INFORMATIE
BEVEILIGINGS
DIENST

Handreiking

Mobile Device Management

Een van de producten van de operationele variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)

INFORMATIE
BEVEILIGINGS
DIENST

Colofon

Naam document
Mobile Device Management

Versienummer
1.1

Versiedatum
Januari 2018

Versiebeheer
Het beheer van dit document berust bij de Informatiebeveiligingsdienst voor gemeenten (IBD).

Copyright

Rechten en vrijwaring
De IBD is zich bewust van haar verantwoordelijkheid een zo betrouwbaar mogelijke uitgave te verzorgen. Niettemin kan de IBD geen aansprakelijkheid aanvaarden voor eventueel in deze uitgave voorkomende onjuistheden, onvolledigheden of nalatigheden. De IBD aanvaardt ook geen aansprakelijkheid voor enig gebruik van voorliggende uitgave of schade ontstaan door de inhoud van de uitgave of door de toepassing ervan.

Met dank aan
De expertgroep en de reviewgemeenten die hebben bijgedragen aan het vervaardigen van dit product.

Wijzigingshistorie:

Versie	Door	Wijziging / Actie
1	Oktober 2013	Initiële versie
1.0.1	Augustus 2015	Aanscherping in verband met meldplicht datalekken en kleine tekstuele aanpassingen
1.0.2	Augustus 2016	Taskforce BID verwijderd
1.1	November 2017	Uitbreiding in het licht van de AVG en beheer toegevoegd

Over de IBD

De IBD is een gezamenlijk initiatief van alle Nederlandse Gemeenten. De IBD is de sectorale CERT / CSIRT voor alle Nederlandse gemeenten en richt zich op (incident)ondersteuning op het gebied van informatiebeveiliging. De IBD is voor gemeenten het schakelpunt met het Nationaal Cyber Security Centrum (NCSC). De IBD beheert de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) en geeft regelmatig kennisproducten uit. Daarnaast faciliteert de IBD kennisdeling tussen gemeenten onderling, met andere overheidslagen, met vitale sectoren en met leveranciers. Alle Nederlandse gemeenten kunnen gebruik maken van de producten en de generieke dienstverlening van de IBD.

De IBD is ondergebracht bij VNG Realisatie.

Leeswijzer

Dit product maakt onderdeel uit van de operationele variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

Doel

Mobiele gegevensdragers zoals smartphones, tablets en laptops worden binnen de gemeenten gebruikt. Deze aanwijzing is geschreven om vanuit verschillende gezichtspunten de risico's en oplossingen weer te geven die gemeenten kunnen inzetten bij de keuzes voor mobiele apparaten. Als laatste wordt een lijst met functionele eisen en wensen gegeven voor het geval dat men een MDM-oplossing wil implementeren voor het beheren van mobiele apparaten en de gemeentelijke gegevens die erop kunnen staan.

Doelgroep

Dit document is van belang voor bestuur (voor het beleid) en ICT-beheer

Relatie met overige producten

Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)

- Strategische variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten
- Tactische variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten

Bring Your Own Device (BYOD)

Mobiele gegevensdragers

Gedragsregels gebruikers

Maatregelen tactische variant Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)

- Hoofdstuk 6.4 in het gemeentelijk informatiebeveiligingsbeleid
- Hoofdstuk 7.1.3 van de BIG
- Hoofdstuk 9.1.3 van de BIG

Inhoudsopgave

1 Inleiding

De Baseline Informatiebeveiliging voor Gemeenten (BIG) heeft maatregelen beschreven die te maken hebben met het gebruik van mobiele apparaten, zie hiervoor hoofdstuk 6.4 in het voorbeeld gemeentelijk informatiebeveiligingsbeleid van de IBD en hoofdstuk 7.1.3 en 9.1.3.1 van de BIG.

Sinds mobiele gegevensdragers persoonsgegevens kunnen bevatten, denk bijvoorbeeld aan documenten en/of e-mails, dient bij verlies of diefstal nagegaan te worden of er sprake is van een datalek. In geval van een datalek dient deze gemeld te worden bij Autoriteit Persoonsgegevens (AP).

Doelstelling mobile device management

Mobiele gegevensdragers zoals smartphones, tablets, laptops en mobiele apparaten voor primaire processen (zoals handhelds voor handhavers worden veel gebruikt. Deze aanwijzing is geschreven om vanuit verschillende gezichtspunten de risico's en oplossingen weer te geven die gemeenten kunnen inzetten bij de keuzes voor mobiele apparaten. Het maakt voor deze aanwijzing niet uit of het een gemeentelijk mobiel device is of een eigen mobiel device (in het geval van Bring Your Own Device), immers op mobiele apparaten kan in meer of mindere mate data van de gemeente staan. Los van het feit of het mobiele apparaat fysiek kan zoekraken, de data is in beide gevallen van de gemeente. Verder wordt er door het 'nieuwe werken' steeds meer gebruik gemaakt van laptops.

Doelstelling is veilig omgaan met mobiele apparaten en de gemeentelijke gegevens die erop kunnen staan, omdat:

- Mobiele apparaten een malware besmetting kunnen oplopen en daarmee ook de gemeente infecteren (het mobiele apparaat wordt door hackers als aanvalsvector gebruikt);
- Mobiele apparaten (persoons) gegevens bevatten en doorgaans buiten de gemeentelijke gebouwen zijn. Deze (persoons) gegevens kunnen zoekraken of worden ingezien door onbevoegden; Dit kan een datalek tot gevolg hebben en deze dient gemeld te worden bij Autoriteit Persoonsgegevens (AP).
- Mobiele apparaten door malware hoge SMS, dataverbruik en telefoon kosten kunnen veroorzaken;
- Mobiele apparaten kunnen zoekraken of gestolen worden (vervangschade en inzien van gegevens);
- Mobiele apparaten kunnen worden gebruikt om gemeentelijke systemen te benaderen (privacy, bewerken gegevens).

Aanwijzing voor gebruik

Deze aanwijzing is qua opzet geschreven om informatiebeveiligingsmaatregelen met betrekking tot mobile device management te duiden en scherper neer te zetten. Deze aanwijzing is niet een volledige procesbeschrijving en bevat geen productnamen, deze aanwijzing bevat wel voldoende informatie om goede keuzes te maken en bewustwording te creëren met betrekking tot mobile device management.

De gemeentelijke beleidsregels met betrekking tot mobile device management (uit het voorbeeld informatiebeveiligingsbeleid document van de IBD): Mobiele (privé)apparatuur en thuiswerkplek

- Beveiligingsmaatregelen hebben betrekking op zowel door de gemeente verstrekte middelen als privé apparatuur die (ook) zakelijk wordt gebruikt ('bring your own device'). Op privé apparatuur waarmee verbinding wordt gemaakt met het gemeentelijke netwerk is de gemeente bevoegd om beveiligingsinstellingen af te dwingen, vermits er data daadwerkelijk op privé apparaat achterblijft bijvoorbeeld in het geval van e-mail synchronisatie. Dit betreft onder meer: controle op wachtwoord, encryptie, aanwezigheid van malware, et cetera. Het gebruik van privé apparatuur waarop beveiligingsinstellingen zijn verwijderd ('jailbreak', 'rooted device') is niet toegestaan. [1]

- Op verzoek van de gemeente dienen medewerkers de installatie van software om bovenstaande

[1] Jailbreak is het mogelijk maken van het draaien van niet goedgekeurde apps op een iOS apparaat, waardoor ook mailware gedraaid kan worden; Rooten is het proces dat het mogelijk maakt dat men meer rechten krijgt op het apparaat (android) en daardoor het complete besturings systeem te wijzigen of te vervangen, en daarmee mailware introduceren en gemeentelijke beveiligingsinstellingen te omzeilen.

beleidsregel te handhaven toe te staan (denk bijvoorbeeld aan ‘mobile device management software’). De beveiligingsinstellingen, zoals bedoeld in bovenstaande regel, zijn uitsluitend bedoeld ter bescherming van gemeentelijke informatie en integriteit van het gemeentelijke netwerk.

- In geval van dringende redenen kunnen noodmaatregelen worden getroffen, zoals wissen van apparatuur op afstand. Deze noodmaatregelen kunnen, voor zover dit noodzakelijk is, betrekking hebben op privémiddelen en privébestanden, hiervoor wordt een regeling ontwikkeld.

De BIG schrijft over mobile device management het volgende:

Hoofdstuk 7.1.3 van de BIG gaat over: Aanvaardbaar gebruik van bedrijfsmiddelen.

Er behoren regels te worden vastgesteld, gedocumenteerd en geïmplementeerd voor aanvaardbaar gebruik van informatie en bedrijfsmiddelen die verband houden met ICT-voorzieningen.

1. Er zijn regels voor acceptabel gebruik van bedrijfsmiddelen (met name internet, e-mail en mobiele apparatuur). De CAR-UWO verplicht ambtenaren zich hieraan te houden. Voor extern personeel is dit in het contract vastgelegd.
2. Gebruikers hebben kennis van de regels.
3. Apparatuur, informatie en programmatuur van de organisatie mogen niet zonder toestemming vooraf van de locatie worden meegenomen. De toestemming kan generiek geregeld worden in het kader van de functieafspraken tussen manager en medewerker.
4. Informatiedragers worden dusdanig gebruikt dat vertrouwelijke informatie niet beschikbaar kan komen voor onbevoegde personen.

Paragraaf 9.1.3 van de BIG beschrijft maatregelen bij gevoelige informatie op een device:
Papieren documenten en mobiele gegevensdragers die vertrouwelijke informatie bevatten worden beveiligd opgeslagen, tenzij de vertrouwelijke informatie op de mobile gegevensdrager voldoende versleuteld is.

In wezen zijn een telefoon of tablet een mobiele gegevensdragers, met behulp van MDM dient er dan voor gezorgd te worden dat de informatie indien nodig beveiligd is.

2 Wat is Mobile Device Management?

Mobile Device Management (MDM) is het stelsel van maatregelen, procedures en ondersteunende producten die het mogelijk maken om mobiele gegevensdragers veilig te kunnen gebruiken en te kunnen beheersen. De controls staan beschreven in de BIG en het afgeleide gemeentelijk beveiligingsbeleid. In dit document wordt aan het einde een aanvullend stuk MDM-beleid gegeven. dat de gemeente aanvullend op het gemeentelijk beveiligingsbeleidsdocument kan uitgeven.

MDM is van toepassing op de volgende mobiele gegevensdragers:

- Smartphones
- Gewone telefoons
- Tablets, zoals een iPad
- Een Dongel of MiFi voor mobiele toegang (MiFi is een Dongel met WiFi ingebouwd)
- Een laptop

De bovenstaande gegevensdragers kunnen al dan niet door de gemeente verstrekt zijn. Dit document gaat specifiek in op smartphones en tablets.

Mobile Application Management (MAM)

Anders dan Mobile Device Management, welke assisteert in activatie, uitrol en inrichting van een apparaat, richt MAM-software zich meer op de uitrol, inrichten, software licensering en configuratie van software op de apparaten.

MAM-software kan voor gemeentes interessant zijn om gebruikt in combinatie met BYOD (zie volgende paragraaf).

Bring Your Own Device (BYOD)

Dit onderwerp komt veelvuldig ter sprake, ook bij gemeenten die gevraagd hebben om aanvullende operationele producten van de IBD aangaande de BIG. BYOD houdt in dat medewerkers eigen apparaten kunnen gebruiken om gemeentelijk werk te doen. De gemeente geeft hier bij voorkeur ook toestemming voor. Op dit moment worden mobiele apparaten ook zonder toestemming voor gemeentelijke informatie gebruikt. Deze apparaten kunnen onderweg, maar ook op kantoor worden gebruikt. Deze mobiele apparaten kunnen dus toegang krijgen tot gemeentelijke (en daarmee mogelijk gevoelige) informatie en deze informatie kan ook op het betreffende apparaat terechtkomen.

Risico's

Welke risico's kunnen samenhangen met het gebruik van mobiele apparaten binnen de gemeente?

1. Malware besmetting op het mobiele apparaat [2]

Oorzaken:

- Geen vastgesteld gemeentelijk beleid over welke applicaties zijn toegestaan, niet-vertrouwde applicatiebronnen gebruiken kan risico verhogend werken.
- Jailbreaken of rooten van apparaten
- Klikken op links in mail, webpagina's en in SMS-berichten die niet vertrouwd zijn
- Verbinden via onveilige open netwerken, waar men kan worden aangevallen door derden
- Openen van met malware besmette bestand, bijvoorbeeld een bijlage van een e-mail.

Gevolgen

- Installatie kwaadaardige software die gegevens steelt[3], zichzelf toegang verschaft, maar ook zichzelf

[2] Zie hiervoor het anti malware beleid van de IBD: https://www.ibdgemeenten.nl/downloads/?id=464

[3] In geval van persoonsgegevens is dit ook een datalek dat waarschijnlijk gemeld moet worden aan de Autoriteit Persoonsgegevens.

verspreidt over andere gemeentelijke systemen.
- Ook is installatie mogelijk van dialers die sms'jes zenden of bellen met dure nummers, met als gevolg hoge kosten.
- Hoge dataverbruik door installatie van kwaadaardige software

Maatregelen
- Vaststellen en implementeren gemeentelijke beleidsregels voor mobiele apparaten;
- Implementeren Mobile Device Management Software om security policies af te dwingen op mobiele apparaten (ook op BYOD-apparaten);
- Uitzetten van services die niet direct nodig zijn;
- Geen onvertrouwde netwerken gebruiken;
- Specifiek aandacht voor dit issue in bewustwordingscampagnes.

2. (Persoons) gegevens verlies, gegevens onbevoegd inzien

Oorzaken:
- Geen vastgesteld gemeentelijk beleid over welke gegevens op mobiele apparaten mogen staan, geen dataclassificatie beleidsregels kan risico verhogend werken;
- Malware op het device;
- Klikken op links in mail, webpagina's en in SMS-berichten die niet vertrouwd zijn;
- Verbinden via onveilige open netwerken;
- Man in the middle attack[4] ;
- Niet locken van het device;
- Geen encryptie, terwijl dat wel nodig is (inhoud apparaat en verbindingsweg).

Gevolgen
- Inzien gegevens door onbevoegden, kopiëren van gegevens, vernietigen van gegevens, veranderen van gegevens met als gevolgd een datalek indien het persoonsgegevens betreft. Een datalek persoonsgegevens kan tot gevolg hebben dat er een datalek gemeld moet worden bij de AP.

Maatregelen
- Vaststellen en implementeren gemeentelijke mobiele apparaten beleidsregels
- Implementeren apparaat encryptie, in ieder geval beveiligde opslag van gemeentelijke gegevens als die al worden toegestaan op het device. Waar mogelijk zero footprint software gebruiken
- Implementeren MDM-software
- Implementeren MAM-software
- Implementeren apparaat authenticatie
- Implementeren kanaal encryptie en twee factor authenticatie
- Specifiek aandacht voor dit issue in bewustwordingscampagnes
- Invoeren incidentmanagement

3. Zoekraken apparatuur (fysiek)

Oorzaken
- Diefstal
- Verlies (onopzettelijk)

[4] Uit wikipedia: Een man-in-the-middle-aanval is een aanval waarbij informatie tussen twee communicerende partijen onderschept wordt, zonder dat beide partijen daar weet van hebben. Dit terwijl de computer van de aanvaller zich tussen deze partijen bevindt.

Gevolgen

- Het mobiele apparaat moet vervangen worden voor een nieuw apparaat.
- Mogelijk inzien (persoons) gegevens door onbevoegden, kopiëren van gegevens, wijzigen van gegevens, vernietigen van gegevens. Een datalek persoonsgegevens kan tot gevolg hebben dat er een datalek gemeld moet worden bij de AP.
- Toegang tot gemeentelijke systemen met het mobiele apparaat.

Maatregelen

- Vaststellen en implementeren gemeentelijke mobiele apparaten beleidsregels;
- Implementeren apparaat encryptie, in ieder geval beveiligde opslag van gemeentelijke gegevens als die al worden toegestaan op het device. Waar mogelijk zero footprint software gebruiken
- Implementeren MDM-software
- Implementeren van een apparaat opzoek functie (in de MDM-software)
- Implementeren van een functie om het apparaat op afstand te wissen
- Toegang tot gemeentelijke systemen door middel van 2 factor authenticatie (dus met het apparaat alleen kan geen toegang worden verkregen)
- Specifiek aandacht voor dit issue in bewustwordingscampagnes
- Invoeren incidentmanagement

Mobiele apparaten die van de gemeente zijn, dienen te worden bijgehouden in de ICT-Configuratie Management Database. Bij (privé) BYOD-apparaten, waaronder zakelijk verstrekte apparaten, is dit lastiger, tenzij er afgedwongen wordt dat alle apparaten waar gemeentelijke informatie op kan staan, geregisterd worden. Binnen MDM-tooling bestaat hier functionaliteit voor. Voor MDM-tooling is op grond van artikel 27, eerste lid, onder K en l, van de Wet op de Ondernemingsraden instemming van de ondernemingsraad (OR) nodig.

Bijlage 1: Voorbeeld Mobile Device Management beleid gemeente <naam gemeente>

Uitgangspunten Mobile Device Management

Ten behoeve van Mobile Device Management dienen er regels binnen de gemeente te zijn die gehanteerd moeten worden als er mobiele apparaten worden geïntroduceerd. Het doel van deze aanwijzing is te voorkomen dat de risico's van in geval van gedeeltelijk of geheel verlies of beschadiging van data en/of programmatuur en hardware, de dienstverlening van de gemeente hinder ondervindt.
Er dient binnen de gemeente ook nagedacht te worden over welke diensten wel, en welke diensten zeker niet uitgevoerd mogen worden op mobiele apparaten.

De volgende regels dienen terug te komen in gemeentelijk aanvullend beleid omtrent Mobile Device Management of gebruikersovereenkomsten als deze niet al opgenomen zijn in gemeentelijke integriteitsregels.

1. Het opstellen van regels voor acceptabel gebruik. Deze regels dienen door de medewerker geaccepteerd en getekend te worden. Binnen de regels voor acceptabel gebruik is aandacht voor:
   - Het proces in geval van verlies of diefstal van alle mobiele gegevensdragers, waarbij meldingen binnen 4 uur gedaan moeten worden
   - Niet voldoen aan beleid en regels kan resulteren in een disciplinair proces volgens de CAR/UWO
   - Een verbod op het downloaden van illegale software en/of software uit niet-vertrouwde bronnen
   - Een verbod op rooten en jailbreaken van een mobiel apparaat (dit vergroot de kans op illegale software of toegang krijgen tot de telefoon)[5]
   - Regels over excessief gebruik in Nederland en tijdens roaming in Europa
   - Bij bellen of gebruik in de auto zich houden aan wettelijke regels
   - Zich houden aan ICT-standaarden en nadere afspraken

2. Gebruikers hebben kennis van de regels:
   - Het gebruik van mobiele apparatuur dient aandacht te hebben in bewustwordings- trainingsmateriaal van de gemeente

3. Toevoegen van regels voor het meenemen van informatie:
   - De gemeente dient ook aandacht te hebben voor de impliciete toestemming aan gebruikers welke informatie zij wel of niet mogen inzien met hun device, of
   - Er dient duidelijk te worden gemaakt dat de medewerker achteraf ter verantwoording geroepen kan worden

4. Detailregels om te zorgen voor bescherming van gegevens op apparaten:
   - De gemeente hanteert classificatie regels van gemeentelijke gegevens en zorgt voor passende maatregelen om dit op apparaten (al of niet) te ondersteunen

5. Alle mobiele apparaten, zowel van de gemeente of privé, waarop gemeentelijke gegevens kunnen staan worden bij voorkeur beheerd met een MDM-tool met functionaliteiten zoals genoemd in de bijlage.

3.1 Jurisprudentie m.b.t. illegale software

Op 10 augustus 2016 heeft de rechtbank Rotterdam uitspraak gedaan over de aansprakelijkheid van een werkgever

[5] Jailbreak is het mogelijk maken van het draaien van niet goedgekeurde apps op een iOS apparaat, waardoor ook mailware gedraaid kan worden; Rooten is het proces dat het mogelijk maakt dat men meer rechten krijgt op het apparaat (android) en daardoor het complete besturings systeem te wijzigen of te vervangen, en daarmee mailware introduceren en gemeentelijke beveiligingsinstellingen te omzeilen.

voor de aanwezigheid van illegale software op de laptop van een werknemer. De werkgever werd veroordeeld voor het betalen van een schadevergoeding aan de softwareleverancier.

Een werknemer had illegale software geïnstalleerd op een laptop, zonder medeweten van de werkgever en zonder dat deze software noodzakelijk was voor zijn werkzaamheden. De softwareleverancier kwam achter de illegale installatie en klaagde de werkgever van de werknemer aan.

De reden van de veroordeling komt voort uit het ”risicoaansprakelijkheid”, art. 6:170 BW. Samengevat zegt deze wet dat in wiens dienst een werknemer zijn taak vervult aansprakelijk is voor zijn of haar fouten. Dit geldt zolang als er een relatie bestaat tussen de fout en diens opgedragen werkzaamheden. Dit wordt over het algemeen zeer ruim uitgelegd.

Vaak kan er op apparatuur van de zaak kan vaak niet zomaar software worden geïnstalleerd. Bij BYOD ligt dit anders. Dit vraagt extra alertheid van de gemeenten. Door gevoerd BYOD-beleid komt de grens tussen zakelijk en privé gebruik steeds verder te vervalen. Maak medewerkers bewust van het gebruik van illegale software zowel binnen- als buitenwerktijd.

De lering die hieruit getrokken kan worden zijn tweeledig:

- Het is verstandig mobiele apparaten zo te beveiligen dat installatie van (illegale) software niet mogelijk is of
- De apparaten op regelmatige wijze (automatisch) te laten controleren op aanwezigheid van (illegale) software.

Bijlage 2: Functionele eisen MDM-software

Om een goede keuze te kunnen maken voor Mobile Device Management-software zijn de volgende vragen van belang:

Kan de software binnen de gemeente worden gebruikt op eigen hardware of is er een cloud/
SaaS-oplossing voor handen?
Welke platforms is de gemeente bereid te ondersteunen en kan de tool deze ook ondersteunen, denk hierbij aan: iOS, Android, BlackBerry, Windows Phone, Symbian, overige?

Zijn de volgende mobile device managementfuncties aanwezig?

- Wachtwoord bescherming instelbaar
- Wachtwoord reset functie beschikbaar
- Op afstand het device leegmaken (remote wipe)
- Selectief leegmaken apparaat
- Op afstand blokkeren
- Instellen netwerk settings
- Uitschakelen functies zoals: netwerk, bluetooth, 3G data, camera.
- Automatische uitrol software en policies
- Monitoring configuraties

Zijn de volgende beveiligingsfuncties aanwezig?

- Applicatie backlisting en applicatie whitelisting
- Apparaat compromitteren (rooting en jailbreaking detectie)
- Wisselen sim-card detectie
- Data protectie (DLP)
- Apparaat encryptie
- Folder/ map encryptie
- Encryptie van e-mail en ook bijlagen
- Geofencing (instellen geografische grenzen waarbij overschrijding zorgt voor een alarm)
- Tijd restricties kunnen opleggen (instellen tijdstippen waarbinnen het apparaat gebruikt mag worden)
- VPN-functies (voor veilige encrypted verbindingen)
- Antivirus functies/ detectie
- Firewall
- Single Sign-on Support

Applicatie beheer functies?

- Kunt u een eigen App Store opzetten waaruit de user kan/mag kiezen? Kan die App Store ook voor desktopapplicaties gebruikt worden?
- Voorkom dat MDM-software verwijderd kan worden en apps geassocieerd daar mee.
- Is applicatie sandboxing mogelijk (applicatie draait dan in een eigen afgeschermde omgeving)?
- Zijn er tools aanwezig voor sandboxing?
- Is er een integratie mogelijk van een andere App Store (bijvoorbeeld Apple)?
- Zijn er virtuele desktopfuncties of applicaties beschikbaar?

Document/ content managementfuncties?

- Is er een aparte encrypted document container/ locatie mogelijk?
- Is e-mail beveiliging mogelijk?
- Is toegang tot (eigen) bestanden op servers mogelijk?
- Is er integratie met Sharepoint of ander Document Management Sofware? (bij voorkeur die de gemeente zelf al heeft)?

Netwerkbeheer functies?

- Data verbruik beheer (over Wi-Fi maar ook mobiele netwerken)
- Controle over roaming-kosten, of blokkeren roaming
- Diagnose functies
- Monitoren gebruik
- Blokkeren van devices als bijvoorbeeld instellingen worden aangepast of als policies niet geaccepteerd worden Service management / ICT-beheer
- Helpdesk supportfuncties
- Service monitoring

Integratie

- Mogelijkheden om te integreren met PC Beheer tooling?
- Met welke andere desktop tooling kan worden geïntegreerd?
- Zijn er integratie API's?
- Is er een Management Console voor Mobile Devices en PC's?

Rapporten

- Zijn er alarmen?
- Geautomatiseerde respons op alarmen instelbaar?
- Real-time overzichten beschikbaar?
- Analyse tot op device niveau?
- Analyse tot op app niveau?

Toekomstige gerichtheid

- Er komen steeds nieuwe (mobiele) apparaten en Operating Systeem versies uit. Een MDM-oplossing dient zo ontworpen te zijn en ingericht kunnen worden dat deze mee kan gaan met deze nieuwe (mobiele) apparaten en Operating Systemen.
- Een MDM-oplossing dient meerdere versies van een Operating Systeem te kunnen ondersteunen.
- Een MDM-oplossing moet zo snel mogelijk bij het verschijnen van een nieuwe versie van een Operating Systeem en/of veiligheidsupdate deze ondersteunen.

Bijlage 3: Beschikbare update(s) installeren?

Geregeld verschijnen er updates voor Operating Systemen en beveiligingsupdates voor (mobiele) apparaten.

Het kan voorkomen dat door de installatie van zo'n update de MDM-oplossing niet meer functioneert. Daarom is het van belang dat voordat er een update wordt uitgerold deze te testen. Voor meer informatie over testen kan het document patchmanagement[6] worden gevonden.

Sommige updates hebben van de fabrikant het predicaat 'kritiek' of vergelijkbaar meegekregen, bijvoorbeeld om een (ernstige) beveilig probleem op te lossen.

Tijdens de testfase van een update met het predicaat 'kritiek' kan worden ontdekt dat de MDM-oplossing niet meer (naar behoren) functioneert. Op dat moment zal er een risicoanalyse[7] moeten plaatsvinden om te bepalen wat prioriteit heeft, de MDM-oplossing of de installatie van de update. De keuze welke prioriteit heeft hangt onder andere af van het risico dat er wordt gelopen wanneer deze update niet wordt geïnstalleerd. Voor meer informatie met betrekking tot het doen van een risicoanalyse kan worden gevonden in het document 'Diepgaande risicoanalyse methode Gemeente '.

6 Zie de handreiking Patchmanagement voor gemeenten: https://www.ibdgemeenten.nl/downloads/?id=458

7 Zie ook de handreiking diepgaande risicoanalyse: https://www.ibdgemeenten.nl/downloads/?id=1788

Kijk voor meer informatie op: www.IBDGemeenten.nl

Nassaulaan 12
2514 JS Den Haag
CERT: 070 373 80 11 (9:00 – 17:00 ma – vr)
CERT 24x7: Piketnummer (instructies via voicemail)
info@IBDGemeenten.nl / incident@IBDGemeenten.nl

VNG Realisatie