



BUREAU KETENINFORMATISERING
W E R K & I N K O M E N

Samenvattende rapportage van de beveiliging van de Gezamenlijke elektronische Voorzieningen Suwi

Inhoudsopgave

| | |
|---|----|
| Inhoudsopgave..... | 2 |
| Management samenvatting..... | 3 |
| Conclusies en aanbevelingen..... | 3 |
| Conclusies over de feitelijke situatie..... | 3 |
| Conclusies met betrekking tot het stelsel..... | 3 |
| Aanbevelingen..... | 4 |
| Opdracht..... | 5 |
| Verantwoordelijkheden..... | 5 |
| Doel en nut van de Samenvattende rapportage..... | 5 |
| Reikwijdte van de Samenvattende rapportage..... | 6 |
| Beperking betekenis van de Samenvattende rapportage..... | 6 |
| Totaaloverzicht..... | 7 |
| Bijzonderheden over de verantwoording over 2009..... | 7 |
| Toelichting op het totaaloverzicht..... | 7 |
| Analyse van de audits en van de inhoud van de tabellen..... | 8 |
| Kerncijfers..... | 9 |
| Arbeidsinspectie (AI)..... | 10 |
| BIBOB..... | 10 |
| Bureau Keteninformatisering Werk en Inkomen (BKWI)..... | 10 |
| College van Zorgverzekeringen (CVZ)..... | 11 |
| Gemeenten (GSD, I(G)SD, RSD, GBD)..... | 11 |
| Immigratie en Naturalisatiedienst (IND)..... | 11 |
| Inlichtingenbureau (IB)..... | 12 |
| Kunstenaars & Co (K&Co)..... | 13 |
| Sociale Verzekeringsbank (SVB)..... | 13 |
| Uitkeringsinstituut Werkgeversverzekeringen (UWV)..... | 13 |
| Document historie..... | 14 |

Management samenvatting

Deze Samenvattende rapportage van de beveiliging van de GeVS beoogt een totaalbeeld te verschaffen over de beveiliging van de GeVS als stelsel voor de uitwisseling van persoonsgegevens, dit ten behoeve van:

- SZW als eigenaar van de infrastructuur;
- de registratiehouders als eigenaar van de via de GeVS uitgewisselde gegevens;
- de aangesloten partijen ter bevestiging van het vertrouwen in dit stelsel voor gegevensuitwisseling.

Conclusies en aanbevelingen

Zowel het niveau van de beveiliging van de GeVS als de inzichtelijkheid ervan zijn in 2009 wederom verbeterd ten opzichte van het voorgaande jaar, maar voldoen nog niet aan alle gestelde eisen.

De conclusies zijn gebaseerd op de uitkomsten van de afzonderlijke onderzoeken, rekening houdend met:

- De schaalvergroting van de gegevensuitwisseling binnen de keten (meer aangesloten organisaties en meer uitgewisselde berichten); deze heeft, dankzij aanvullend getroffen maatregelen, het beveiligingsniveau niet negatief beïnvloed.
- De mens; deze vormt zoals algemeen bekend is - en zoals zichtbaar is in de rapportage van het BKWI onder het kopje "privacy" - een veel groter risico wat betreft informatiebeveiliging dan de techniek.

Conclusies over de feitelijke situatie

- Waar in voorgaande jaren de oorzaak van een aantal afwijkingen bij de afzonderlijke organisaties met extra ketenbrede aandacht en met ketenbrede maatregelen kon worden weggenomen of worden verminderd, moet de oorzaak van huidige afwijkingen meer vanuit de eigen organisatie opgepakt worden.
- De beveiliging bij uitbesteding van diensten is verbeterd; inzichtelijkheid of en in hoeverre de beveiliging aan alle eisen voldoet blijft lastig.
- Sommige partijen in het gemeentelijk veld - dit is niet herleidbaar vanuit de aangeleverde rapportages - testen ondanks ketenbrede afspraken met productiegegevens.
- Informatiebeveiliging heeft extra aandacht gekregen bij de gemeenten. Door het rapport van de IWI en de brief van de Staatssecretaris besteden gemeenten aandacht aan beveiligingsbeleid en beveiligingsplannen. Daarnaast - mede door de inspanningen van de accountmanagers van BKWI, IB en CP-ICT - is vanuit besef dat met de GeVS toch wel erg veel persoonsgegevens worden uitgewisseld privacy en het proces van interne controle bij veel gemeenten op de agenda gezet. Ook dit is niet zichtbaar in de aangeleverde rapportages, maar wel in de verzoeken die BKWI krijgt voor specifieke rapportages.

Conclusies met betrekking tot het stelsel

- Niet alle op de GeVS aangesloten organisaties verplicht zijn een rapportage aan te leveren. Daardoor geeft deze rapportage uitsluitend een beeld van beveiliging van de GeVS bij de organisaties die daartoe wel verplicht zijn en niet van de GeVS als geheel.
- Afwijkend van de ketenbrede en met SZW afgestemde afspraken heeft UWV eenzijdig met de IWI een afspraak gemaakt aangaande de verantwoording. UWV heeft de keten niet - via de geëigende kanalen, te weten de Domeingroep Privacy en Beveiliging en/of het Algemeen Ketenoverleg - geïnformeerd over deze afwijking. Daarbij rekening houdend dat de verantwoordingsrapportage (van UWV) niet slechts bedoeld is als verantwoording aan SZW en IWI, maar dat deze ook bedoeld is als verantwoording naar de registratiehouders waarvan gegevens worden ontvangen. In de afspraak tussen UWV en IWI zijn deze laatste partijen niet gekend.
- Het stelsel van procedures en maatregelen voor de beveiliging van de gegevensuitwisseling dient bij alle op de GeVS aangesloten organisaties aan het zelfde minimumniveau te voldoen. Niet alle organisaties zijn gehouden aan hetzelfde verantwoordingsregime en zodoende voldoet het stelsel voor de gegevensuitwisseling per definitie niet aantoonbaar aan de hieraan gestelde eisen. Positieve ontwikkeling hierbij is dat nieuw aangesloten partijen willen voldoen aan (Suwi-)eisen wat betreft verantwoording. Partijen willen echter een situatie waarbij de organisatie slechts "lastig

gevallen” wordt met een enkelvoudig onderzoek, waaruit - zo nodig - meerdere rapportages kan worden gegenereerd.

- Door het late aanleveren van de rapportages door de aangesloten organisaties is BKWI niet in staat geweest - conform de afspraken - de Samenvattende rapportage tijdig te verspreiden.
- Een kunstmatig onderscheid is gemaakt tussen de beveiliging van de gegevensuitwisseling en van de gegevensverwerking en tussen de beveiliging van de GeVS en van de eigen informatiehuishouding als totaal. Deze vier zaken zijn echter verweven en daarom is het reëel te stellen dat het gewenst is te komen tot een situatie waarbij aangesloten organisaties zich verantwoorden over de beveiliging van de informatiehuishouding als geheel en wel conform een generieke richtlijn en generiek normenkader, waarbij elke materiële afwijking, onder vermelding van de hieraan verbonden risico's en getroffen maatregelen, wordt benoemd.
- De gewijzigde wetgeving, de nieuwe visie aangaande verantwoording en het normenkader zijn (nog) niet verwerkt in de huidige Verantwoordingsrichtlijn. In verband met mogelijke impact op de verantwoording over 2010 is het van belang aanpassingen zo snel mogelijk vast te stellen en aan partijen te communiceren.

Aanbevelingen

Het verdient aanbeveling:

- Te borgen dat alle aangesloten organisaties BKWI tijdig die informatie verstrekt welke nodig is voor het samenstellen van de Samenvattende rapportage van de beveiliging van de GeVS als geheel.
- Te borgen dat afspraken over het afwijken, wat betreft ketenbrede afspraken of verplichtingen, in de daarvoor bestemde gremia worden behandeld.
- Dat de aangesloten organisaties die geen rapportage hebben aangeleverd dit in het vervolg wel gaan doen, opdat met de Samenvattende rapportage een beeld kan worden gegeven van de GeVS als totaal, ter bevestiging van het onderlinge vertrouwen en van het vertrouwen van de registratiehouders in relatie tot de door hen verstrekte gegevens.
- Centraal een voldoende grote set met bruikbare testgevallen beschikbaar te stellen, die door elke aangesloten organisatie kan worden gebruikt.
- De Verantwoordingsrichtlijn zodanig aan te passen, dat partijen niet geconfronteerd worden met meerdere onderzoeken, maar kunnen volstaan met een enkelvoudig onderzoek dat voldoende zekerheid biedt aan alle verantwoordelijken (inclusief de registratiehouders).

Achtergrond van de Samenvattende rapportage

Opdracht

Ingevolge artikel 6.4 Regeling SUWI d.d. 21 december 2001 is de Security Officer van het BKWI verplicht om jaarlijks, ten behoeve van SZW en de IWI, een totaaloverzicht samen te stellen over de beveiliging van de gegevensuitwisseling via de GeVS. Daarnaast voorziet deze Samenvattende rapportage de registratiehouders van informatie over de beveiliging van de GeVS als “veilig” instrument voor het uitwisselen van gegevens.

Het begrip ‘beveiliging’ is nader gepreciseerd met de onderstaande kwaliteitscriteria:

- beschikbaarheid: de mate waarin de bedrijfsprocessen voor het beheer van de GeVS en de koppelvlakken gericht op de gegevensuitwisseling, ongestoord voortgang kunnen vinden.
- exclusiviteit: de mate waarin de toegang tot de gegevensuitwisseling via de GeVS en de koppelvlakken en de kennisname van de informatie daarin, is beperkt tot een gedefinieerde groep van gerechtigden.
- integriteit: de mate waarin de gegevensuitwisseling via de GeVS en in het koppelvlak zonder fouten is.
- controleerbaarheid: de mate waarin door de mens kan worden vastgesteld dat de bedrijfsprocessen gericht op de gegevensuitwisseling via de GeVS en het koppelvlak tot het beoogde resultaat hebben geleid.

Verantwoordelijkheden

Het management van de afzonderlijke Suwi-organisaties en het BKWI zijn elk zelf verantwoordelijk voor de beveiliging van de eigen delen van de GeVS. De beveiliging van de gegevensuitwisseling via de GeVS is ingericht en wordt beoordeeld conform de vigerende versie van het Suwinet-Normenkader¹.

Ook zijn zij elk zelf verantwoordelijk voor de inhoud van de eigen jaarlijkse rapportage aan de Minister van SZW, aan de IWI en aan de registratiehouders van wie zij persoonsgegevens raadplegen. Voor zover hieraan gehouden, verantwoorden zij zich conform de vigerende versie van de Verantwoordingsrichtlijn, waarmee de resultaten in de afzonderlijke rapportages op elkaar aansluiten.

Het staat het management van de aangesloten organisaties vrij te kiezen of zij in haar jaarverslag verantwoording aflegt over de informatiebeveiliging via het oordeel van een geregistreerde edp-auditor (over de beveiliging van - de eigen delen van - de GeVS) of dat zij dit zelf doet in de mededeling bedrijfsvoering².

De edp-auditor/accountant van elk van deze organisaties is verantwoordelijk voor:

- het oordeel over de mate waarin de verantwoording van het management getrouw weergeeft in hoeverre is voldaan aan de vastgestelde normenkaders en gemaakte afspraken betreffende de beveiliging van de gegevensuitwisseling (conform artikel 6.4 Regeling Suwi)

of

- het oordeel over de beveiliging van - de eigen delen van - de GeVS van de beoordeelde organisatie.

De Security Officers van de afzonderlijke organisaties brengen (de publieke versie van) de verantwoording van hun organisatie in de DPB. De publieke versies dienen de garantie te bevatten dat deze correspondeert met de onderliggende auditrapporten.

De Security Officer van het BKWI stelt op basis van (de publieke versies van) de rapportages van de afzonderlijke organisaties (over de beveiliging van de gegevensuitwisseling via de GeVS) - een Samenvattende rapportage samen.

In overleg met de DPB formuleert de Security Officer van het BKWI conclusies en aanbevelingen over de beveiliging van de GeVS als geheel.

De Security Officer van het BKWI en de DPB zijn niet verantwoordelijk voor de beoordeling van de juistheid van de publieke rapportages of voor het oordeel in hoeverre de beveiliging aan de gestelde eisen voldoet; dit valt onder de verantwoordelijkheid van de IWI.

Doel en nut van de Samenvattende rapportage

Deze Samenvattende rapportage van de beveiliging van de GeVS beoogt de minister, de IWI, de registratiehouders en de aangesloten organisaties, respectievelijk als verantwoordelijke,

¹ Bijlage bij de Verantwoordingsrichtlijn voor de edp-audit van de beveiliging van Suwinet.

² In dit laatste geval dient dit vergezeld te gaan van een oordeel/verklaring van getrouwheid van een geregistreerde auditor.

toezichthouder en/of belanghebbenden, een totaalbeeld te tonen van het gehele stelsel van maatregelen en procedures ter bescherming van de privacy en de beveiliging van de GeVS. Dit totaalbeeld dient de beoordeling te ondersteunen of alle risico's zijn afgedekt en of met de besteding van geld en inspanningen de gewenste reductie van risico's is bereikt. In overeenstemming met de rol en taken van het BKWI wordt de minister - door middel van evaluatie van inhoud en toepassing van het beveiligingsbeleid - aldus ondersteund in zijn regelgevende verantwoordelijkheid. Tegelijkertijd biedt een totaalbeeld registratiehouders een indicatie over de beveiliging van de verstrekte gegevens.

Reikwijdte van de Samenvattende rapportage

In de Samenvattende rapportage wordt een beeld gegeven van de beveiliging van het stelsel voor gegevensuitwisseling via de GeVS, conform Art. 6.4 Regeling SUWI. In dit beeld is niet opgenomen een beeld van de beveiliging van de gegevensverwerking, conform Art. 5.22 Regeling SUWI³. Ook bevat de rapportage geen informatie over de beveiliging van die delen van de GeVS waarover de Security Officer van het BKWI geen informatie heeft ontvangen, zoals van de gemeenten.

Gemeenten zijn niet gehouden verantwoording af te leggen aan de minister van SZW en wettelijk niet verplicht om aan [de Security Officer van] het BKWI te rapporteren en geven derhalve geen inzage in de mate waarin zij aan de gestelde eisen voldoen. De organisaties welke niet aan BKWI rapporteren vormen ca. 46% van het totaal aantal gebruikers van de GeVS, zodat het maar de vraag is in hoeverre de informatie in deze Samenvattende rapportage een reële weergave is van de beveiliging van de GeVS als geheel en in wezen wordt BKWI belemmerd in het uitvoeren van haar wettelijke taak wat betreft het samenstellen van een totaaloverzicht van de beveiliging van de GeVS als geheel en voldoet de Samenvattende rapportage in feite niet aan het gestelde doel.

Beperking betekenis van de Samenvattende rapportage

In het jaarverslag van de betrokken organisaties wordt verslag gedaan over de gehele informatiebeveiliging, zowel over de gegevensuitwisseling als over de gegevensverwerking. In de beveiligingsparagraaf, opgenomen in het managementstatement van het Jaarverslag doet het management verslag van:

- alle materiële afwijkingen aangaande de beveiliging van de eigen delen van de GeVS;
- de daarbij gelopen risico's;
- de daarop getroffen maatregelen.

Deze Samenvattende rapportage bevat geen informatie over:

- de beveiliging van de gegevensverwerking;
- de beveiliging van de gegevensuitwisseling via die delen van de GeVS, welke onder de verantwoordelijkheid vallen van organisaties die hierover niet aan het BKWI rapporteren;
- de beveiliging van de gegevensuitwisseling via de applicatiekoppelingen waarmee gegevens via de GeVS uitgewisseld worden;
- getroffen maatregelen of procedures.

In de rapportage wordt zo veel mogelijk getracht een vergelijk mogelijk te maken; zo worden de huidige bevindingen naast de bevindingen van het voorgaande jaar gepresenteerd. De Verantwoordingsrichtlijn en het bijbehorende Suwinet-Normenkader worden jaarlijks geëvalueerd, waardoor bij wijziging van richtlijn of normen, de grondslag van de beoordeling (de normen) aangaande het "voldoen aan de norm" over de verschillende jaren niet per definitie gelijk hoeven te zijn.

De rapportage biedt alleen een betrouwbaar en bruikbaar beeld wanneer alle aangesloten organisaties zich - op vergelijkbare wijze - over hun deel van de beveiliging verantwoorden. Aangezien deze Samenvattende rapportage is samengesteld uit een beperkt aantal rapportages heeft informatie in deze rapportage slechts beperkte betekenis. De betekenis van onderstaande conclusie moet dan ook - rekening houdend met deze beperking - worden gelezen.

³ De verantwoording van de verwerking van de via de GeVS uitgewisselde gegevens vindt plaats in de eigen reguliere verantwoording van de afzonderlijke organisaties.

Totaaloverzicht

Bijzonderheden over de verantwoording over 2009

Voor de verantwoording over het jaar 2009 is versie 2.0 van de Verantwoordingsrichtlijn gebruikt en gelijk aan 2008 vindt verantwoording plaats conform een Addendum op de Verantwoordingsrichtlijn, welke in overleg tussen de Suwi-partijen, SZW, de IWI en door het Algemeen Ketenoverleg is vastgesteld⁴.

De beoordeling van de werking van het stelsel van procedures en maatregelen van de GeVS vond voor het eerst plaats in 2005. Hierbij moet worden opgemerkt dat eenduidige richtlijnen voor het ketenbreed beoordelen van de werking van procedures en maatregelen nog niet bestonden. De NOREA⁵ heeft hiervoor wel een handreiking opgesteld.

De auditors van de Suwi-organisaties hebben in overleg met de IWI een werkprogramma opgesteld voor het beoordelen van de werking van het Suwinet-Normenkader. Om tot een zoveel mogelijk gelijkwaardige werkwijze te komen hebben de auditors de door hen te hanteren werkprogramma's uitgewisseld en deze afgestemd wat betreft reikwijdte en diepgang.

Toelichting op het totaaloverzicht

Zoals uit deze rapportage is op te maken heeft niet elke aangesloten organisatie een rapportage aangeleverd, ook heeft een enkele partij niet alle normen beoordeeld.

Niet in alle gevallen is tegelijk met het aanleveren van de rapportage het oordeel (van getrouwheid) van de auditor meegestuurd.

Als gevolg hiervan is de juistheid van de aangeleverde informatie niet beoordeeld.

De informatie in de Samenvattende rapportage van de beveiliging van de GeVS over 2009 is gebaseerd op - zover aangeleverd - de rapportages van de volgende organisaties:

| | | |
|-----------------------------|--|--|
| AI & SIOD | Arbeidsinspectie en Sociale Inlichtingen en Opsporingsdienst | De gezamenlijke rapportage van AI en SIOD is verwerkt. |
| BIBOB | | Geen rapportage ontvangen |
| BKWI | Bureau Keteninformatisering Werk en Inkomen | De rapportage van BKWI is verwerkt. |
| CVZ | College van Zorgverzekeringen | Per eind 2009 is CVZ aangesloten en zal per 2010 verantwoording afleggen. |
| GSD GBD I(G)SG RSD | Gemeentelijke sociale diensten Gemeentelijke belastingdeurwaarders Inter(gemeentelijke) sociale diensten Regionale sociale diensten | Per eind 2009 zijn (in het kader van een pilot) 5 GBD'en aangesloten, deze zullen per 2010 verantwoording afleggen. Met de IGSD'en, de ISD'en en RSD'en zijn geen afspraken gemaakt wat betreft verantwoording. |
| IB | Stichting het Inlichtingenbureau | De rapportage van het IB is verwerkt. |
| IND | Immigratie en Naturalisatiedienst | De rapportage van de IND is verwerkt. |
| IVT | Landelijke Interventieteams | De Interventieteams leggen verantwoording af via de verantwoordingsrapportage van de eigen organisatie. Met de Belastingdienst zijn geen afspraken gemaakt wat betreft verantwoording. |
| K&Co | Kunstenaars en Co | Geen rapportage ontvangen |
| SVB | Sociale Verzekeringsbank | De rapportage van SVB is verwerkt. |
| UWV | Uitkeringsinstituut Werknemersverzekeringen | De verantwoording van de UWV omvat ook het UWV WERKbedrijf (het voormalige CWI) en is verwerkt. |

Aangesloten partijen per 2009

⁴ Deze is vastgesteld per d.d. 11 augustus 2009.

⁵ NOREA is de beroepsorganisatie voor ICT-auditors.

De volgende tabel toont - over de situatie in 2009 - per organisatie de beoordeling van "opzet, bestaan en werking" voor de verschillende aandachtsgebieden van het stelsel van procedures en maatregelen.

| Org | Aandachtsgebied | | | | | | | | | | | | | | | | | | | | | |
|-----------------|-----------------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 |
| AI/SIOD | P | P | P | P | P | NT | NT | P | P | NT | NT | P | P | P | P | NT | NT | NT | P | P | P | P |
| BIBOB | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA |
| BKWI | P | P | P | B | B | B | P | B | P | B | B | P | P | B | B | P | P | B | P | P | P | B |
| CVZ | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA |
| GBD | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA |
| GSD'en | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA |
| IB ⁶ | P | B | P | B | P | P | B | P | P | B | P | P | F | P | P | NT | NT | NT | NT | F | B | B |
| IND | B | B | P | P | P | P | P | P | P | P | P | P | P | P | P | NT | NT | NT | P | P | P | P |
| IVT | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA |
| K&co | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA |
| SVB | P | P | P | P | P | P | P | P | P | P | P | P | P | P | P | NT | NT | NT | P | B | P | P |
| UWV | NB | NB | NB | P | P | P | P | B | P | P | P | NB | NB | NB | NB | NB | NB | NB | NB | NB | NB | NB |

Resultaten over 2009

| | |
|----|--|
| P | Voor dit aspect van de beveiliging zijn voldoende effectieve procedures en maatregelen getroffen. |
| B | Voor dit aspect van de beveiliging zijn getroffen procedures en maatregelen maar gedeeltelijk geïmplementeerd. |
| F | Voor dit aspect van de beveiliging zijn geen of vrijwel geen procedures en maatregelen getroffen. |
| NA | Voor dit aspect van de beveiliging is geen informatie beschikbaar gesteld voor deze rapportage. |
| NB | Voor dit aspect van de beveiliging is niet beoordeeld. |
| NT | Voor dit aspect van de beveiliging is niet van toepassing. |

Legenda

Ter vergelijking toont de volgende tabel de situatie in 2008.

In de tabel voor 2009 zijn de nieuwe partijen toegevoegd. Van BIBOB, de Gemeentelijke Belastingdeurwaarders, en CVZ is wel al deels informatie aangeleverd, maar deze rapportage is nog niet vergelijkbaar en is niet in de huidige Samenvattende rapportage opgenomen. De rode vlakken zijn nog niet allemaal verdwenen. Hierbij moet in acht genomen worden dat het inlichtingenbureau over 2009 een conceptrapportage heeft aangeleverd. De definitieve rapportage kan aangaande deze aspecten wijzigen.

| Org | Aandachtsgebied | | | | | | | | | | | | | | | | | | | | | |
|---------|-----------------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 |
| AI/SIOD | P | P | NT | P | NT | NT | NT | P | P | NT | NT | P | P | P | P | NT | NT | NT | P | P | P | P |
| BKWI | P | P | B | B | B | B | P | B | P | F | B | P | P | P | P | B | P | P | P | P | P | P |
| GSD'en | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA |
| IB | P | F | P | P | P | P | B | F | F | B | F | P | F | P | P | NT | NT | NT | NT | B | P | P |
| IND | B | B | P | P | P | P | P | P | P | P | P | P | P | P | P | NT | NT | NT | P | P | P | P |
| K&co | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA |
| SVB | P | P | P | P | P | P | P | P | P | P | P | P | P | P | P | NT | NT | NT | P | B | P | P |
| UWV | P | P | P | P | P | P | P | P | P | NT | NT | P | P | P | P | P | P | P | P | B | P | P |
| CWI | P | P | P | P | P | P | P | B | P | P | B | P | B | P | P | P | P | P | P | P | P | P |

Resultaten over 2008

De bovenstaande tabellen bevatten per organisatie de samenvatting van de edp-auditor over de beveiliging van de afzonderlijke aandachtgebieden⁷. De bevindingen zijn samengevat via een kleurencode welke is bepaald aan de hand van de uitkomsten van de beoordeling van de individuele normen waaruit een onderwerp is samengesteld en is mede gebaseerd op het professional judgment van de edp-auditor. Deze bevindingen vormen een element bij de oordeelsvorming door de edp-auditor

Analyse van de audits en van de inhoud van de tabellen

Informatiebeveiliging kan slechts dan effectief en efficiënt zijn wanneer alle procedures en maatregelen van alle aangesloten organisaties gezamenlijk voldoende bescherming bieden. Niet alle aangesloten organisaties zijn echter onderworpen aan het verantwoordingsregime (van de GeVS).

⁶Het Inlichtingenbureau heeft een conceptversie aangeleverd.

Het is alleszins logisch te verlangen dat alle aangesloten organisaties input leveren voor een Samenvattende rapportage, opdat daarmee een totaaloverzicht samengesteld kan worden van de beveiliging van het stelsel van gegevensuitwisseling als geheel. Dit overzicht is immers van belang voor alle op de GeVS aangesloten organisaties, maar in het bijzonder voor de registratiehouders van wie de gegevens worden geraadpleegd en voor SZW als eigenaar van de infrastructuur.

Aangezien niet alle aangesloten partijen input hebben geleverd heeft deze rapportage en (hebben de conclusies) maar zeer beperkte nut of waarde.

De vraag of de ingezette middelen om in deze rapportage te voorzien wel in verhouding staan tot het beoogde doel is daarmee gerechtvaardigd.

Kerncijfers

Onderstaande tabel toont een aantal kerncijfers over het gebruik van de GeVS.

| | 2009 | 2008 |
|--|--------------|--------------|
| Aangesloten organisaties ⁷ | 384 | 372 |
| Aangesloten bronnen | 14 | 11 |
| Gebruikersaccounts Suwinet-Inkijk | 50.626 | 43.695 |
| Gebruikte overzichtspagina's | 33 | 26 |
| Gebruikte rollen (differentiatie van gebruikersgroepen) | 107 | 102 |
| Gebruikte accounts | 50.626 | 43.695 |
| Uitgewisselde berichten via Suwinet-Inkijk (gestructureerde berichten) | 36.661.773 | 37580742 |
| Uitgewisselde berichten via Suwinet-Inlezen (gestructureerde berichten via applicatiekoppeling) | Niet gemeten | Niet gemeten |
| Uitgewisselde berichten via Suwinet-Melding (gestructureerde berichten) | Niet gemeten | 490.802 |
| Uitgewisselde berichten via Suwinet-Mail (ongestructureerde berichten) | 1.270.922 | 1.749.333 |

Overzicht van behaalde resultaten

Onderstaande tabel toont aantallen en percentages accounts voor Suwinet-Inkijk

| Organisatie | 2009 | | 2008 | |
|---------------------------|--------|---------|--------|---------|
| | Aantal | Pct. | Aantal | Pct. |
| AI | 256 | 0,51% | 239 | 0,60% |
| BIBOB | 36 | 0,07% | | |
| BKWI | 48 | 0,09% | 64 | 0,16% |
| CVZ* | 15 | 0,03% | | |
| GBD* | 50 | 0,10% | | |
| GSD'en | 22.873 | 45,18% | 18.694 | 46,57% |
| IB | 8 | 0,02% | 10 | 0,02% |
| IND | 131 | 0,26% | | |
| IVT ⁸ | 187 | 0,37% | | |
| K&co | 11 | 0,02% | | |
| SIOD | 147 | 0,29% | 89 | 0,22% |
| SVB | 2.153 | 4,25% | 236 | 0,59% |
| UWV | 18.997 | 37,52% | 16.674 | 41,54% |
| UWVWb | 4.714 | 9,19% | 4.135 | 10,30% |
| Aantal gebruikers, totaal | 50.626 | 100,00% | 40.141 | 100,00% |

Totaaloverzicht Suwinet-Inkijk van de afzonderlijke organisaties⁹

⁷ Verscheidene gemeenten hebben een gezamenlijke aansluiting binnen een samenwerkingsverband.

⁸ Verantwoording over informatiebeveiliging van de Interventieteams vindt plaats vanuit de organisaties van de binnen deze teams opererende personen.

⁹ Het aantal gebruikers is inclusief de beheersaccounts.

Overzicht van de verantwoording

De op de GeVS aangesloten partijen leggen op basis van Art. 6.4 Regeling Suwi jaarlijks verantwoording af over de beveiliging van de gegevensuitwisseling via de GeVS en op basis van Art. 5.22 Regeling Suwi over de beveiliging van de gegevensverwerking.

Dit hoofdstuk bevat per organisatie het managementstatement uit het jaarverslag of het oordeel van de beveiliging over 2009.

Arbeidsinspectie (AI)

Informatiebeveiliging (Regeling Suwi, artikelen 5.22 en 6.4)

Gedurende 2008 hebben Arbeidsinspectie en SIOD gebruik gemaakt van SUWI inkijk.

SIOD en Arbeidsinspectie dragen zorg voor een adequaat niveau van informatiebeveiliging conform de vastgestelde normen VIR 2007, en WBP. Het aspect informatiebeveiliging wordt meegenomen in alle projecten en bij alle reguliere wijzigingen.

SIOD en Arbeidsinspectie hebben een Veiligheidsofficier /Security Officer in dienst die periodiek vaststelt of aan alle vastgelegde beveiligingseisen wordt voldaan.

De rapportage over de beveiliging van Suwinet beoogt een totaalbeeld te verschaffen over het betrouwbaarheidsniveau van de gegevensverwerking Suwi, gebaseerd op de interne controle- en beheersmaatregelen.

Hierbij verklaren ondergetekenden dat de rapportage over de beveiliging van Suwinet een getrouw beeld geeft. Daarmee wordt recht gedaan aan de artikelen 5.22 en 6.4 van de Regeling Suwi.

BIBOB

Van BIBOB is geen rapportage ontvangen.

Bureau Keteninformatisering Werk en Inkomen (BKWI)

4.3 Beveiliging en beveiligingsincidenten

Privacy

Tijdens het weekeinde rond Koninginnedag is bij BKWI een opvallende hoeveelheid netwerkverkeer opgevallen. Dit verkeer betrof (het raadplegen in) Suwinet-Inkijk. Vanuit het vermoeden dat zeker een deel van de raadplegingen onrechtmatig zouden zijn, zijn de betrokken organisaties aangeschreven met de bevindingen uit een eerste inventarisatie. Vanuit de betrokken organisaties is teruggemeld dat - nagenoeg in alle gevallen - sprake was van onrechtmatig handelen en dat hierop passende maatregelen zijn getroffen. Gezien het grote aantal personen dat via Suwinet persoonsgegevens kunnen raadplegen is het aannemelijk dat oneigenlijk/onrechtmatig gebruik - in casu van Suwinet-Inkijk - vaker plaatsvindt dan alleen in de onderzochte gevallen.

Gezien dit risico heeft BKWI extra aandacht besteed aan de volgende maatregelen:

- de aangesloten partijen gewezen op het interne controleproces;
- de interne controleprocessen ondersteund met specifieke rapportages, waarmee oneigenlijk gebruik zichtbaar gemaakt kan worden;
- een filter ontwikkeld als aanzet dat partijen of organisatieonderdelen slechts BSN's (en daarmee de persoonsgegevens) van hun doelgroep kunnen raadplegen.

Met het Inlichtingenbureau en CP-ICT zijn nadere afspraken gemaakt over de ondersteuning van gemeenten aangaande de informatiebeveiliging en over het interne controleproces.

*** Organisatie van de beveiliging**

Geconstateerd is dat een deel van de procedures verouderd zijn en dat van procedures afgeweken wordt. Eind eerste helft van 2010 worden alle procedures opnieuw beoordeeld en zo nodig aangepast.

*** Dienstenniveaubeheer**

Ondanks alle zorg en aandacht blijven afspraken met leveranciers vaak een zorg en punt van aandacht. Uit de TPM-verklaring van een van onze leveranciers blijkt dat deze niet aan alle normen heeft voldaan. BKWI zal de leverancier hierop aanspreken.

*** Rapportages en verantwoording**

De technische problemen met het leveren van gebruiksrapportages Suwinet zijn opgelost.

Toch zijn in de eerste helft van 2009 niet alle rapportages op tijd verspreid.

Inhoud en betrouwbaarheid van de rapportages en de verspreiding zijn met de extra aandacht die hieraan besteed is verbeterd, er bestaat echter nog steeds ruimte voor verbetering wat in 2010 meer vorm zal krijgen. Ook zijn latente gebruikerswensen ten aanzien van de

rapportages geïnventariseerd en gehonoreerd. Ook in 2010 blijft het rapportageproces onder verhoogde dijkbewaking.

*** Incidenten en problemen**

De volledigheid van de incidenten registratie - en daarmee ook de rapportage over incidenten - is voor verbetering vatbaar. Hier wordt in 2010 extra aandacht aan besteed.

*** Ketenbrede wijzigingen**

Niet alle wijzigingen met impact op andere dan de eigen organisatie werden in 2009 gemeld aan het CMK, waardoor coördinatie en implementatie werden bemoeilijkt.

Per december 2009 wordt een deel van deze wijzigingen ook gemeld aan het CMK, het overige deel wordt ter kennisname opgenomen in de releasedocumentatie, zodat bij de ketenpartners een totaalbeeld ontstaat van de alle ketenbrede wijzigingen.

Met het doorvoeren van wijzigingen werd niet altijd rekening gehouden met de rapportages, waardoor deze verstoord konden worden en wat uiteindelijk leidde tot een incident in de rapportages. Eind 2009 is een coördinator Rapportages aangesteld, hiermee moet het issue uit 2009 in 2010 opgelost zijn.

De documentatie rondom het testen gaat weliswaar beter, echter zijn nog steeds verdere verbeteringen mogelijk. In 2010 wordt extra aandacht besteed aan het structureel maken van de verbeteringen.

*** Kantoorautomatisering/werkplekken**

Op basis van een business-case worden alle werkstations, zowel die van UWV als die van BKWI zelf, vervangen door iMacs en wordt een geheel nieuwe kantoorautomatiseringomgeving ingericht; tevens wordt zoveel mogelijk gebruik gemaakt van open software.

Bij de uitrol van de nieuwe machines was de beveiliging in eerste instantie nog niet optimaal ingericht, De benodigde maatregelen en procedures worden a tempo ingericht. Bij de overgang naar de nieuwe omgeving wordt een externe partij gevraagd een onderzoek uit te voeren naar aanwezige kwetsbaarheden. Komend jaar zullen, nadat alle documenten zijn overgezet naar de nieuwe kantoorautomatiseringomgeving en deze nieuwe omgeving is gestabiliseerd, de procedures en werkinstructies up-to-date gebracht worden en opnieuw ondergebracht worden in de Administratieve Organisatie.

College van Zorgverzekeringen (CVZ)

Van het College van Zorgverzekeringen is geen rapportage ontvangen.

Gemeenten (GSD, I(G)SD, RSD, GBD)

Van de (inter)gemeentelijke sociale diensten en regionale sociale diensten is geen rapportage ontvangen.

Immigratie en Naturalisatiedienst (IND)

Verklaring Suwinet 2009

Binnen de IND is het gebruik van en de autorisatie voor het instrument Suwinet-Inkijk momenteel toebedeeld aan medewerkers van de Directie Regulier, verspreid over verschillende locaties. De gegevensset in Suwinet-Inkijk wordt door deze IND medewerkers geraadpleegd ter verificatie van de door de klant reeds overgelegde gegevens en gebruikt als signaalmiddel bij de beoordeling van de aanvraag. In 2009 is de gegevensset herzien en is de doelbinding opnieuw aangegeven.

De door de Departementale Audit Dienst van Justitie in 2008 geconstateerde verbeterpunt rond het onvoldoende bekend met de afspraken rondom Suwinet bij sleutelrollen is opgepakt. Daarnaast is de ontvangst en verwerking van de logfiles rond het gebruik van Suwinet - Inkijk binnen de IND beter georganiseerd.

Het in de loggingbestanden weergegeven gebruik van de inkijkfunctie komt ruwweg overeen met het aantal aanvragen dat door de IND in behandeling wordt genomen waarbij aan het inkomensvereiste wordt getoetst. In bijzonder de aanvragen waarbij een natuurlijk persoon als referent optreedt. Daarmee bestaat op kwantitatief niveau geen indicatie van verkeerd of onterecht gebruik van de Suwinet - Inkijk. Omdat in het huidige informatiesysteem dat de IND gebruikt het BSN van de referent niet wordt geregistreerd, is inhoudelijke controle op juist gebruik middels de loggingfiles op dit moment niet te realiseren. In het nieuwe informatiesysteem van de IND (INDiGO) dat dit jaar in gebruik gaat worden genomen, wordt het BSN van de referent wel geregistreerd, waarmee inhoudelijke controle in de toekomst wel uitvoerbaar wordt.

Met de komst van INDiGO zal de toegang tot Suwinet-Inkijk worden geconcentreerd in de Centrale Verificatie Unit. Vanaf dat moment zullen alleen de medewerkers (naar verwachting circa vijftig) van deze unit toegang hebben tot de gegevens van Suwinet-Inkijk. Zij bedienen de rest van de organisatie op basis van het zogeheten "hit/no-hit"principe. Deze werkzaamheden zullen tijdelijk van aard zijn, tot het moment dat volledig geautomatiseerde gegevensuitwisseling kan plaatsvinden tussen het INDiGO en andere systemen. Het tijdspad waarbinnen dit gerealiseerd zal worden is mede afhankelijk van de ontwikkelingen van het stelsel van basisregisters.

Zoals eerder aangegeven beschouwt de IND de maatregelen rondom het gebruik van Suwinet-Inkijk als integraal onderdeel van haar informatiebeveiligings- en integriteitbeleid. Op dit moment voert de DAD een audit uit op het informatiebeveiligingsplan van de IND. Later in het jaar staat een departementale audit naar het integriteitsbeleid van de IND op de agenda. De I D heeft haar partners in de sociale keten, in het bijzonder UWV en BKWI, aangeboden inzage te verlenen in zowel het informatiebeveiligingsplan als de resultaten van de audits daarop. Dit in het kader van de professionalisering rond de integrale informatiebeveiliging van de keten.

Gelet op bovenstaande, het relatief gering aantal autorisaties door IND, de intensieve samenwerking tussen IND, BKWI en UWV in het afgelopen jaar, de onderhanden zijnde audit op de informatiebeveiliging van de IND en de noodzaak op kosten te besparen, heb ik besloten deze verklaring niet te laten vergezellen van een verklaring van getrouwheid afkomstig van een geregistreerd ED P auditor.

Inlichtingenbureau (IB)

De aangeleverde rapportage is nog een CONCEPTVERSIE.

1.1. Bedrijfsvoering

1.1.2 Beheersmaatregelen

Het Inlichtingenbureau kent een structuur waarbij de directeur en de afdelingsmanagers binnen een Management Team sturing geven aan de dagelijkse werkzaamheden en het bestuur van de Stichting de directeur controleert. Het ingerichte management control systeem geeft een gestructureerde basis voor de wijze van verantwoording afleggen over de afgesproken prestaties, de totale bedrijfsvoering en de mededeling over de bedrijfsvoering. Het management control systeem bevat onder meer de volgende onderdelen:

- Een door directie voorbereid en door bestuur vastgesteld jaarplan met begroting;*
- Releaseplanning en begroting;*
- Maand-, kwartaal- en (half)jaarverslagen;*
- Quality assurance beleid waarin MT-leden de inhoud van plannen en resultaten mede beoordelen;*
- Afdelingsgericht, projectgericht en beleidsgericht overleg;*
- Overleg met vertegenwoordigers van gemeenten (bestuur) en ketenpartners over doelen en resultaten van ketensamenwerking.*

1.1.7 ICT algemeen

Met betrekking tot het lopende contract met HP zijn in 2009 nieuwe werkafspraken gemaakt. Vanuit deze nieuwe werkafspraken is er in 2009 een aantal toetsmomenten geweest om problemen zoals deze zich in 2008 voordeden te voorkomen. Dit heeft zowel in kwaliteit als tijdige oplevering van nieuwe releases aanzienlijke verbeteringen opgeleverd. De operationele situatie met HP kan daardoor over 2009 gekenmerkt worden als stabiel. In 2009 hebben er zich twee lastige gevallen van storing voorgedaan in de KA voorziening. Beide verstoringen, met totaal verschillende oorzaken, waren aanleiding om het continuïteitsplan op dit punt opnieuw onder de loep te nemen. Dit heeft in de tweede helft van 2009 geleid tot een aanscherping van het continuïteitsbeleid van het IB. Daardoor wordt er sneller en effectiever geanticipeerd op verstoringen. De continuïteit van de bedrijfsvoering is daarmee nog beter gewaarborgd.

1.1.8 Opmenging bevindingen IWI

Naar aanleiding van het jaarverslag 2008 vroeg de IWI specifiek aandacht voor de (definities van de) prestatie-indicatoren. In de paragraaf hierboven werd hierop ingegaan. Een ander aandachtspunt van de IWI betrof de kwaliteit van de programmatuur in het sectorloket die in 2008 fors was teruggelopen. De kwaliteit is inmiddels weer op orde. In paragraaf 2.7 werd hier nader op ingegaan.

1.1.9 Betrouwbaarheid gegevensverwerking

In 2009 is - in samenwerking met de EDP auditors - het vigerende normenkader betrouwbare gegevensverwerking beoordeeld en aangepast. De controle op de aanlevering van bronnen gebeurde in 2009 op ad hoc basis en op basis van opmerkingen van gemeenten die aangaven dat gegevens van een bron ontbreken. Wel is per kwartaal gerapporteerd over het uitwisselen van gegevens via Rinis.

Deze werkwijze biedt onvoldoende waarborgen voor dat het tijdig aanleveren van informatie van bronnen. Om deze tekortkoming te repareren is in het informatiebeveiligingsplan van 2010 als maatregel opgenomen het periodiek uitvoeren van interne controles op volledigheid van aanleveren. Tevens zal er een werklijst "periodieke te controleren aanlevering" worden opgesteld als leidraad voor de uitvoerende medewerkers. Deze maatregelen zullen de (controle op) de uitvoering verder verbeteren.

Kunstenaars & Co (K&Co)

Van Kunstenaars & Co is geen rapportage ontvangen.

Sociale Verzekeringsbank (SVB)

1.1 Oordeel ex artikel 6.4 van de Regeling SUWI

Op grond van de uitgevoerde auditwerkzaamheden met betrekking tot de beveiliging van de gegevensuitwisseling via Suwinet door de SVB ben ik van oordeel, dat het stelsel van procedures en maatregelen, opgenomen in de onder het beheer van de SVB vallende bedrijfsprocessen in het koppelvlak gericht op de beveiliging van de gegevensuitwisseling via Suwinet, gedurende 2009 heeft voldaan aan de normen.

Uitkeringsinstituut Werkgeversverzekeringen (UWV)

1.ICT

1.1 Inleiding

UWV is voor haar bedrijfsvoering afhankelijk van de kwaliteit van de geautomatiseerde gegevensverwerking. UWV verantwoordt zich daarover in haar jaarverslag 2009 in paragraaf x.x en x.x en in de katern hoofdstuk xx en xx.

Volgens artikel 5.22 van de Regeling SUWI dient deze verantwoording vergezeld te worden van een oordeel en een rapport van bevindingen van een geregistreerd ICT-auditor.

De kwaliteit van de geautomatiseerde gegevensverwerking wordt in belangrijke mate bepaald door de kwaliteit van de beheersing- en beveiligingsmaatregelen bij de ICT- leveranciers van UWV. UWV is met deze ICT-leveranciers overeengekomen dat zij jaarlijks een Third Party Mededeling (TPM) dan wel SAS70-verklaring verstrekken. De TPM of SAS70 wordt afgegeven door een onafhankelijke partij, op basis van een uitgevoerde Third Party Audit (TPA) en bevat een oordeel over, respectievelijk een beschrijving van, de kwaliteit van de geleverde diensten. Wij hebben, volgens afspraak alle TPM's en SAS-70 verklaringen ontvangen. Voor ons oordeel maken wij, naast informatie uit de door ons uitgevoerde audits, gebruik van de ontvangen TPM's, SAS70-verklaringen en de verantwoording met betrekking tot de getroffen verbetermaatregelen over 2009.

1.2 Oordeel

Wij zijn van oordeel dat de verantwoording UWV een getrouw beeld geeft van de getroffen maatregelen en hun uitvoering en de nog te treffen maatregelen ter waarborging van de exclusiviteit, integriteit, beschikbaarheid en controleerbaarheid van de gegevensverwerking binnen UWV en de gegevensuitwisseling via SUWInet.

1.3 Belangrijkste aanvullende bevindingen

Zonder afbreuk te doen aan ons oordeel vermelden wij aanvullend onderstaand de belangrijkste bevindingen.

Wijzingenbeheer bij de leveranciers

De ontvangen TPM's en SAS70-verklaringen geven voldoende inzicht in de door de leveranciers getroffen en nog te treffen verbetermaatregelen. Een aantal leveranciers zal specifieke verbetermaatregelen treffen met betrekking tot het wijzingenbeheer.

Business continuity management

Ter zake de continuïteit van de ICT-voorzieningen hebben we vastgesteld dat met elke leverancier afspraken zijn gemaakt betreffende de te treffen ICT continuïteitsvoorzieningen. Met de overgang van het uitkeringssysteem UWV-1 naar het hoofdrekencentrum is de continuïteit van in ketens aan elkaar geschakelde applicaties een stap dichterbij gekomen.

Wij stellen vast dat de maatregelen ter zake de continuïteitsvoorzieningen van ICT meer in lijn zijn met de bedrijfscontinuïteit.

SUWInet

In 2008 hebben wij, in overleg met de Inspectie Werk en Inkomen, een cyclus opgesteld om eens in de drie jaar één van de volgende aspecten te beoordelen:

1. Organisatie en beveiliging;
2. Beheer;
3. Technische instellingen.

In lijn met voornoemde afspraak hebben we ons voor 2009 gericht op het onderdeel "2 Beheer". De getroffen maatregelen ter zake voldoen aan de daaraan te stellen eisen.

Polis+

In 2009 was er sprake van een incident. De foutieve levering is met alle betrokken partijen geëvalueerd en adequate maatregelen zijn getroffen. Bij de jaarlevering heeft een en ander succesvol gewerkt.

Tactisch beleid Beveiliging en Privacy

Sinds 2009 vormen de "werkpleinen" een onderdeel van UWV. Uit onderzoek is gebleken dat het open karakter van de werkpleinen niet in te passen is op alle onderdelen van het tactisch beleid Beveiliging en Privacy. Eind 2009 is een werkgroep geformeerd om dit beleid bij te stellen, rekening houdend met het specifieke karakter van de werkpleinen.

Document historie

| Datum en versienummer | | Auteur | Opmerking |
|-----------------------|-------------|-------------|--|
| 23 februari 2009 | Concept 0.1 | J.E.Breeman | Eerste versie |
| 1 maart 2009 | Concept 0.2 | J.E.Breeman | Verwerking van de publieke rapportages van de aangesloten organisaties |
| 15 maart 2009 | Concept 0.3 | J.E.Breeman | Verwerking van de reactie van de DPB en de directeur BKWI |
| 16 maart 2009 | Versie 1.0 | J.E.Breeman | Vastgesteld |