.
- De mogelijkheid dat het mobiele apparaat via het netwerk (op afstand) wordt aangevallen te verlagen en zo ongeautoriseerde toegang tot het mobiele apparaat te voorkomen.
- Het mobiele apparaat, de privacygevoelige en vertrouwelijke gegevens die op het mobiele apparaat worden verwerkt afdoende te beschermen en het vrijgeven van deze gegevens tot een minimum te beperken.
- De kans op misbruik van deze gegevens te minimaliseren en de schade bij misbruik zo beperkt mogelijk te houden.

Rationale

Persoonlijke hotspot kan worden gebruikt om een internetverbinding te delen met computers of ander apparaten die via Wi-Fi, Bluetooth of USB met het mobiele apparaat zijn verbonden. Er wordt aanbevolen om Persoonlijke hotspot uit te schakelen als dit niet wordt gebruikt of als beveiliging van belang is. Het uitschakelen van Persoonlijke hotspot voorkomt dat andere apparaten verbinding maken met het internet via de mobiele netwerkverbindingen van het mobiele apparaat. Als Persoonlijke hotspot wordt uitgeschakeld worden bestaande verbindingen meteen verbroken en wordt voorkomen dat nieuwe verbindingen worden opgezet. Als netwerkverbindingen worden opgezet via Wi-Fi voor Persoonlijke hotspot wordt een wachtwoord geëist. Een wachtwoord dat is opgebouwd uit alfabetische, numerieke en niet-alfanumerieke tekens is complex en verlaagt de kans dat misbruik wordt gemaakt van Persoonlijke hotspot.

Configureren

Deze functionaliteit/feature is handmatig te configureren via de gebruikersinterface van het mobiele apparaat, zie hiervoor de gebruikershandleiding van het mobiele apparaat of het betreffende besturingssysteem.

Niveau 1

iOS	Android
Ja	Ja

25. Ook vaak aangeduid met tetheren en betekent dat de mobiele internetverbinding van het mobiele apparaat wordt gedeeld met een laptop of tablet.

Nr.	Beveiligingslaag	Beschrijving van richtlijn
B3-06	Netwerk	Schakel Wi-Fi uit als hier geen gebruik van wordt gemaakt[26]

Doelstelling

- Misbruik van deze netwerkverbindingen tot een minimum te beperken.
- De privacygevoelige en vertrouwelijke gegevens die via deze netwerkverbindingen worden verstuurd afdoende te beschermen en het vrijgeven van deze gegevens tot een minimum te beperken.
- De mogelijkheid dat het mobiele apparaat via het netwerk (op afstand) wordt aangevallen te verlagen en zo ongeautoriseerde toegang tot het mobiele apparaat te voorkomen.
- Het mobiele apparaat, de privacygevoelige en vertrouwelijke gegevens die op het mobiele apparaat worden verwerkt afdoende te beschermen en het vrijgeven van deze gegevens tot een minimum te beperken.
- De kans op misbruik van deze gegevens te minimaliseren en de schade bij misbruik zo beperkt mogelijk te houden.

Rationale

- Het wordt aanbevolen om Wi-Fi uit te schakelen als hier geen gebruik van wordt gemaakt. Als Wi-Fi is uitgeschakeld op een mobiel apparaat, zal verbinding met het internet worden gemaakt via de mobiele internetverbinding, indien beschikbaar (zie ook richtlijn B3-03). De meeste apps werken ook over de mobiele internetverbinding. Het kan wel voorkomen dat er beperkingen zijn met betrekking tot de maximale grootte van te downloaden apps (zie ook richtlijn B2-05).
- Het uitschakelen van de Wi-Fi-interface verkleint de mogelijkheid van een externe aanval op het mobiele apparaat.

Configureren

Deze functionaliteit/feature is handmatig te configureren via de gebruikersinterface van het mobiele apparaat, zie hiervoor de gebruikershandleiding van het mobiele apparaat of het betreffende besturingssysteem.

Niveau 2

iOS	Android
Ja	Ja

26. Dit is een ongebruikelijke (ongewone) instelling voor een mobiel apparaat en beperkt de functionaliteit van het mobiele apparaat aanzienlijk.

Nr.	Beveiligingslaag	Beschrijving van richtlijn
B3-07	Netwerk	Stel het mobiele apparaat zo in dat Wi-Fi-netwerken waar eerder verbinding mee is gemaakt, worden vergeten

Doelstelling

- Misbruik van deze netwerkverbindingen tot een minimum te beperken.
- De privacygevoelige en vertrouwelijke gegevens die via deze netwerkverbindingen worden verstuurd afdoende te beschermen en het vrijgeven van deze gegevens tot een minimum te beperken.
- De mogelijkheid dat het mobiele apparaat via het netwerk (op afstand) wordt aangevallen te verlagen en zo ongeautoriseerde toegang tot het mobiele apparaat te voorkomen.
- Het mobiele apparaat, de privacygevoelige en vertrouwelijke gegevens die op het mobiele apparaat worden verwerkt afdoende te beschermen en het vrijgeven van deze gegevens tot een minimum te beperken
- De kans op misbruik van deze gegevens te minimaliseren en de schade bij misbruik zo beperkt mogelijk te houden.

Rationale

Een mobiel apparaat kan worden geconfigureerd om Wi-Fi-netwerken waar eerder een verbinding mee is gemaakt niet te onthouden. Een mobiel apparaat onthoudt standaard Wi-Fi-netwerken waarmee het eerder verbinding heeft gemaakt. Het zal hiermee opnieuw automatisch verbinding maken als het Wi-Fi-netwerk binnen het bereik van het mobiele apparaat is. Het wordt aanbevolen om het mobiele apparaat zo in te stellen dat deze netwerken worden vergeten, zodat er niet automatisch een verbinding mee wordt gemaakt.

Een vertrouwd maar niet-geverifieerd Wi-Fi-netwerk kan worden vervalst. Het mobiele apparaat zal hiermee automatisch een verbinding maken op het moment dat niet is ingesteld om het netwerk te vergeten na het laatste gebruik. Bovendien, als een dergelijk Wi-Fi-netwerk een gemeenschappelijke Service Set Identifier (SSID) heeft, zal het mobiele apparaat automatisch een verbinding maken met deze niet-vertrouwde instantie van een Wi-Fi-netwerk (met dezelfde SSID).

Configureren

Deze functionaliteit/feature is handmatig te configureren via de gebruikersinterface van het mobiele apparaat, zie hiervoor de gebruikershandleiding van het mobiele apparaat of het betreffende besturingssysteem.

Niveau 1

iOS	Android
Ja	Ja

Nr.	Beveiligingslaag	Beschrijving van richtlijn
B3-08	Netwerk	Stel het mobiele apparaat zo in dat er niet wordt gevraagd om een verbinding te maken met een Wi-Fi-netwerk

Doelstelling

- Misbruik van deze netwerkverbindingen tot een minimum te beperken.
- De privacygevoelige en vertrouwelijke gegevens die via deze netwerkverbindingen worden verstuurd afdoende te beschermen en het vrijgeven van deze gegevens tot een minimum te beperken.
- De mogelijkheid dat het mobiele apparaat via het netwerk (op afstand) wordt aangevallen te verlagen en zo ongeautoriseerde toegang tot het mobiele apparaat te voorkomen.
- Het mobiele apparaat, de privacygevoelige en vertrouwelijke gegevens die op het mobiele apparaat worden verwerkt afdoende te beschermen en het vrijgeven van deze gegevens tot een minimum te beperken
- De kans op misbruik van deze gegevens te minimaliseren en de schade bij misbruik zo beperkt mogelijk te houden.

Rationale

Wanneer de gebruiker gebruikmaakt van een app die toegang nodig heeft tot het internet en de gebruiker is niet binnen het bereik van een Wi-Fi-netwerk dat door de gebruiker eerder is gebruikt (zie ook richtlijn B3-07), dan geeft de iOS-optie ‘Vraag om verbinding’ en de Android-optie ‘Netwerkmelding’ aan dat het mobiele apparaat moet zoeken naar een ander netwerk.

Op het moment dat een nieuw Wi-Fi-netwerk beschikbaar is, wordt een lijst weergegeven van alle beschikbare Wi-Fi-netwerken waaruit de gebruiker kan kiezen.

Als de iOS-optie ‘Vraag om verbinding’ en de Android-optie ‘Netwerkmelding’ is uitgeschakeld, moet de gebruiker handmatig zoeken naar een Wi-Fi-netwerk om verbinding met het internet te maken wanneer een eerder gebruikt Wi-Fi-netwerk (zie ook richtlijn B3-07) of een mobiel datanetwerk niet beschikbaar is. Het wordt aanbevolen om deze mogelijkheid uit te schakelen, zodat niet automatisch een lijst wordt weergegeven van alle beschikbare Wi-Fi-netwerken waaruit de gebruiker kan kiezen.

De eis dat een gebruiker handmatig een Wi-Fi-netwerk moet configureren en hiermee ook handmatig een verbinding maakt, vermindert de kans op het onbedoeld maken van een verbinding met een gelijknamig maar niet-vertrouwd Wi-Fi-netwerk (zie ook richtlijn B3-09).

Configureren

Deze functionaliteit/feature is handmatig te configureren via de gebruikersinterface van het mobiele apparaat, zie hiervoor de gebruikershandleiding van het mobiele apparaat of het betreffende besturingssysteem.

Niveau 1

iOS	Android
Ja	Ja

Nr.	Beveiligingslaag	Beschrijving van richtlijn
B3-09	Netwerk	Stel het mobiele apparaat zo in dat er niet automatisch met een Wi-Fi-netwerk wordt verbonden

Doelstelling

- Misbruik van deze netwerkverbindingen tot een minimum te beperken.
- De privacygevoelige en vertrouwelijke gegevens die via deze netwerkverbindingen worden verstuurd afdoende te beschermen en het vrijgeven van deze gegevens tot een minimum te beperken.
- De mogelijkheid dat het mobiele apparaat via het netwerk (op afstand) wordt aangevallen te verlagen en zo ongeautoriseerde toegang tot het mobiele apparaat te voorkomen.
- Het mobiele apparaat, de privacygevoelige en vertrouwelijke gegevens die op het mobiele apparaat worden verwerkt afdoende te beschermen en het vrijgeven van deze gegevens tot een minimum te beperken
- De kans op misbruik van deze gegevens te minimaliseren en de schade bij misbruik zo beperkt mogelijk te houden.

Rationale

Wanneer verbindt automatisch is ingeschakeld voor een Wi-Fi-netwerk, onthoudt het mobiele apparaat de netwerk- en logingegevens. Het zal dan automatisch opnieuw een verbinding maken met dat Wi-Fi-netwerk wanneer het mobiele apparaat binnen bereik is.
Opmerking: Niet elk abonnement voor Wi-Fi-hotspots ondersteunt de mogelijkheid van automatisch verbinden. Sommige abonnementen maar verlangen dat iedere keer handmatig wordt ingelogd, zoals bijvoorbeeld Wi-Fi-hotspots in hotels.

Er is een aantal mogelijke risico's bij het gebruik van deze functie. Voor Wi-Fi-netwerken die HTTP(S)-formulieren gebruiken voor authenticatie, zorgt deze functie ervoor dat de referenties op het mobiele apparaat bewaard blijven (zie ook richtlijn B1-09). Bij verlies of diefstal van het mobiele apparaat komt de vertrouwelijkheid van deze bewaarde referenties in gevaar - en de bronnen die hierdoor worden beveiligd. Het gevaar wordt veroorzaakt door het feit dat een kwaadwillende de inhoud van het mobiele apparaat weet te achterhalen, inclusief de referenties.
Opmerking: Als de gegevens die bij de formuliergebaseerde authenticatie worden gebruikt over een niet-versleutelde HTTP-verbinding worden verstuurd, bestaat het risico dat de referentie wordt onderschept tijdens transport. Hoewel dit ook geldt als er geen gebruik wordt gemaakt van de 'verbind automatisch' functionaliteit, zorgt het inschakelen van deze functionaliteit voor een verhoogd risico.

Configureren

Deze functionaliteit/feature is handmatig te configureren via de gebruikersinterface van het mobiele apparaat, zie hiervoor de gebruikershandleiding van het mobiele apparaat of het betreffende besturingssysteem.

Niveau 1	
iOS	**Android**
Ja	Ja

Nr.	Beveiligingslaag	Beschrijving van richtlijn
B3-10	Netwerk	Maak zoveel mogelijk gebruik van een VPN-verbinding

Doelstelling

Misbruik van deze netwerkverbindingen tot een minimum te beperken door de privacygevoelige en vertrouwelijke gegevens die via deze netwerkverbindingen worden verstuurd afdoende te beschermen en het vrijgeven van deze gegevens tot een minimum te beperken en hierdoor de kans op misbruik van deze gegevens te minimaliseren en de schade bij misbruik zo beperkt mogelijk te houden.

Rationale

Virtual Private Network (VPN) zorgt voor een beveiligde 'tunnel' van het mobiele apparaat naar een server die wordt vertrouwd. Al het dataverkeer wordt dan versleuteld over deze VPN-verbinding. Een kwaadwillende die het netwerkverkeer op het openbare netwerk afluistert, zal dan enkel versleutelde gegevens zien.

VPN-verbindingen kunnen worden opgezet over zowel Wi-Fi-netwerken als mobiele datanetwerken. Het wordt aanbevolen zoveel mogelijk gebruik te maken van VPN-verbindingen om de vertrouwelijkheid van de gegevens tijdens transport te waarborgen.

Configureren

Deze functionaliteit/feature is handmatig te configureren via de gebruikersinterface van het mobiele apparaat, zie hiervoor de gebruikershandleiding van het mobiele apparaat of het betreffende besturingssysteem.

Niveau 1	
iOS	**Android**
Ja	Ja

Nr.	Beveiligingslaag	Beschrijving van richtlijn
B3-11	Netwerk	Schakel Bluetooth uit als hier geen gebruik van wordt gemaakt.

Doelstelling

- Misbruik van deze netwerkverbindingen tot een minimum te beperken.
- De privacygevoelige en vertrouwelijke gegevens die via deze netwerkverbindingen worden verstuurd afdoende te beschermen en het vrijgeven van deze gegevens tot een minimum te beperken.
- De mogelijkheid dat het mobiele apparaat via het netwerk (op afstand) wordt aangevallen te verlagen en zo ongeautoriseerde toegang tot het mobiele apparaat te voorkomen.
- Het mobiele apparaat, de privacygevoelige en vertrouwelijke gegevens die op het mobiele apparaat worden verwerkt afdoende te beschermen en het vrijgeven van deze gegevens tot een minimum te beperken
- De kans op misbruik van deze gegevens te minimaliseren en schade bij misbruik zo beperkt mogelijk te houden.

Rationale

Het wordt aanbevolen om Bluetooth uit te schakelen wanneer het niet wordt gebruikt, om te voorkomen dat wordt achterhaald welke Bluetooth-diensten worden ondersteund door het mobiele apparaat. Tevens zorgt het uitschakelen van Bluetooth ervoor dat er geen verbinding wordt opgezet met de Bluetooth-diensten die worden ondersteund.

Configureren

Deze functionaliteit/feature is handmatig te configureren via de gebruikersinterface van het mobiele apparaat, zie hiervoor de gebruikershandleiding van het mobiele apparaat of het betreffende besturingssysteem.

Niveau 1	
iOS	**Android**
Ja	Ja

Nr.	Beveiligingslaag	Beschrijving van richtlijn
B3-12	Netwerk	Schakel Near Field Communication (NFC) uit als hier geen gebruik van wordt gemaakt

Doelstelling

- Misbruik van deze netwerkverbindingen tot een minimum te beperken.
- De privacygevoelige en vertrouwelijke gegevens die via deze netwerkverbindingen worden verstuurd afdoende te beschermen en het vrijgeven van deze gegevens tot een minimum te beperken.
- De mogelijkheid dat het mobiele apparaat via het netwerk (op afstand) wordt aangevallen te verlagen en zo ongeautoriseerde toegang tot het mobiele apparaat te voorkomen.
- Het mobiele apparaat, de privacygevoelige en vertrouwelijke gegevens die op het mobiele apparaat worden verwerkt afdoende te beschermen en het vrijgeven van deze gegevens tot een minimum te beperken
- De kans op misbruik van deze gegevens te minimaliseren en de schade bij misbruik zo beperkt mogelijk te houden.

Rationale

Near Field Communication (NFC)[27] is een technologie waarmee een kleine hoeveelheid informatie kan worden opgeslagen op stickers[28] of andere kleine apparaten, die op korte afstand door een NFC-lezer kunnen worden gescand. NFC-tags kunnen URL's, foto's, Google Maps-locaties, contacten en veel andere soorten informatie bevatten.
Als het mobiele apparaat over de functionaliteit beschikt om NFC-tags te scannen, kan de Android toepassing Tags gebruikt worden om gescande tags te openen, ermee te werken en deze te ordenen.

Ook bestaat de mogelijkheid om met mobiele apparaten die NFC ondersteunen mobiel te betalen.

Aanvallen zouden er voor kunnen zorgen dat kwaadwillenden een mobiel apparaat naar een website met malware sturen zonder dat de gebruiker dit merkt. Zo kan een kwaadwillende bijvoorbeeld een NFC-tag veranderen die vervolgens nietsvermoedend gescand wordt door een gebruiker. Doordat men op voorhand niet kan zien wat er gescand wordt, is het kwaad vaak al geschied voordat de gebruiker hier erg in heeft.
(Dit scenario geldt overigens ook voor QR-codes)

Kanttekeningen:
- NFC werkt over het algemeen niet als het scherm niet ingeschakeld is en als het mobiele apparaat is vergrendeld.
- Kwaadwillenden dienen erg dicht (ongeveer 10 cm) in de buurt te komen van het mobiele apparaat.

Configureren

Deze functionaliteit/feature is handmatig te configureren via de gebruikersinterface van het mobiele apparaat, zie hiervoor de gebruikershandleiding van het mobiele apparaat of het betreffende besturingssysteem.

Niveau 1

iOS	Android
NFC wordt niet ondersteund door enig mobiel apparaat met iOS	Ja

27. Meer informatie over Near Field Communication (NFC) is te vinden in het eindrapport NFC van SURFnet en Kennisnet.nl: http://innovatie.kennisnet.nl/wp-content/uploads/2012/04/Eindrapport_NFC.pdf.
28. Near Field Communication (NFC) is een technologie voor draadloze communicatie die gebaseerd is op de Radio Frequency Identification (RFID)-standaard voor contactloze smartcards.

Nr.	Beveiligingslaag	Beschrijving van richtlijn
B3-13	Netwerk	Schakel vliegtuigmodus in[29, 30, 31] als geen draadloze netwerkverbindingen en voorzieningen nodig zijn

Doelstelling

Het beschermen van het mobiele apparaat en de gegevens die erop zijn opgeslagen, doordat de kans wordt verkleind dat het mobiele apparaat via het netwerk (op afstand) wordt aangevallen.

Rationale

Met vliegtuigmodus kunnen alle draadloze voorzieningen van het mobiele apparaat worden uitgeschakeld.

Opmerking: Als een mobiel apparaat geen netwerkverbinding meer heeft, dan wordt de gegevensbeveiliging op het mobiele apparaat bepaald door hoe het mobiele apparaat de bescherming van gegevens lokaal heeft geïmplementeerd. Het mobiele apparaat kan namelijk niet het beveiligingsbeleid van een server ophalen en het wissen op afstand werkt ook niet als er geen netwerkverbinding aanwezig is.

Het uitschakelen van alle netwerkverbindingen verkleint de mogelijkheid van een externe aanval op het mobiele apparaat.

Opmerking: Op het moment dat speciale zones zijn ingericht omdat zeer strenge veiligheidseisen worden gesteld aan de vertrouwelijkheid van gegevens, kunnen de volgende beleidsmaatregelen worden vastgesteld voor mobiele apparaten in deze speciale zones[32]:
- Laat mobiele apparaten buiten deze vertrouwelijke zones.
- Apps die audio- of video-opnames kunnen maken moet worden verwijderd of het gebruik ervan moet beperkt worden.
- Zorg dat de camera's van het mobiele apparaat zijn geblokkeerd (bijvoorbeeld door deze af te plakken met ondoorzichtige tape) om het maken van foto's of video's te voorkomen.
- Zorg dat op alle mobiele apparaten, indien toch meegenomen, vliegtuigmodus is ingeschakeld en de draadloze verbindingen Wi-Fi en Bluetooth blijven uitgeschakeld.

Configureren

Deze functionaliteit/feature is handmatig te configureren via de gebruikersinterface van het mobiele apparaat, zie hiervoor de gebruikershandleiding van het mobiele apparaat of het betreffende besturingssysteem.

Niveau 2

iOS	Android
NFC wordt niet ondersteund door enig mobiel apparaat met iOS	Ja

29. 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.
30. Dit is een ongebruikelijke (ongewone) instelling voor een mobiel apparaat en beperkt de functionaliteit van het mobiele apparaat aanzienlijk.
31. In vliegtuigmodus kunnen Wi-Fi en Bluetooth opnieuw worden ingeschakeld: http://support.apple.com/kb/ht1355?viewlocale=nl_NL.
32. Dit geldt voor zowel medewerkers als bezoekers.

BIJLAGE A » AFKORTINGEN

BYOD	Bring Your Own Device
CoIT	Consumerization of IT
GPS	Global Positioning System
GSM	Global System for Mobile Communications, officieel Groupe Spécial Mobile
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
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
QR-code	Quick Response Code
SIM	Subscriber Identity Module
SMS	Short Message Service
SSID	Service Set Identifier
SSL	Secure Sockets Layer
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

[8] 'iPhone Gebruikershandleiding Voor iOS 5.1-software' http://manuals.info.apple.com/nl_NL/iphone_gebruikershandleiding.pdf

[9] 'iPad Gebruikershandleiding Voor iOS 5.1-software' http://manuals.info.apple.com/nl_NL/ipad_gebruikershandleiding.pdf

[10] 'Exchange ActiveSync en iOS-apparaten' http://help.apple.com/iosdeployment-exchange/?lang=nl

[11] 'Apple-beveiligingsupdates' http://support.apple.com/kb/HT1222?viewlocale=nl_NL

[12] 'Implementatiehandleiding voor bedrijven - Tweede editie, voor versie 3.2 of hoger' http://manuals.info.apple.com/nl_NL/Implementatiehandleiding_voor_bedrijven.pdf

[13] 'Deploying iPhone and iPad - Security Introduction', d.d maart 2012. http://images.apple.com/ipad/business/docs/iOS_Security_Introduction_Mar12.pdf '

[14] 'iOS Security', d.d. mei 2012. http://images.apple.com/ipad/business/docs/iOS_Security_May12.pdf

[15] 'iPhone and iPad in Business Deployment Scenarios', d.d. maart 2012. http://images.apple.com/ipad/business/docs/iOS_Business_Mar12.pdf

[16] 'Deploying iPhone and iPad Exchange ActiveSync', d.d. maart 2012. http://images.apple.com/ipad/business/docs/iOS_EAS_Mar12.pdf

[17] 'Deploying iPhone and iPad Standards-Based Services', d.d. maart 2012. http://images.apple.com/ipad/business/docs/iOS_IMAP_Mar12.pdf

[18] 'Deploying iPhone and iPad Virtual Private Networks', d.d. maart 2012. http://images.apple.com/ipad/business/docs/iOS_VPN_Mar12.pdf

[19] 'Deploying iPhone and iPad Wi-Fi', d.d. maart 2012. http://images.apple.com/ipad/business/docs/iOS_WiFi_Mar12.pdf

[20] ‘Deploying iPhone and iPad Digital Certificates’, d.d. maart 2012.
http://images.apple.com/ipad/business/docs/iOS_Certificates_Mar12.pdf

[21] ‘Deploying iPhone and iPad Mobile Device Management’, d.d. maart 2012.
http://images.apple.com/ipad/business/docs/iOS_MDM_Mar12.pdf en
http://www.apple.com/ipad/business/integration/mdm/

[22] ‘Deploying iPhone and iPad Apple Configurator’, d.d. maart 2012.
http://images.apple.com/ipad/business/docs/iOS_Apple_Configurator_Mar12.pdf en
http://itunes.apple.com/us/app/apple-configurator/id434433123?mt=12&ls=1

[23] ‘Managing Exchange ActiveSync with Policies’
http://technet.microsoft.com/nl-nl/library/aa998614
- ‘View or Configure Exchange ActiveSync Mailbox Policy Properties’
  http://technet.microsoft.com/nl-nl/library/bb123994
- ‘Perform a Remote Wipe on a Mobile Phone’
  http://technet.microsoft.com/nl-nl/library/aa998614

[24] ‘Een nieuwe apparaatbeleidsregel van ActiveSync maken’
http://technet.microsoft.com/nl-nl/exchangelabshelp/ms.exch.ecp.newactivesyncmailboxpolicy

[25] ‘Android 4.0.4 Support on Galaxy Nexus, Nexus S, and Motorola Xoom for Microsoft Exchange Policies’
http://static.googleusercontent.com/external_content/untrusted_dlcp/www.google.com/en/us/help/hc/pdfs/mobile/ExchangeAndAndroid4.0.4.pdf

[26] ‘Microsoft Exchange Information Services and Security Policies Supported by Android 2.2 and 2.3’
http://static.googleusercontent.com/external_content/untrusted_dlcp/www.google.com/en//help/hc/pdfs/mobile/ExchangeAndAndroid2.2and2.3-003.pdf

[27] ‘Microsoft Exchange Information Services and Security Policies Supported by Android 2.2’
http://static.googleusercontent.com/external_content/untrusted_dlcp/www.google.com/en/us/help/hc/pdfs/mobile/ExchangeAndAndroid2.2-002.pdf

BIJLAGE C » IPHONE-CONFIGURATIE-PROGRAMMA

In deze bijlage wordt beschreven hoe configuratieprofielen kunnen worden gemaakt met behulp van het iPhone-configuratieprogramma. Configuratieprofielen bepalen hoe iOS-apparaten samenwerken met uw bedrijfs-systemen.

Met het iPhone-configuratieprogramma kunt u configuratieprofielen aanmaken, coderen en installeren, voorzieningenprofielen en bevoegde apps volgen en installeren en apparaatgegevens (zoals console-logbestanden) vastleggen.

Hieronder staan de instellingen die kunnen worden geconfigureerd met het iPhone-configuratieprogramma en die relevant zijn voor deze richtlijn (identiteits- en toegangsbeheer, applicaties, iCloud en beveiliging en privacy) en er wordt tevens aangegeven wat de default-waarde is.

Toegangscontrole		
Instelling	**Omschrijving**	**Default**
Wachtwoord vereisen Toegangscode	Schakel dit selectievakje in om te vereisen dat mobiele apparaten worden vergrendeld met een toegangscode. De andere toegangscodeopties zijn niet beschikbaar, tenzij u dit selectievakje inschakelt.	Ja
Eenvoudige waarde toestaan	Staat toe dat gebruikers een toegangscode kiezen waarin gebruik wordt gemaakt van een opeenvolgende reeks tekens of waarin tekens worden herhaald. (Een eenvoudige toegangscode is bijvoorbeeld ‘3333’ of ‘DEFG’.) Als u dit selectievakje uitschakelt, zullen gebruikers worden verplicht een veiliger wachtwoord te gebruiken.	Nee
Alfanumerieke waarde vereist	Toegangscodes moeten minimaal één letter of cijfer bevatten. De eis van niet-numerieke tekens in toegangscodes verhoogt de kracht van toegangscode-beveiliging.	Ja
Minimale lengte toe-gangscode	Het minimale aantal tekens waaruit de toegangscode moet bestaan. Lange toegangscodes verhogen de beveiliging van het mobiele apparaat. Echter, lange toegangscodes kunnen de gebruiksvriendelijkheid van het mobiele apparaat verlagen.	6
Minimale aantal complexe tekens	Het kleinste aantal niet-alfanumerieke tekens (zoals $, & en !) die de toegangs-code moet bevatten. Selecteer een waarde van 1 t/m 3.	1
Maximale gebruiks-duur toegangscode	Het aantal dagen waarna gebruikers hun toegangscode moeten wijzigen	120
Geschiedenis toegangscodes	Nieuwe toegangscodes worden niet geaccepteerd als deze gelijk zijn aan eerder gebruikte toegangscodes. U kunt opgeven hoeveel eerdere toegangscodes vergeleken en bewaard moeten blijven. U kunt een waarde opgeven tussen 0 en 50. Geef 0 op als u wilt dat gebruikers hun toegangscodes onmiddellijk kunnen herhalen.	3

Vervolg toegangscontrole		
Instelling	**Omschrijving**	**Default**
Maximale automatische vergrendeling	Als het mobiele apparaat gedurende het opgegeven aantal minuten niet wordt gebruikt, wordt het automatisch vergrendeld. Het mobiele apparaat kan worden ontgrendeld door de toegangscode op te geven. Deze instelling bepaalt de maximumwaarde die de gebruiker mag configureren. Deze optie wordt alleen afgedwongen als een toegangscode is vereist. U kunt een aantal minuten van 1 tot 60 opgeven.	5 of minder
Geldigheid toegangscode bij vergrendeling	Hiermee wordt aangegeven hoe snel het mobiele apparaat na gebruik weer kan worden ontgrendeld, zonder dat hierbij opnieuw om de toegangscode wordt gevraagd. Deze instelling bepaalt de maximumwaarde die de gebruiker mag configureren. Wanneer u als instelling 'Geen' kiest, mag de gebruiker alle beschikbare intervallen kiezen. Wanneer u als instelling 'Onmiddellijk' kiest, moet er altijd een toegangscode worden ingevoerd wanneer het mobiele apparaat wordt ontgrendeld	5 of minder
Maximale aantal mislukte pogingen	Hiermee wordt bepaald hoeveel pogingen mogen worden gedaan om de juiste toegangscode in te voeren voordat het mobiele apparaat wordt gewist. Na zes mislukte pogingen treedt een vertraging op, zodat het even duurt voordat de toegangscode opnieuw kan worden ingevoerd. De vertraging wordt na iedere mislukte poging langer. Na de laatste mislukte poging worden alle gegevens en instellingen veilig van het apparaat gewist. De vertraging wordt na de zesde poging gestart, dus als u hier een waarde van 6 of lager opgeeft, vindt geen vertraging plaats en wordt het apparaat direct gewist zodra het opgegeven maximum wordt overschreden.	10 of minder
Gebruiker mag niet-vertrouwde TLS-certificaten accepteren	Als dit aankruisvak is uitgeschakeld, wordt gebruikers niet gevraagd of ze certificaten die niet kunnen worden gecontroleerd, willen vertrouwen. Deze instelling geldt voor Safari en voor Mail-, Contacten- en Agenda-accounts.	Nee
Diagnostische gegevens mogen naar Apple worden verstuurd	Als dit aankruisvak is uitgeschakeld, worden geen diagnostische iOS-gegevens naar Apple verstuurd.	Nee
Uitschrijven (opt out) op interesse gebaseerde advertenties van het iAd-advertentienetwerk	iAd, het Apple-platform voor mobiele advertenties, streeft ernaar relevante advertenties op basis van uw interesses te versturen. Opmerking voor als u zich uitschrijft: • U ziet mogelijk evenveel advertenties als voordien, maar die zijn mogelijk minder interessant omdat die niet op uw interesse gebaseerd zijn. • U ziet mogelijk advertenties die zijn gerelateerd aan de inhoud van een programma of gebaseerd op andere onpersoonlijke informatie. • U schrijft zich alleen uit van Apple-advertenties en niet van andere advertentienetwerken. Oplossing: http://support.apple.com/kb/HT4228?viewlocale=nl_NL	

Applicatie		
Instelling	**Omschrijving**	**Default**
Gebruik van YouTube toestaan	Als dit aankruisvak is uitgeschakeld, wordt YouTube uitgeschakeld en wordt het appsymbool uit het beginscherm verwijderd. (De YouTube-app wordt meegeleverd met iOS 5 en eerdere versies.)	Nee
Gebruik van iTunes Store toestaan	Als dit aankruisvak is uitgeschakeld, wordt de iTunes Store uitgeschakeld en wordt het appsymbool uit het beginscherm verwijderd. Gebruikers kunnen materiaal niet vooraf bekijken of beluisteren en geen materiaal aanschaffen of downloaden.	Nee
Gebruik van Safari toestaan	Als dit aankruisvak is uitgeschakeld, wordt Safari uitgeschakeld en wordt het appsymbool uit het beginscherm verwijderd. Met deze optie kunt u ook voorkomen dat gebruikers webfragmenten kunnen openen. Let op: Dit selectievakje heeft geen controle over de toegang tot browsers van derden die op het mobiele apparaat zijn geïnstalleerd.	Nee
JavaScript activeren	Als dit aankruisvak is uitgeschakeld, wordt alle JavaScript-code op websites door Safari genegeerd.	Nee
Fraudewaarschuwacti viteit forceren	Als dit aankruisvak is uitgeschakeld, verschijnt in Safari geen waarschuwing wanneer een gebruiker potentieel frauduleuze of verdachte websites bezoekt.	Ja
Automatisch vullen activeren	Als dit aankruisvak is uitgeschakeld, onthoudt Safari niet wat gebruikers invullen in webformulieren.	Nee
Cookies accepteren	U kunt instellen dat alle of geen cookies worden geaccepteerd, of dat alleen cookies van direct bezochte websites worden geaccepteerd.	Nee
Pop-ups blokkeren	Als dit aankruisvak is uitgeschakeld, worden in Safari geen pop-ups geblokkeerd.	Nee

Onlinegegevensopslag (Cloud)		
Instelling	**Omschrijving**	**Default**
Reservekopieën toestaan	Wanneer dit aankruisvak is ingeschakeld, kunnen gebruikers een reservekopie van hun apparaat in iCloud bewaren.	
Document-synchronisatie toestaan	Wanneer dit aankruisvak is ingeschakeld, kunnen gebruikers documenten bewaren in iCloud.	
Fotostream toestaan	Wanneer dit aankruisvak is uitgeschakeld, kunnen gebruikers Fotostream niet inschakelen. Wanneer een configuratieprofiel met deze beperking wordt geïnstalleerd, worden Fotostream-foto's van het apparaat van de gebruiker gewist en kunnen er geen foto's van de Filmrol worden verstuurd naar Fotostream. Als er geen andere kopieën van deze foto's zijn, kunnen deze foto's verloren gaan.	
Gedeelde Fotostreams toestaan	Wanneer deze optie is ingeschakeld, kunnen gebruikers anderen uitnodigen om hun Fotostreams te bekijken en kunnen gebruikers Fotostreams bekijken die door anderen worden gedeeld.	

BIJLAGE D » EXCHANGE ACTIVESYNC

Configureren van Exchange ActiveSync Mailbox beleidseigenschappen
Met de apparaatbeleidsregels van Exchange ActiveSync (EAS) bepaalt u hoe gebruikers hun mobiele apparaten gebruiken en synchroniseren met EAS in uw organisatie. Wanneer u een apparaatbeleidsregel van EAS wijzigt, heeft dit betrekking op alle gebruikers waarvan het postvak is gekoppeld aan het desbetreffende beleid. Het beleid dat u als standaard instelt, beïnvloedt automatisch alle gebruikers in de organisatie met uitzondering van de gebruikers waaraan u expliciet andere apparaatbeleidsregels hebt toegewezen.

Het configureren van de EAS Mailbox-beleidseigenschappen kan zowel via de 'Exchange Management Console' (EMC) als de 'Exchange Management Shell'. Als u een Exchange ActiveSync Mailbox-beleid via de EMC creëert, kunt u slechts een deel van de beschikbare eigenschappen configureren. De rest van de eigenschappen kunt u met behulp van de Exchange Management Shell configureren. Zie de specifieke documentatie van Microsoft voor hoe de EAS Mailbox-beleidseigenschappen kunnen worden beheerd.[33, 34]

Opmerking: Niet alle mobiele apparaten ondersteunen alle EAS-beleidseigenschappen. Als een EAS-beleidsinstelling niet wordt ondersteund op een bepaald mobiel apparaat, is het mogelijk dat het mobiele apparaat de instelling niet toepast[35]. Bij de algemene instellingen voor het EAS-beleid kunt u bepalen of apparaten die bepaalde beleidsregels niet ondersteunen, verbinding mogen maken.

Algemene Exchange ActiveSync Mailbox-beleidseigenschappen
Met deze instellingen bepaalt u welke mobiele apparaten kunnen synchroniseren, en hoe vaak het beleid wordt vernieuwd op mobiele apparaten.

Algemene Exchange ActiveSync Mailbox-beleidseigenschappen		
ActiveSync-instelling	**Omschrijving**	**Default**
Naam	Geef een naam op die een unieke aanduiding vormt voor dit beleid.	
Dit is het standaardbeleid	Schakel dit selectievakje in als u dit beleid het standaardbeleid wilt maken voor uw organisatie. Het standaardbeleid heeft betrekking op alle gebruikers waaraan niet expliciet een ander beleid is toegewezen.	
Mobiele apparaten toestaan die de beleidsregels niet volledig ondersteunen	Schakel dit selectievakje in om mobiele apparaten toe te staan om te synchroniseren hoewel deze geen ondersteuning bieden voor het afdwingen van het beleid of die niet alle instellingen ondersteunen die zijn opgegeven in dit beleid. Als u dit selectievakje niet inschakelt, krijgen deze mobiele apparaten een foutbericht '403 Toegang geweigerd' wanneer zij proberen te synchroniseren met Microsoft Exchange.	Ja
Beleidsregels vernieuwingsinterval	Als u wilt dat beleidsregels op apparaten regelmatig worden vernieuwd, schakelt u dit selectievakje in en geeft u op hoe vaak ActiveSync de beleidsregels op mobiele apparaten moet vernieuwen. Beleidsregels worden pas vernieuwd als dit selectievakje is ingeschakeld. Als u geen tijdsinterval opgeeft, worden beleidsregels elke 24 uur vernieuwd.	Onbeperkt

33. http://technet.microsoft.com/nl-nl/exchangelabshelp/ms.exch.ecp.newactivesyncmailboxpolicy
34. http://technet.microsoft.com/nl-nl/library/bb123994 (Van toepassing op Exchange Server 2010 SP2)
35. http://technet.microsoft.com/en-us/library/bb232129 (Van toepassing op Exchange Server 2010 SP2)

Wachtwoorden
Met deze instellingen bepaalt u de wachtwoordeisen voor Exchange ActiveSync-clients.

Wachtwoorden		
ActiveSync-instelling	**Omschrijving**	**Default**
Wachtwoord vereisen	Schakel dit selectievakje in om te vereisen dat mobiele apparaten worden vergrendeld met een wachtwoord. De andere wachtwoordopties zijn niet beschikbaar, tenzij u dit selectievakje inschakelt.	Nee
Alfanumeriek wachtwoord vereisen	Schakel dit selectievakje in om te vereisen dat wachtwoorden van mobiele apparaten zowel getallen als letters bevatten. De eis van niet-numerieke tekens in wachtwoorden verhoogt de kracht van wachtwoordbeveiliging.[36]	Nee
De toegangscode moet minimaal dit aantal (complexe) tekensets bevatten	U kunt vereisen dat wachtwoorden tekens uit meerdere tekensets bevatten om de beveiliging van mobiele apparaatwachtwoorden te verbeteren Selecteer een waarde van 1 t/m 3. De tekensets bevatten letters, hoofdletters, cijfers en symbolen. Als u bijvoorbeeld 3 selecteert, moeten wachtwoorden tekens bevatten uit drie tekensets.	0
Wachtwoordherstel	Schakel dit selectievakje in om op te geven of gebruikers het wachtwoord van hun mobiele apparaat kunnen herstellen. Gebruikers kunnen gebruikmaken van Outlook Web App voor het opzoeken van hun herstelwachtwoord en om hun mobiele apparaat ontgrendelen. Beheerders kunnen de EMC gebruiken voor het opzoeken van een gebruikerherstelwachtwoord.	Nee
Versleuteling vereisen voor apparaat	Schakel dit selectievakje in om te vereisen dat mobiele apparaten versleuteling gebruiken. Dit verhoogt de beveiliging door het versleutelen van alle informatie op het mobiele apparaat.	Nee
Versleuteling vereisen voor opslagkaarten	Schakel dit selectievakje in om te vereisen dat mobiele apparaten verwijderbare opslagmedia versleutelen. Dit verhoogt de beveiliging door het versleutelen van alle gegevens op de verwijderbare opslagmedia voor het mobiele apparaat.	Nee
Eenvoudige wachtwoorden toestaan	Schakel dit selectievakje in om gebruikers toe te staan dat deze een eenvoudig wachtwoord gebruiken, zoals 1234 of 1111, om hun mobiele apparaat te vergrendelen. Als u dit selectievakje uitschakelt, zullen gebruikers worden verplicht om een veiliger wachtwoord te gebruiken.	Nee
Maximaal aantal toegestaan mislukte aanmeldpogingen	Schakel dit selectievakje in en geef het aantal pogingen op dat een gebruiker zonder succes mag ondernemen om zich aan te melden voordat alle informatie op het mobiele apparaat wordt verwijderd en het mobiele apparaat automatisch wordt teruggebracht naar de oorspronkelijke fabrieksinstellingen. Dit vermindert de kans dat niet-geautoriseerde gebruikers toegang krijgen tot informatie op een verloren of gestolen mobiel apparaat dat is beveiligd met een wachtwoord.	4

36. Lees meer informatie over het gebruik van sterke wachtwoorden op waarschuwingsdienst.nl: http://www.waarschuwingsdienst.nl/Computer+beveiligen/Wachtwoorden/Moelijke+wachtwoorden+op+een+makkelijke+manier.html

Vervolg wachtwoorden		
ActiveSync-instelling	**Omschrijving**	**Default**
Minimale wachtwoord-lengte	Schakel dit selectievakje in en geef de minimale wachtwoordlengte op waaraan de toegangscode voor het mobiele apparaat moet voldoen. Lange wachtwoorden verhogen de beveiliging van het mobiele apparaat. Lange wachtwoorden kunnen echter de gebruiksvriendelijkheid van het mobiele apparaat verlagen.	4
Maximale tijd zonder invoer van de gebruiker voordat de toegangs-code opnieuw moet worden ingevoerd (in minuten)	Schakel dit selectievakje in en geef het aantal minuten op voordat het mobiele apparaat na inactief te zijn geweest wordt vergrendeld en er wordt vereist dat de gebruiker zich opnieuw moet aanmelden. Deze optie wordt alleen afgedwongen als een wachtwoord is vereist. U kunt een aantal minuten van 1 tot 60 opgeven.	15
Wachtwoord expiratie (in dagen)	Schakel dit selectievakje in en geef het aantal dagen op dat een wachtwoord geldig is, waarna gebruikers het wachtwoord van hun mobiele apparaat moeten wijzigen.	Onbeperkt
Wachtwoord-geschiedenis	Geef het aantal recentst gebruikte wachtwoorden op dat gebruikers niet mogen gebruiken als nieuw wachtwoord op hun mobiele apparaat. U kunt een waarde opgeven tussen 0 en 50. Geef 0 op als u wilt dat gebruikers hun wachtwoorden onmiddellijk kunnen herhalen.	0

Synchronisatie-instellingen
Deze instellingen bepalen wat gebruikers kunnen synchroniseren naar hun mobiele apparaten en of zij kunnen synchroniseren tijdens het dataroamen.[37]

Synchronisatie-instellingen		
ActiveSync-instelling	**Omschrijving**	**Default**
Maximale leeftijdsfilter agendaitems	Selecteer, via de dropdownlijst, van hoe lang geleden oude agendaitems moeten worden gesynchroniseerd met het mobiele apparaat. De beschikbare opties zijn: Alle, twee weken, een maand, drie maanden en zes maanden. Als u andere opties wilt opgeven, dient u gebruik te maken van de Shell om deze instelling te configureren.	7
Maximale leeftijdsfilter e-mailberichten	Selecteer, via de dropdownlijst, van hoe lang geleden oude e-mailberichten moeten worden gesynchroniseerd met het mobiele apparaat. De beschikbare opties zijn: Alle, een dag, drie dagen, een week, twee weken en een maand. Als u andere opties wilt opgeven, dient u gebruik te maken van de Shell om deze instelling te configureren.	3
Maximale grootte e-mailbericht (KB)	Schakel dit selectievakje in om de maximale grootte van het e-mailbericht, in kilobytes (KB) op te geven dat kan worden gedownload naar het mobiele apparaat. E-mailberichten die groter zijn dan deze waarde worden wel afgeleverd, maar afgekapt tot de maximale grootte.	3
Handmatige synchronisatie bij roamen vereisen	Schakel dit selectievakje in om het mobiele apparaat te synchroniseren, via Direct Push, als nieuwe items arriveren tijdens het roamen. Als dit selectievakje niet is ingeschakeld wordt de gebruiker gedwongen om de synchronisatie handmatig te starten.	Nee
E-mail met HTML-opmaak toestaan	Schakel dit selectievakje in zodat e-mailberichten die zijn opgemaakt in HTML worden gesynchroniseerd met het mobiele apparaat. Als dit selectievakje niet is ingeschakeld worden alle e-mailberichten geconverteerd naar platte tekst voordat deze worden gesynchroniseerd. Het gebruik van dit selectievakje heeft geen invloed op het al dan niet ontvangen van de berichten op het mobiele apparaat.	Ja
Downloaden van bijlagen naar mobiele apparaat toestaan	Schakel dit selectievakje in zodat bijlagen worden gedownload naar het mobiele apparaat. Als dit selectievakje niet is ingeschakeld, is de naam van de bijlage zichtbaar in het e-mailbericht maar kunnen gebruikers de bijlage niet downloaden naar hun mobiele apparaat.	Ja
Maximale grootte van bijlagen (KB)	Schakel dit selectievakje in en geef de maximale grootte van bijlagen, in kilobytes (KB), op die worden gedownload naar het mobiele apparaat. Als dit selectievakje is ingeschakeld, kunnen bijlagen die groter zijn dan de opgegeven waarde niet worden gedownload naar het apparaat.	Onbeperkt

37. 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.

Apparaatinstellingen
Deze instellingen bepalen welke functies gebruikers op hun mobiele apparaat kunnen gebruiken.

Opmerking: Om deze instellingen op het mobiele apparaat te kunnen implementeren, moet u over een Exchange Enterprise Clienttoeganglicentie (Client Access License) beschikken voor ieder postvak waarop dit beleid van toepassing is.

Apparaatinstellingen		
ActiveSync-instelling	**Omschrijving**	**Default**
Tekstberichten (SMS) toestaan	Schakel dit selectievakje in waardoor het is toegestaan om tekstberichten (SMS) te versturen vanaf het mobiele apparaat.	Ja
Verwisselbare opslag toestaan	Schakel dit selectievakje in waardoor het is toegestaan dat geheugen-/opslagkaarten kunnen worden benaderd via het mobiele apparaat.	Ja
Camera toestaan	Schakel dit selectievakje in waardoor het is toegestaan dat de camera op het mobiele apparaat kan worden gebruikt.	Ja
Wi-Fi toestaan	Schakel dit selectievakje in waardoor het is toegestaan dat het mobiele apparaat gebruik kan maken van een Wi-Fi-verbinding. Direct Push wordt niet ondersteund over een Wi-Fi-verbinding.	Ja
Infrarood (IrDa) toestaan	Schakel dit selectievakje in waardoor het is toegestaan dat het mobiele apparaat een infraroodverbinding met andere apparaten of computers kan opzetten.	Ja
Internet delen toestaan (tethering)	Schakel dit selectievakje waardoor het is toegestaan dat de internetverbinding van het mobiele apparaat wordt gedeeld met een ander apparaat. Het delen van de internetverbinding wordt vaak gebruikt wanneer het apparaat fungeert als modem voor een laptop- of desktopcomputer.	Ja
Remote desktop toestaan	Schakel dit selectievakje waardoor het is toegestaan dat een remote desktop verbinding kan worden opgezet vanaf het mobiele apparaat naar een andere computer.	Ja
Desktop synchronisatie toestaan	Schakel dit selectievakje waardoor het is toegestaan dat het mobiele apparaat wordt gesynchroniseerd met een computer via Desktop ActiveSync of Windows Mobile Device Center.	Ja
Bluetooth toestaan	Selecteer, via de dropdownlijst, of het gebruik van Bluetooth is toegestaan op het mobiele apparaat. De beschikbare opties zijn: toestaan, uitschakelen of alleen inschakelen voor handsfreegebruik.	Ja

Apparaatapplicaties
Deze instellingen bepalen of specifieke functies op een mobiel apparaat in of uit worden geschakeld.

Opmerking: om deze instellingen op het mobiele apparaat te kunnen implementeren moet u over een Exchange Enterprise Clienttoeganglicentie (Client Access License) beschikken voor ieder postvak waarop dit beleid van toepassing is.

Apparaatapplicaties		
ActiveSync-instelling	**Omschrijving**	**Default**
Browser toestaan	Schakel dit selectievakje in waardoor het is toegestaan om gebruik te maken van de Pocket Internet Explorer op het mobiele apparaat.	Ja
E-mail toestaan	Schakel dit selectievakje in waardoor het is toegestaan om naast Microsoft Exchange-accounts ook andere e-mailaccounts te benaderen. Hieronder worden e-mailaccounts bedoeld die toegankelijk zijn via POP3 en IMAP4. Let op: Dit selectievakje heeft geen controle over de toegang voor het mobiele apparaat tot e-mailapplicaties van derden.	Ja
Niet-ondertekende (ofwel 'unsigned') applicaties toestaan	Schakel dit selectievakje in waardoor het is toegestaan om niet-ondertekende applicaties te installeren op het mobiele apparaat.	Ja
Niet-ondertekende installatieprogramma's/ installatiepakketten toestaan	Schakel dit selectievakje in waardoor het is toegestaan om niet-ondertekende installatieprogramma's/installatiepakketten uit te voeren op het mobiele apparaat.	Ja

Overige
Met deze instellingen kunnen applicaties worden gespecificeerd die zijn toegestaan of worden geblokkeerd op een mobiel apparaat.

Opmerking: om deze instellingen op het mobiele apparaat te kunnen implementeren moet u over een Exchange Enterprise Clienttoeganglicentie (Client Access License) beschikken voor ieder postvak waarop dit beleid van toepassing is.

Overige		
ActiveSync-instelling	**Omschrijving**	**Default**
Applicaties die zijn toegestaan	U kunt applicaties toevoegen aan of verwijderen uit de lijst met applicaties die zijn toegestaan. Applicaties die zijn toegestaan kunnen worden geïnstalleerd en uitgevoerd op het mobiele apparaat.	
Applicaties die worden geblokkeerd	U kunt applicaties toevoegen aan of verwijderen uit de lijst met applicaties die worden geblokkeerd. Applicaties die zijn geblokkeerd kunnen niet worden uitgevoerd op het mobiele apparaat.	

Op afstand wissen (Remote Wipe)
Met behulp van Microsoft Exchange Server kunt u door middel van het versturen van een commando naar een mobiel apparaat alle configuratiegegevens en andere informatie verwijderen die op dat mobiele apparaat is opgeslagen. Dit proces wordt afgesloten door het mobiele apparaat terug te brengen naar de oorspronkelijke fabrieksinstellingen.[38]

Let op: wanneer een iPhone of iPhone 3G wordt gewist, worden de gegevens op het apparaat overschreven; de wisbewerking kan voor elke 8 GB aan opslagcapaciteit één uur in beslag nemen.
Op iPhone 3GS en iPad vindt het wissen onmiddellijk plaats en wordt de coderingssleutel voor de gegevens (die zijn versleuteld met 256-bits AES-versleuteling) verwijderd.

U kunt deze functionaliteit gebruiken om gegevens te wissen van een gestolen of verloren apparaat of om gegevens te wissen van een apparaat voordat het wordt overhandigd aan een andere gebruiker.

Gebruikers kunnen hun de gegevens op hun mobiele apparaat ook zelf wissen. Bij het lokaal wissen van de gegevens op het mobiele apparaat wist het mobiele apparaat alle gegevens zonder een verzoek van de server. Het is ook mogelijk om het mobiele apparaat zo te configureren dat het mobiele apparaat automatisch wordt gewist nadat er een bepaald aantal keer een onjuiste toegangscode is ingevoerd. Zie hiervoor ook de Active-Sync-instelling “Maximaal aantal toegestaan mislukte aanmeldingspogingen”. Als deze limiet is bereikt voert het mobiele apparaat het lokaal wissen uit. Het eindresultaat van het lokaal of op afstand wissen van een mobiel apparaat is hetzelfde: het mobiele apparaat wordt terug-gebracht naar de oorspronkelijke fabrieksinstellingen.

Op afstand wissen (Remote Wipe)		
ActiveSync-instelling	**Omschrijving**	**Default**
Op afstand wissen (Remote Wipe)	Door middel van het versturen van een commando naar een mobiel apparaat alle configuratiegegevens en andere informatie verwijderen die op dat mobiele apparaat is opgeslagen. Dit proces wordt afgesloten door het mobiele apparaat terug te brengen naar de oorspronkelijke fabrieksinstellingen	

38. Met Microsoft Exchange Server 2007 en Microsoft Exchange Server 2010 kunt u een Remote Wipe uitvoeren via de Exchange Management Console, Outlook Web Access of Exchange ActiveSync Mobile Administration Web Tool.
http://help.apple.com/iosdeployment-exchange/?lang=nl#exchange2e5bed3

BIJLAGE E » SAMENVATTING RICHTLIJNEN

Algemeen					
Nr.	**Beschrijving van richtlijn**	**Level**	**iOS**	**Android**	**Compliance** [39]
B0-01	Er dienen maatregelen genomen te worden die gebruikers bewust en bekwaam maken	1	Ja	Ja	
B0-02	Er dient inzichtelijk te zijn welke privacygevoelige en vertrouwelijke gegevens worden verwerkt	1	Ja	Ja	
B0-03	Er dienen maatregelen genomen te worden die de privacy-gevoelige en vertrouwelijke gegevens afdoende beschermen	1	Ja	Ja	
B0-04	Er dienen maatregelen genomen te worden die het aantal kwetsbaarheden tot een minimum beperken	1	Ja	Ja	
B0-05	Er dient zoveel mogelijk gebruik gemaakt te worden van bestaande beveiligingsfuncties (features)	1	Ja	Ja	
B0-06	• Maak regelmatig een back-up • Test regelmatig of de back-up ook teruggezet kan worden	1	Ja	Ja	
B0-07	Jailbreak of root nooit het mobiele apparaat	1	Ja	Ja	

39. Voor het aanduiden van de mate van compliance kan gebruik worden gemaakt van de volgende classificatieschema’s:
• Nee/Niet; Eerste aanzet; Halverwege; Voldoende; Goed; Niet van toepassing of Onbekend.
• Nee/Niet; Gedeeltelijk; Ja/Goed; Niet van toepassing; of Onbekend.

Toegangscontrole					
Nr.	**Beschrijving van richtlijn**	**Level**	**iOS**	**Android**	**Compliance**
B1-01	Versleutel opgeslagen gegevens waar mogelijk	1	Ja	Ja	
B1-02	Maak gebruik van verschillende toegangscodes voor het mobiele apparaat, de verschillende diensten en apps	1	Ja	Ja	
B1-03	Wijzig regelmatig de toegangscode van het mobiele apparaat, de verschillende diensten en apps	1	Ja	Ja	
B1-04	Stel een toegangscode in om het mobiele apparaat te ontgrendelen	1	Ja	Ja	
B1-05	Stel een toegangscode in om het mobiele apparaat te ontgrendelen die bestaat uit een combinatie van alfabetische, numerieke en niet-alfanumerieke tekens	1	Ja	Ja	
B1-06	Stel het maximaal aantal toegestane mislukte aanmeldings-pogingen in	1	Ja	Ja	
B1-07	Schakel SIM-kaartvergrendeling in	1	Ja	Ja	
B1-08	Stel automatische vergrendeling in waardoor het mobiele apparaat na een bepaalde periode wordt vergrendeld	1	Ja	Ja	
B1-09	Sta apps niet toe om de gecodeerde opslag van certificaten, toegangscodes en andere credentials te benaderen	2	Nee[40]	Ja	
B1-10	Schakel het tonen van de toegangscode tijdens het invoeren uit	2	Nee[41]	Ja	
B1-11	Schakel voorvertoning van berichten (voor Android alleen SMS-berichten) op het beginscherm uit	2	Ja	Ja	
B1-12	Schakel de functies die ondersteuning bieden bij het ontwikkelen van apps - zoals USB-foutopsporing - uit	1	Nee[42]	Ja	
B1-13	Maak gebruik van volgsoftware	1	Ja	Ja	

40. iOS bevat deze instelling niet.
41. iOS bevat deze instelling niet.
42. Deze instelling wordt niet ondersteund door iOS en vormt dus geen risico voor iOS.

Applicatie					
Nr.	**Beschrijving van richtlijn**	**Level**	**iOS**	**Android**	**Compliance**
B2-01	Het aantal geïnstalleerde apps dient te worden beperkt	1	Ja	Ja	
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	Ja	Ja	
B2-03	Beperk de rechten van geïnstalleerde apps tot een absoluut minimum	1	Ja	Ja	
B2-04	Configureer de browser zodanig dat het noodzakelijke beveiligingsniveau wordt gegarandeerd	1	Ja	Ja	
B2-05	Voorzie tijdig alle software van de laatste versies/patches	1	Ja	Ja	
B2-06	Locatievoorzieningen dienen zoveel mogelijk te zijn uitgeschakeld	1	Ja	Ja	
B2-07	Het mobiele apparaat dient ‘schoon’ in te worden geleverd	1	Ja	Ja	
B2-08	Installeer alleen apps als de bron bekend is	1	Nee[43]	Ja	
B2-09	Schakel JavaScript uit	2	Ja	Ja	
B2-10	Schakel fraudemeldingen in	1	Ja	Nee[44]	
B2-11	Schakel automatisch vullen van webformulieren uit	2	Ja	Ja	
B2-12	Schakel Privémodus (Incognitomodus) in	1	Ja	Ja	
B2-13	Schakel cookies accepteren uit	1	Ja	Ja	
B2-14	Schakel beveiligingswaarschuwingen weergeven in	1	Nee[45]	Ja	

43. Voor iOS geldt dat het niet mogelijk is om van deze richtlijn af te wijken.
44. Android bevat deze instelling niet.
45. iOS bevat deze instelling niet.

Netwerk					
Nr.	**Beschrijving van richtlijn**	**Level**	**iOS**	**Android**	**Compliance**
B3-01	Versleutel verzonden gegevens waar mogelijk	1	Ja	Ja	
B3-02	Schakel netwerkverbindingen zoveel mogelijk uit wanneer deze niet worden gebruikt	1	Ja	Ja	
B3-03	Schakel de mobiele internetverbinding (mobiele data) uit als hier geen gebruik van wordt gemaakt	2	Ja	Ja	
B3-04	Schakel dataroaming uit als hier geen gebruik van wordt gemaakt	1	Ja	Ja	
B3-05	Schakel Persoonlijke hotspot uit als hier geen gebruik van wordt gemaakt	1	Ja	Ja	
B3-06	Schakel Wi-Fi uit als hier geen gebruik van wordt gemaakt	2	Ja	Ja	
B3-07	Stel het mobiele apparaat zo in dat Wi-Fi-netwerken, waar eerder verbinding mee is gemaakt, worden vergeten	1	Ja	Ja	
B3-08	Stel het mobiele apparaat zo in dat er niet wordt gevraagd om een verbinding te maken met een Wi-Fi-netwerk	1	Ja	Ja	
B3-09	Stel het mobiele apparaat zo in dat er niet automatisch met een Wi-Fi-netwerk wordt verbonden	1	Ja	Ja	
B3-10	Maak zoveel mogelijk gebruik van een VPN-verbinding	1	Ja	Ja	
B3-11	Schakel Bluetooth uit als hier geen gebruik van wordt gemaakt	1	Ja	Ja	
B3-12	Schakel Near Field Communication (NFC) uit als hier geen gebruik van wordt gemaakt	1	Nee[46]	Ja	
B3-13	Schakel vliegtuigmodus in als geen draadloze netwerk-verbindingen en voorzieningen nodig zijn.	2	Ja	Ja	

46. Deze instelling wordt niet ondersteund door iOS en vormt dus geen risico voor iOS.

Totaaloverzicht Richtlijnen

Onderdeel	Totaal		Niet door iOS ondersteund	Niet door Android ondersteund
	Niveau 1	Niveau 2		
Algemeen en specifiek beleid	7	-	-	-
Toegangscontrole	9	4	3	-
Applicatie	12	2	2	1
Netwerk	10	3	1	-
Totaal	38	9	6	1
	47			

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