Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Directie Dienstverlening, Regeldruk en informatiebeleid
Cluster Informatiebeleid
Basisvoorzieningen Overheid

Contactpersoon
Kim Schamp

T 070-4268269
kim.schamp@minbzk.nl

bijlage

Reactie op uitkomsten audit Beheervoorziening BSN

Bijlage nummer	1
Datum	6 september 2011
Ons Kenmerk	2011-2000282822

Aanleiding

De Rijksauditdienst heeft in 2010 in opdracht van BZK het onderzoek verricht naar de inrichting, de werking en de beveiliging van de beheervoorziening BSN.

Dit onderzoek is nu voor de eerste keer uitgevoerd. De Rijksauditdienst heeft hiervoor in afstemming met BZK een apart normenkader ontwikkeld. Met dit normenkader is het fundament gelegd voor het (herhaald) uitvoeren van het 3 jaarlijks onderzoek. De ervaringen van dit onderzoek zijn weer input voor het verbeteren van het normenkader

Het onderliggende rapport "Uitkomsten audit beheervoorziening BSN" is het resultaat van het eerste onderzoek.

Dit onderzoek geeft aan in hoeverre praktijk voldoet aan de eisen die de wet daaraan heeft gesteld. In het algemeen zijn er tijdens de audit geen ernstige afwijkingen vastgesteld.

Inhoudelijke reactie

Bijgaand treft u mijn reactie aan, op de uitkomsten van de audit op de beheervoorziening Burgerservicenummer (BvBSN). Per aanbeveling wordt een inhoudelijke reactie gegeven de opvolging ervan.

§ 3.3.2 Convenant DRI – agentschap BPR

Aanbeveling: Neem in het convenant tussen DRI en het agentschap BPR een afspraak op dat jaarlijks expliciet wordt gerapporteerd over de naleving van de Wabb waarbij ook rekening dient te worden gehouden met actuele juridische ontwikkelingen.

Aanbeveling: Draag binnen BPR zorg voor de adequate uitvoering van de afspraken in het convenant tussen DRI en BPR rondom rapportage. Uitbreiding van het convenant op basis van de voorgaande aanbeveling kan hieraan bijdragen. Ons inziens dient hierbij ook aandacht te worden besteed aan

organisatieculturele aspecten als openheid en transparantie

Reactie: Naast de al bestaande maatregelen worden deze aanbevelingen overgenomen en geïmplementeerd.

Actiehouders: DRI/BPR

§ 3.4.2 Volgordelijkheid en informatieloosheid

Aanbeveling: Onderzoek de wijze waarop rondom het punt van informatieloosheid en volgordelijkheid van het BSN de wet- en regelgeving en BvBSN met elkaar in overeenstemming kunnen worden gebracht. Betrek hier ook de Belastingdienst bij voor wat betreft de uitgave van sociaal-fiscaalnummers.

Reactie: De Wet algemene bepalingen burgerservicenummer (Wabb) schrijft in artikel 2 voor dat het BSN geen informatie over de persoon mag bevatten. In de Memorie van Toelichting is dat verder uitgelegd als 'informatieloos'.

De rijksauditdienst heeft geconstateerd dat het Burgerservicenummer niet volledig informatieloos is. Het geeft weliswaar geen directe informatie over de persoon, zoals naam, geslacht of leeftijd, maar wel geeft echter wel beperkte indirecte informatie. Voor kenners is het bijvoorbeeld herkenbaar of een BSN voor of na 26 november 2007 is uitgegeven. Ook is herkenbaar of een BSN na 26 november 2007 eerst door de Belastingdienst als een sociaal-fiscaalnummer is uitgegeven.

Zoals de auditers zelf in de rapportage hebben aangegeven zijn hierdoor geen belangrijke scenario's van misbruik door ontstaan.

Enkele overwegingen vanuit BZK:

- Deze beperkte informatie is een direct gevolg van de beleidskeuze om sofinummers die voor 26 november 2007 zijn uitgegeven op te waarderen naar een BSN en aan een niet-ingezetene na die datum een sofinummer te verstrekken.
- Alleen al aan de lengte van de cijferreeks en de 11-proef is af te leiden dat het om een BSN gaat. Kortom, een volledig informatieloos burgerservicenummer bestaat niet.
- Vervanging van de huidige BSN's is een kostbare zaak en introduceert veel afbreukrisico's die samenhangen met een conversie.

Het blijft echter wel een feit dat de wettekst (in letterlijke zin) niet overeenkomt met de praktijk. Deze horen met elkaar in lijn te zijn.

BZK/DRI zal daarom een impactanalyse uitvoeren, waarin naar de mogelijke oplossingen zal worden gezocht, waarvan vervolgens de impact zal worden bepaald, met als doel de wet- en regelgeving en de huidige praktijk in lijn met elkaar te brengen. Als onderdeel hiervan zal het CBP om haar zienswijze in

deze worden gevraagd.

Actiehouder: DRI

Aanbeveling: Verbeter de wijze waarop de toevalsgetallen worden gegenereerd die de basis vormen voor de huidige uitgifte van BSN's. Het advies is hierbij gebruik te maken van de expertise van het Nationaal Bureau voor Verbindingsbeveiliging (onderdeel Ministerie van BZK).

Reactie: Een nadere analyse met de NVB zal moeten uitwijzen of de bestaande nummergenerator aanpassing, dan wel vervanging behoeft. DRI zal hiertoe het initiatief nemen.

Actiehouder: DRI in afstemming met BPR

§ 3.4.3 Vastlegging informatie genereren BSN's

Aanbeveling: Breng de BvBSN voor wat betreft het gegeven 'datum waarop het nummer is aangemaakt' in overeenstemming met wet- en regelgeving.

Reactie: Het toevoegen van de datum waarop het nummer is aangemaakt is in principe herstelbaar, maar lastig realiseerbaar. DRI/BPR zal de mogelijkheden onderzoeken om wet- en regelgeving (i.c. het Logisch Ontwerp BSN) en de inrichting van de BvBSN met elkaar in lijn te brengen.

Actiehouders: BPR/DRI

§ 3.6.2 Aandachtspunten functioneel beheervoorziening BSN

Aanbeveling: Concretiseer de eis dat de Bv BSN niet mag worden aangesloten op internet. Onderzoek vervolgens of de IT-infrastructuur voor de BvBSN voldoende invulling geeft aan deze eis en onderneem indien noodzakelijk actie. Zet in ieder geval de voorgenomen opheffing van de Virtual Private Network (VPN) koppeling voor beheerdoeleinden door aangezien deze koppeling in ieder geval strijdig is met de norm.

Reactie: Het Logisch Ontwerp BSN en het IBP van de BvBSN wordt hiermee in lijn gebracht. Voor het correct en efficiënt kunnen uitvoeren van zowel functioneel- als applicatiebeheer, is op onderdelen een internetkoppeling onontbeerlijk. BPR heeft mitigerende maatregelen getroffen, welke zijn beschreven in het IBP van de BvBSN, om de risico's die samenhangen met de toegang tot het internet af te vangen.

Actiehouders: BPR in afstemming met DRI

Aanbeveling: Maak gebruik van kennis en bezit voor authenticatie van beheerders op de BvBSN. Stel verder een wachtwoordbeleid vast voor alle beheerders van de beheervoorziening, zoals bijvoorbeeld de gedwongen periodieke wijziging van

wachtwoorden en implementeer dit beleid. Maak hierbij gebruik van de mogelijkheden die standaard in de gebruikte IT-infrastructuur aanwezig zijn en kies redelijke waarden.

Reactie: Er zijn met betrekking tot de toegang tot de beheerterminals andersoortige fysieke maatregelen[1] geïmplementeerd. De onderzoekers refereren naar de wet- en regelgeving en noemen het invoeren van een securitytoken als een mogelijke oplossing. Dit zal worden gewogen tegen de huidige fysieke en organisatorische maatregelen die voorkomen dat onbevoegden toegang kunnen verkrijgen tot de BvBSN. De aanbeveling om het token- en wachtwoordbeleid aan te scherpen, zal worden bekeken. De wet- en regelgeving (lees IBP) wordt desgewenst hiermee in lijn gebracht.

Actiehouders: BPR in afstemming met DRI

Aanbeveling: Onderzoek de wijze waarop de bewaartermijnen voor logboeken en de langdurige opslag van de gegevens uit de logboeken in backup's met elkaar in overeenstemming kunnen worden gebracht.

Reactie: Aanbeveling wordt overgenomen en er zal een verkenning uitgevoerd worden.

Actiehouders: BPR in afstemming met DRI

§ 3.7.2 Informatiebeveiligingsplan

Aanbeveling: Stel als BPR een nieuw IBP BvBSN op waarin de Wabb en andere relevante regelgeving expliciet als uitgangspunt wordt gehanteerd en stel dit IBP formeel vast. In dit IBP dient een integraal overzicht te worden gegeven van het stelsel van maatregelen in en rondom de BvBSN. Hiervoor kan worden verwezen naar b.v. het handboek functioneel beheer, ontwerpdocumentatie van de BvBSN applicatie, werkinstructies, eventueel het IBP BPR, het huidige IBP BvBSN etc. Ook moet expliciet aandacht worden besteed aan maatregelen die worden getroffen om de toegang van medewerkers van de leverancier van buiten de EU tot de BvBSN te beperken. Vervolgens kan BPR vaststellen of het stelsel van maatregelen in voldoende mate de eisen afdekt

Reactie: De aanbeveling zal overgenomen worden en er zal een aparte verkenning uitgevoerd worden naar het functioneel- en applicatiebeheer.

Actiehouders: BPR voor 1 oktober 2011

§ 3.7.3 Toezicht en verantwoording

Aanbeveling: Evalueer en verbeter de wijze waarop het instrument assurance

[1] *Er wordt hier gerefereerd naar de dubbel uitgevoerde toegangsschil. Niet alleen de beheerterminals zijn beveiligd, maar ook de kamer van de functioneel beheerder en het gebouw zelf.*

	rapport voor de BvBSN wordt ingezet in samenhang met de uitvoering van de aanbeveling uit paragraaf 3.7.2. Wij maken hierbij de vergelijking met de Berichtendienst GBA waarbij jaarlijks een assurance rapport wordt verkregen dat zekerheid biedt over de aanwezigheid van het stelsel van maatregelen gedurende het volledige jaar en dat een bredere afbakening kent. In dit rapport wordt naast een uitgebreidere beoordeling van de beveiligingsmaatregelen ook een oordeel gegeven over een aantal belangrijke beheerprocessen.
Reactie:	Aanbeveling is reeds overgenomen en geïmplementeerd. In de jaarlijkse externe audit die eind juni wordt afgerond, is niet alleen gekeken naar opzet en bestaan van de beveiligingsmaatregelen maar tevens ook naar de werking van deze beveiligingsmaatregelen.
Actiehouders:	BPR in afstemming met DRI
Aanbeveling:	Ga door met het uitvoeren van een verbeterprogramma gericht op het wegnemen van de vastgestelde tekortkomingen.
Reactie:	Aanbeveling wordt overgenomen. BPR zal DRI over de vorderingen informeren.
Actiehouders:	BPR in afstemming met DRI
Aanbeveling:	Breng een duidelijke functiescheiding aan tussen de uitvoerende taken op het gebied van informatiebeveiliging (inclusief de aansturing hiervan door BPR bij Logica) en de controlerende taken op dit gebied zoals betrokkenheid van BPR bij de (de opdrachtformulering voor) het assurance rapport bij Logica.
Reactie:	Aanbeveling wordt overgenomen. BPR komt met een voorstel.
Actiehouders:	BPR in afstemming met DRI

§ 3.8.2 Aandachtspunt raadpleegfunctie beheervoorziening BSN

Aanbeveling:	Breng wet- en regelgeving en het gebruik van het gegeven 'Land vanwaar ingeschreven' met elkaar in overeenstemming.
Reactie:	Aanbeveling wordt overgenomen. Er zal onderzocht worden of, en zo ja hoe, de raadpleegfunctie kan worden aangepast.
Actiehouders:	DRI in afstemming met BPR