WERKORGANISATIE DUIVENVOORDE

BLAD GEMEENSCHAPPELIJKE REGELING

Nr. 1057

20 juli 2018

Officiële uitgave van de gemeenschappelijke regeling Werkorganisatie Duivenvoorde

Regeling mobile device management en mobiel werken

Inhoudsopgave

Definities

1. **Rooten** is het proces dat het mogelijk maakt dat men meer rechten krijgt op het apparaat (android) en daardoor in staat is het complete besturings systeem te wijzigen of te vervangen, en daarmee malware introduceren en gemeentelijke beveiligingsinstellingen te omzeilen.
2. **Jailbreak** is het mogelijk maken van het gebruiken van niet goedgekeurde apps op een iOS apparaat, waardoor ook malware gebruikt kan worden;
3. **Man in the middle**: 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.
4. **Zero footprint**: er worden geen gegevens opgeslagen op het apparaat zelf.
5. **2 factor authenticatie** is een authenticatie methode waarbij je twee stappen succesvol moet doorlopen om ergens toegang tot te krijgen. Naast het traditionele wachtwoord moet je een tokencode invoeren (SMS of softtoken).

1. Inleiding

De Baseline Informatiebeveiliging voor Gemeenten heeft maatregelen beschreven die te maken hebben met het gebruik van mobiele apparaten, o.a. hoofdstuk 7.1.3, 9.1.3, 10.4.1 van de BIG. Het dagelijks bestuur van de WODV heeft op 14-2-2017 het informatiebeveiligingsbeleid vastgesteld voor de WODV en de gemeenten Voorschoten en Wassenaar. Met het vaststellen van het beleid wordt de BIG als normenkader voor informatiebeveiliging gehanteerd.

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 apparaat:
"Papieren documenten en mobiele gegevensdragers die vertrouwelijke informatie bevatten worden beveiligd opgeslagen. Een telefoon, laptop of tablet is een mobiele gegevensdrager."
Paragraaf 10.4.1 van de BIG beschrijft maatregelen tegen virussen:
"Op mobile devices wordt antivirus software toegepast, waarbij bij BYOD de eindgebruiker verplicht is deze zelf toe te passen."
Paragraaf 11.7.1 van de BIG beschrijft maatregelen voor draagbare computers en communicatievoorzieningen:
"Er behoort formeel beleid te zijn vastgesteld en er behoren geschikte beveiligingsmaatregelen te zijn getroffen ter bescherming tegen risico's van het gebruik van draagbare computers en communicatiefaciliteiten.

1. *Het mobiele apparaat is waar mogelijk zo ingericht dat geen bedrijfsinformatie wordt opgeslagen ('zero footprint'). Voor het geval dat zero footprint (nog) niet realiseerbaar is, of functioneel onwenselijk is, geldt:*
   een mobiel apparaat (zoals een handheld computer, tablet, smartphone, PDA) biedt de mogelijkheid om de toegang te beschermen d.m.v. een wachtwoord en versleuteling van die gegevens. Voor printen in onvertrouwde omgevingen vindt een risicoafweging plaats.
2. *Er zijn, waar mogelijk, voorzieningen om de actualiteit van anti-malware programmatuur op mobiele apparaten te garanderen.*
3. *Bij melding van verlies of diefstal wordt de communicatiemogelijkheid met de centrale applicaties afgesloten."*

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 beveiligingsbeleid.
MDM is van toepassing op de volgende mobiele gegevensdragers:

- Smartphones
- Tablets, zoals een iPad
- Een (hybride) laptop

Er is binnen de WODV een toename van het gebruik van mobiele gegevensdragers zoals smartphones, tablets en laptops. Dit beleidsstuk is geschreven om vanuit verschillende gezichtspunten de risico's en oplossingen weer te geven die betrekking hebben op de inzet van mobiele apparaten. In het kader van de doorontwikkeling van het telefonie- en werkplekconcept zal er medio 2018 gefaseerd een uitrol gaan plaatsvinden van (hybride) laptops. Dit versterkt de noodzaak om vooraf beleid vast te stellen.

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

- Mobiele apparaten een malware besmetting kunnen oplopen en daarmee ook het WODV netwerk infecteren (het mobiele apparaat wordt door hackers als aanvalsvector gebruikt);
- Mobiele apparaten gegevens bevatten en doorgaans buiten de gemeentelijke gebouwen zijn. Deze gegevens kunnen zoekraken of worden ingezien door onbevoegden;
- Mobiele apparaten door malware hoge SMS of telefoonkosten kunnen veroorzaken;
- Mobiele apparaten kunnen zoekraken of gestolen worden (vervangschade);
- Mobiele apparaten gebruikt kunnen worden om gemeentelijke systemen te benaderen (privacy, inzien gegevens).

1. Malware besmetting op het mobiele apparaat

Mogelijke oorzaken:

- Niet toegestane applicaties installeren of niet-vertrouwde applicatiebronnen gebruiken;
- 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;
- Aansluiten van usb devices zoals een dvd/cd apparaat, opslagapparaat etc.

<u>Gevolg</u>
Installatie van kwaadaardige software die gegevens steelt, zichzelf toegang verschaft, maar ook zichzelf verspreidt over andere WODV systemen. Ook is installatie mogelijk van dialers die sms'jes zenden of bellen met dure nummers, met als gevolg hoge kosten.

<u>Maatregelen</u>

- Implementeren MDM Software om beveiligingsmaatregelen af te dwingen op mobiele apparaten;
- Uitzetten van services die niet direct nodig zijn;
- Geen onvertrouwde netwerken gebruiken;
- Specifiek aandacht voor dit onderwerp opnemen in bewustwordingscampagnes.

2. Gegevensverlies, gegevens onbevoegd inzien
Mogelijke oorzaken:
- Het niet toepassen van dataclassificatie beleidsregels voor data op mobiele apparaten;
- Malware op het apparaat;
- 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;
- Niet vergrendelen van het apparaat;
- Geen encryptie (inhoud apparaat en verbinding).

Gevolg
Inzien gegevens door onbevoegden, kopiëren van gegevens, vernietigen van gegevens, veranderen van gegevens. Dergelijke gevolgen worden beschouwd als datalekken en moeten gemeld worden bij de Autoriteit persoonsgegevens (AP), waarna zij onderwerp van onderzoek door de AP kunnen worden. Boetes kunnen het gevolg zijn.

Maatregelen
- Vaststellen en implementeren beleidsregels mobiele apparaten;
- Implementeren apparaat encryptie. Waar mogelijk zero footprint toepassen.
- Implementeren MDM software;
- Implementeren apparaat authenticatie;
- Implementeren netwerk encryptie en 2 factor authenticatie;
- Specifiek aandacht voor dit onderwerp opnemen in bewustwordingscampagnes.

3. Zoekraken apparatuur (fysiek)
Mogelijke oorzaken:
- Diefstal
- Verlies (onopzettelijk)

Gevolg
- Het mobiele apparaat moet vervangen worden voor een nieuw apparaat.
- Mogelijk inzien gegevens door onbevoegden, kopiëren van gegevens, vernietigen van gegevens.
- Toegang tot WODV systemen met het mobiele apparaat.

Maatregelen
- Vaststellen en implementeren beleidsregels mobiele apparaten;
- Implementeren apparaat encryptie. Waar mogelijk zero footprint toepassen.
- Implementeren MDM software;
- Implementeren van een apparaat opzoek functie (binnen de MDM software);
- Implementeren van een functie om het apparaat op afstand te kunnen wissen;
- Externe toegang (buiten de gemeentelijke kantoren) tot WODV systemen door middel van twee factor authenticatie;
- Mobiele apparaten (en alle overige ICT middelen) dienen te worden bijgehouden in de ICT-Configuratie Management Database. (CMDB);
- Specifieke aandacht voor dit onderwerp opnemen in bewustwordingscampagnes.

3. Beleidsregels mobiele apparaten

De hierna beschreven beleidsregels mobiele apparaten zijn uitsluitend bedoeld ter bescherming van WODV c.q. gemeentelijke informatie en integriteit van het WODV netwerk. De beleidsregels volgen op de in hoofdstuk 2 beschreven risico's en de mogelijk te nemen maatregelen.

1.
De WODV is bevoegd om beveiligingsinstellingen af te dwingen op de mobiele apparaten. Dit betreft onder meer:

- controle op en toepassen van wachtwoord-beleid (o.a. sterkte wachtwoord, apparaat vergrendeling, resetten van wachtwoorden);
- toepassen van encryptie van apparaat;
- toepassen van zero footprint;
- toepassen van encryptie op verbindingen;
- controle op aanwezigheid van virussen en malware;
- verplichten van gebruik anti-virus / anti-malware toepassingen;
- controle op internet en mail content op aanwezigheid van virussen en malware;
- controle op niet toegestane applicaties op basis van blacklist/whitelist;
- controle op het verwijderen van beveiligingsinstellingen ('jailbreak', 'rooted device');
- toepassen van beperkingen voor het aansluiten van (USB) devices zoals een dvd/cd apparaat, opslagapparaat etc.
- verplichten van 2 factor authenticatie voor externe toegang (buiten de gemeentelijke kantoren) tot WODV systemen;
- toepassen van beperkingen voor het raadplegen van specifieke informatiesystemen (o.a. BRP) buiten de gemeentelijke kantoren.

2.
In geval van dringende redenen kunnen noodmaatregelen worden getroffen, zoals het traceren, blokkeren en/of wissen van apparatuur op afstand.

3.
Er zijn (aangepaste) bruikleenovereenkomsten opgesteld (zie bijlagen 1 t/m 3). Hierin zijn aanvullende voorwaarden en gebruiksregels opgenomen die betrekking hebben op informatieveiligheid. Dit betreft onder meer:

- voorkomen van diefstal of verlies van apparaat;
- hoe te handelen bij diefstal of verlies van apparaat;
- het wachtwoord-beleid;
- het niet onbeheerd / niet vergrendeld achter laten van apparatuur;
- het installeren van niet toegestane applicaties; (illegale software en software uit niet vertrouwde bronnen)
- het verwijderen van beveiligingsinstellingen ('jailbreak', 'rooted device');
- het uitvoeren van activiteiten op de apparatuur die in strijd zijn met organisatiedoelen of die het imago van de WODV en/of de gemeenten kunnen schaden.

4.
Mobiele apparaten (en alle overige ICT middelen) worden bijgehouden in de ICT-Configuratie Management Database. (CMDB)

5.
Bring Your Own Device (BYOD) houdt in dat medewerkers eigen apparaten kunnen gebruiken om toegang te krijgen tot informatiesystemen van de WODV. Dit kan een laptop zijn waar het thuiswerk portaal op gestart wordt. Maar ook Smartphones die de mail en agenda synchroniseren. Vanaf medio 2018, na invoering van het nieuwe telefonie- en werkplekconcept, wordt het BYOD principe afgeschaft. Toegang tot informatiesystemen of synchronisatie van mail / agenda mag alleen vanaf de door de WODV beschikbaar gestelde hybride laptop of Smartphone. Dit geldt ook voor het thuiswerk portaal. Het is wel toegestaan om met eigen apparatuur binnen de gemeentelijke kantoren gebruik te maken van de beveiligde openbare (en apart gesegmenteerde) WiFi verbinding.

6.
Berichten die via de smartphone of hybride laptop worden uitgewisseld, via mail of andere apps zoals WhatsApp, kunnen op grond van de Wet openbaarheid van bestuur opgevraagd worden.

Doelgroepen

Het gebruik van mobiele gegevensdragers is geregeld in het directiebesluit m.b.t. het nieuwe telefonie- en werkplekconcept (13-09-2017) en in het directiebesluit ICT faciliteiten OGB Buitendienst. (6-12-2017) De WODV onderkent de volgende typen medewerkers die gebruik maken van mobiele gegevensdragers.

Type	Omschrijving	Toegewezen apparatuur	Externe toegang*
Interne medewerker	Tijdelijk of vast	Hybride laptop + Smartphone**	Standaard

Buitendienst medewerker	Tijdelijk of vast	Geen***	Nee
Stagiaires	Tijdelijk	Hybride laptop uit de pool	Nee
Ingehuurde medewerker	Tijdelijk	Hybride laptop uit de pool	Nee
Raadslid	Raadsperiode	Hybride laptop	Beperkt
Commissielid	Raadsperiode	Hybride laptop (1 per fractie)	Beperkt

Standaard = toegang tot alle gemeentelijke informatiesystemen en diensten met uitzondering van de door de dataclassificatie beperkte specifieke informatiesystemen. (o.a. BRP)
Beperkt = toegang tot een beperkte set aan gemeentelijke informatiesystemen en diensten (o.a. Mail/Agenda/Vergader App)
Nee = in principe geen toegang. Alleen in uitzonderlijke gevallen kan de leidinggevende gemotiveerd een aanvraag indienen voor tijdelijke externe toegang. De externe toegang wordt alleen verleend voor de hybride laptop. Het team I&A beoordeelt de aanvraag. Een afwijzing wordt door het team gemotiveerd.
***= Externe toegang is toegang tot gemeentelijke informatiesystemen en diensten vanaf een locatie buiten de gemeentelijke kantoren. Dit kan de thuiswerkplek van een medewerker zijn, maar ook alle andere externe locaties vallen hieronder.
****= Medewerkers die geen Smartphone toegewezen krijgen, maar wel bereikbaar moeten zijn op een 088-nummer van de WODV kunnen op aanvraag een (tijdelijke) doorschakeling krijgen naar het eigen mobiele nummer of met een headset bellen vanaf de hybride laptop. De leidinggevende dient de aanvraag gemotiveerd in. Het team I&A beoordeelt de aanvraag. Een afwijzing wordt door het team gemotiveerd.
*****= Buitendienst medewerkers ontvangen een sim kaart. Deze kaart kan gebruikt worden in een eigen smartphone waarbij gebruik gemaakt kan worden van de beveiligde openbare (en apart gesegmenteerde) WiFi verbinding (zie ook par. 3.5)