TASKFORCE
Bestuur & Informatieveiligheid Dienstverlening

Mobiele gegevensdragers

Een operationeel product op basis van de Baseline Informatiebeveiliging Rijksdienst (BIR)

Rijksoverheid VNG Vereniging van Nederlandse Gemeenten Interprovinciaal Overleg ip MANIFESTgroep UNIE VAN WATERSCHAPPEN

Colofon

Onderhavig operationeel product, behorende bij de Baseline Informatiebeveiliging Rijksdienst (BIR), is mogelijk gemaakt door de Taskforce Bestuur en Informatieveiligheid Dienstverlening (Taskforce BID). Het product is gebaseerd op het operationele product ‘Mobiele Gegevensdragers’ behorende bij de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). Dit product is ontwikkeld door de Informatiebeveiligingsdienst voor gemeenten (IBD).

Leeswijzer

Dit document is een van de operationele producten op basis van de Baseline Informatiebeveiliging Rijksdienst (BIR).

Doel

Dit document biedt een handreiking voor het veilig gebruik van mobiele gegevensdragers, zoals USB-sticks, door organisaties binnen de Rijksoverheid.

Doelgroep

Dit document is van belang voor de verantwoordelijke ICT-beheerder voor mobiele gegevensdragers en eindgebruikers van mobiele gegevensdragers.

Reikwijdte

Dit document heeft voornamelijk betrekking op de maatregelen 7.1.3, 9.1.3, 9.2.6, 10.7.1, 10.8.1, 10.10.1 en 13.1.1 van de Baseline Informatiebeveiliging Rijksdienst (BIR). Het document gaat in op personele, organisatorische en technische informatiebeveiligingsaspecten die organisaties binnen de Rijksoverheid dienen te overwegen in relatie tot mobiele gegevensdragers.

Relatie met overige producten

- Baseline Informatiebeveiliging Rijksdienst (BIR). Tactisch Normenkader (TNK)
- Voorschrift Informatiebeveiliging Rijksdienst (VIR:2007)
- Informatiebeveiligingsbeleid
- Dataclassificatie
- Encyptiebeleid
- Antimalwarebeleid
- Mobiele apparaten

Inhoudsopgave

1 Inleiding

Dit document biedt een handreiking voor het veilig gebruik van mobiele gegevensdragers, zoals USB-sticks, door organisaties binnen de Rijksoverheid. Onder mobiele gegevensdragers worden ook CD-ROM's, flash cards, smartphones en tablets begrepen. In de BIR worden in onder andere hoofdstuk 10.1.1 maatregelen benoemd met betrekking tot digitale media, onder meer opgeslagen op mobiele gegevensdragers.

Mobiele gegevensdragers worden gebruikt voor de transport van data. Er zijn steeds meer digitale apparaten die van dataopslag gebruik maken. Het aantal vormen en het gebruik van mobiele gegevensdragers nemen toe. De kans op verlies van een apparaat en daarmee het verlies van data wordt daardoor groter. De opslagcapaciteit neemt eveneens steeds meer toe. Bij verlies van de gegevensdrager is er potentieel een veel groter dataverlies dan voorheen. Mobiele gegevensdragers kunnen daarnaast een bron en een verspreider zijn van kwaadaardige software als virussen.

Deze handleiding gaat niet over Mobile Device Management, dat onder meer het op afstand distribueren van applicaties, data en configuratie instellingen betreft.

1.1 Mobiele gegevensdragers

USB-sticks worden veel gebruikt en daarmee nemen ook de risico's toe, zoals gegevens verlies en het introduceren van schadelijke software binnen een netwerk. Het gebruik van een USB-stick kan op zich handig zijn om informatie mee te nemen naar een andere organisatie of om een persoonlijke back-up te maken. Het is daarbij aan te raden om de regels rondom het gebruik van USB-sticks binnen de organisatie af te dwingen door een geautomatiseerde systeemoplossing, waarmee USB-sticks en de inhoud kunnen worden beheerd en waarmee ook alle USB-poorten op alle apparaten binnen de organisatie kunnen worden beheerd. Bij voorkeur worden alleen USB-sticks gebruikt die geadviseerd zijn door het Nationaal Bureau voor Verbindingsbeveiliging (NBV).[1]

Geheugenkaarten worden gebruikt in apparaten, zoals in digitale camera's, en steeds meer computers hebben de mogelijkheid om geheugenkaarten te lezen en te beschrijven. Waar het geheugenkaarten in smartphones betreft, kan binnen Mobile Device Management worden overwogen om het hele geheugenkaartje, of alleen die gebieden waar informatie van de organisatie op staat, te versleutelen.

1.2 Informatiebeveiliging

Het is aan de overheidsorganisatie in hoeverre de ingeschatte risico's van mobiele gegevensdragers als USB-sticks opwegen tegen de geboden functionaliteit. In ieder geval dienen er beleids- en gedragsregels te zijn beschreven die gebaseerd zijn op het informatiebeveiligingsbeleid van de organisatie.

Het gebruik van digitale media zoals USB-sticks en het risico van gegevensverlies en het introduceren van malware zou bij uitstek op de agenda moeten staan van bewustwordingscampagnes over informatiebeveiliging.

[1] https://www.aivd.nl/onderwerpen/infobeveiliging/beveiligingsproducte/goedgekeurde/

Het zakelijk gebruik van privé-USB-sticks zou niet door de organisatie moeten worden toegestaan. Te allen tijde dient een door de organisatie beheerde en versleutelde USB-stick te worden gebruikt om het risico op gegevensverlies of het introduceren van malware te verminderen.

Verlies of diefstal van een mobiele gegevensdrager met vertrouwelijke informatie moet direct als een beveiligingsincident worden gemeld. Afhankelijk van de aard van de informatie kunnen maatregelen worden getroffen. Deze melding moet minimaal altijd worden gedaan aan de CISO, of een andere verantwoordelijke medewerker voor informatiebeveiliging van de betreffende organisatie.

Zelf-startende USB-sticks moeten worden voorkomen.[2] USB-sticks moeten bij gebruik automatisch gescand worden op malware. Ingeleverde USB-sticks worden na inname gewist met een NBV goedgekeurd wisprogramma.

[2] https://www.aivd.nl/publish/pages/1475/beschermingtegenonveiligeusb-sticks.pdf

Bijlage: Mobiele gegevensdragers beleid <naam organisatie>

Beleidsuitgangspunten mobiele gegevensdragers van <naam organisatie>

Ten behoeve van de beveiliging van informatie op mobiele gegevensdragers is er beleid gericht op mobiele gegevensdragers. Het doel van dit beleid is te voorkomen dat onbevoegden toegang krijgen tot informatie op mobiele gegevensdragers waar zij geen kennis van behoren te nemen dan wel waarop zij informatie kunnen aanpassen.

De <naam organisatie> hanteert de volgende beleidsuitgangspunten en deze zijn ontleend aan de Baseline Informatiebeveiliging Rijksdienst:

Algemene punten

- Mobiele gegevensdragers worden geregistreerd en er wordt bijgehouden wie deze in gebruik heeft.
- Geregistreerde media met vertrouwelijke gegevens mogen alleen de organisatie verlaten na goedkeuring van de eigenaar.
- Het bewaren van mobiele gegevensdragers geschiedt overeenkomstig de eigenschappen van de media in een veilige omgeving.
- Mobiele gegevensdragers die gevoelige informatie bevatten, moet voldoen aan de NBV standaard.
- Procedures voor het beheer van mobiele gegevensdragers hebben minimaal aandacht voor het veilig verwijderen van informatie voordat de mobiele gegevensdrager de organisatie verlaat of in een ander proces gebruikt wordt.
- Als verwijderen van informatie van mobiele gegevensdragers door een derde partij gebeurt, dient er een controlemechanisme te zijn ingeregeld om te waarborgen dat media ook daadwerkelijk veilig gewist worden.
- Er mag alleen gebruik worden gemaakt van door de CISO aangewezen en geselecteerde bedrijven voor het verwijderen van informatie van media.
- Beschermingsmaatregelen worden opgesteld voor mobiele gegevensdragers tegen onbevoegde toegang, misbruik of het corrumperen tijdens transport buiten de fysieke begrenzing van de organisatie.

Mobiele gegevensdragers met geclassificeerde gegevens of persoonsgegevens

Mobiele gegevensdragers met geclassificeerde gegevens of persoonsgegevens dienen met extra zorg te worden behandeld. Deze aanvullende eisen dienen genomen te worden en terug te komen in procedures:

- De data moeten worden versleuteld op het niveau van de BIR.
- Bij voorkeur wordt de gegevensdrager door een koerier van de organisatie of een particuliere koerier aangetekend getransporteerd, waarbij een neutrale beschermende verpakking wordt gebruikt. Indien het om een magnetische gegevensdrager (bijvoorbeeld harddisk) gaat zijn maatregelen genomen om de data

te beschermen tegen magnetische invloeden. De koerier gaat bij voorkeur via de kortste weg. Dezelfde dag moet er terugmelding plaatsvinden door de ontvanger van de media.

- Indien er encryptie plaatsvindt, worden de sleutels via een ander kanaal verzonden en niet tegelijkertijd met de mobiele gegevensdrager. Dit kan bijvoorbeeld middels een SMS naar de contactpersoon.
- Een mobiele gegevensdrager die verloren raakt, dient altijd te worden gemeld als een beveiligingsincident aan de CISO.

Aldus vastgesteld door de directie van *[organisatie]* op *[datum],*

[Naam. Functie] [Naam. Functie]

_____ _____