Doelbinding en beveiliging in de keten van werk en inkomen

De beveiliging van Suwinet en de privacy van de burger

Doelbinding en beveiliging in de keten van werk en inkomen

De beveiliging van Suwinet en de privacy van de burger

R06/01, januari 2006
ISSN 1383-8733
ISBN 90-5079-146-8

Voorwoord

Uitvoeringsorganisaties en gemeenten werken in de keten van werk en inkomen intensief met elkaar samen. Door middel van de elektronische voorziening Suwinet-Inkijk hebben ze de beschikking over de persoonsgegevens van miljoenen Nederlanders. Burgers moeten ervan op aan kunnen dat hun privacy daarbij voldoende gewaarborgd is.

De Inspectie Werk en Inkomen (IWI) heeft onderzoek gedaan naar de beveiliging van Suwinet-Inkijk. De inspectie heeft het onderzoek gericht op de privacyaspecten doelbinding en beveiliging.

Uitvoeringsorganisaties, en sinds de invoering van de Wet werk en bijstand (WWB) ook gemeenten, verantwoorden zich jaarlijks over de maatregelen die ze nemen om de beveiliging van Suwinet te waarborgen. De inspectie onderzoekt deze verantwoordingen en rapporteert in haar jaarverslag over haar bevindingen.
Met het onderzoek naar de waarborgen voor doelbinding en beveiliging wil de inspectie, in aanvulling op haar verantwoordingsgericht onderzoek, gericht het verband leggen tussen specifieke maatregelen die uitvoeringsorganisaties en gemeenten nemen en de daadwerkelijke waarborgen voor de privacy van de burger.
Dit rapport gaat onder meer in op relevante lopende ontwikkelingen in 2005. Het loopt daarmee vooruit op de verantwoordingen van uitvoeringsorganisaties en gemeenten over dit jaar.

Mr. L.H.J. Kokhuis
Inspecteur-generaal

Inhoud

1 Inleiding

De Inspectie Werk en Inkomen (IWI) heeft onderzoek gedaan naar de beveiliging van Suwinet-Inkijk. De elektronische voorziening Suwinet wordt binnen de keten van werk en inkomen gebruikt bij het uitwisselen van gegevens. Suwinet-Inkijk geeft medewerkers van ketenpartners de mogelijkheid om gegevens in te zien die afkomstig zijn uit gegevensverzamelingen van andere ketenpartners. Van de mogelijkheden die Suwinet biedt wordt Inkijk verreweg het meest gebruikt: eind 2004 hadden ruim 25.000 medewerkers van uitvoeringsorganisaties en gemeenten toegang tot Suwinet-Inkijk. Het grootschalige gebruik van een dergelijke voorziening vraagt goede waarborgen voor de privacy van de burger.

Doel van het onderzoek was om vast te stellen in hoeverre de beveiliging van Suwinet-Inkijk waarborgen biedt voor de privacy van de burger. Naast Suwinet-Inkijk beschikken uitvoeringsorganisaties en gemeenten over eigen geautomatiseerde systemen waarin ze gegevens verwerken. De beveiliging van die systemen is niet in het onderzoek betrokken. De inspectie heeft zich, bij het beantwoorden van de vraag naar de waarborgen voor de privacy van de burger, gericht op de privacyaspecten doelbinding en beveiliging.[1] Doelbinding houdt in dat persoonsgegevens alleen maar mogen worden gebruikt voor het doel waarvoor ze zijn verzameld. Beveiliging houdt in dat persoonsgegevens beschermd moeten worden tegen verstrekking aan personen of organisaties die daar geen recht op hebben.

1
De privacyaspecten 'doelbinding' en 'beveiliging' komen uit het Raamwerk Privacy Audit van het College Bescherming Persoonsgegevens. Dit 'raamwerk' vormt een vertaling van de Wet bescherming persoonsgegevens in concrete eisen aan informatiesystemen.

Het onderzoek richtte zich op de huidige gebruikers van Suwinet-Inkijk. Het gebruik van Suwinet-Inkijk door de Arbeidsinspectie en de Sociale Inlichtingen en Opsporingsdienst (SIOD), en op termijn mogelijk ook door reïntegratiebedrijven, is niet in het onderzoek betrokken. De Sociale Verzekeringsbank (SVB) voert dit jaar een proef uit met het gebruik van Suwinet-Inkijk. Aangezien het gebruik van Suwinet-Inkijk door de SVB nog geen onderdeel is van het reguliere proces, is ook het gebruik van Suwinet-Inkijk door de SVB niet bij het onderzoek betrokken. Ook initiatieven om fraude op te sporen door gegevens uit het sociale verzekeringsdomein te combineren met gegevens uit andere sectoren vallen buiten de reikwijdte van het onderzoek.

De inspectie heeft in dit onderzoek zo veel mogelijk gebruik gemaakt van verantwoordingen van uitvoeringsorganisaties en gemeenten, resultaten van eigen onderzoek van de uitvoeringsorganisaties, en andere reeds beschikbare informatie. Uitvoeringsorganisaties en gemeenten zijn zelf verantwoordelijk voor de beveiliging van (hun deel van) Suwinet. Ze verantwoorden zich jaarlijks over de beveiliging van Suwinet, en van de uitvoeringsorganisaties is ook veel informatie uit eigen onderzoek beschikbaar. De inspectie beoordeelt de verantwoordingen ieder jaar in haar verantwoordingsgericht onderzoek. De inspectie heeft verder gesprekken gevoerd met, onder meer, beveiligingsfunctionarissen en medewerkers die zijn belast met het afhandelen van klachten van burgers. Ook heeft de inspectie de relevante klachten geïnventariseerd die in 2004 en 2005 zijn behandeld door het College bescherming persoonsgegevens (CBP), de Nationale Ombudsman, het Ministerie van Sociale Zaken en Werkgelegenheid (SZW) en de inspectie zelf.

Het onderzoek is uitgevoerd in de tweede helft van 2005. De inspectie heeft de relevante ontwikkelingen uit 2005 zo veel mogelijk in het onderzoek betrokken. Als toetsingskader heeft de inspectie gebruik gemaakt van Bijlage XIV bij de Regeling SUWI. Bijlage XIV bevat de eisen aan de beveiliging van Suwinet.

2 Doelbinding en beveiliging vanuit de burger bezien

2.1 Doelbinding en beveiliging

Doelbinding en beveiliging maken deel uit van het recht op informationele privacy, op bescherming van de eigen persoonsgegevens. Doelbinding houdt in dat persoonsgegevens alleen maar mogen worden gebruikt voor het doel waarvoor ze zijn verzameld. Beveiliging betekent dat persoonsgegevens beschermd moeten worden tegen verstrekking aan personen of organisaties die daar geen recht op hebben.

2.2 Het perspectief van de burger

De burger krijgt met de keten van werk en inkomen te maken als hij zich, bijvoorbeeld, bij het Centrum Werk en Inkomen (CWI) meldt voor werk of voor een uitkeringsaanvraag. Om in aanmerking te komen voor arbeidsbemiddeling, reïntegratie of een uitkering verstrekt hij of zij gegevens aan uitvoeringsorganisatie of gemeente. Daarnaast verzamelen de uitvoeringsorganisaties gegevens die nodig zijn om het recht op uitkering vast te kunnen stellen, onder meer over het arbeidsverleden van de burger.
Burgers lopen risico's als deze gegevens, binnen of buiten de keten van werk en inkomen, worden gebruikt voor doelen waar ze niet voor bestemd zijn. Misbruik van loon- en uitkeringsgegevens zou er, bijvoorbeeld, toe kunnen leiden dat bijstandsgerechtigden problemen ondervinden bij het aanvragen van een subsidie of het afsluiten van een telefoonabonnement.
Misbruik van arbeidsgeschiktheidgegevens zou ertoe kunnen leiden dat mensen die (gedeeltelijk) arbeidsongeschikt zijn, of zijn geweest, belemmeringen ondervinden bij, bijvoorbeeld, het vinden van een nieuwe baan of het afsluiten van een arbeidsgeschiktheidverzekering.
Het is de vraag in hoeverre burgers misbruik van hun werk- en inkomensgegevens als zodanig zullen herkennen. De verwerking van hun persoonsgegevens speelt zich grotendeels buiten hun blikveld af.

2.3 Klachten van burgers

Burgers die constateren dat hun persoonsgegevens worden misbruikt kunnen daarover klagen bij, onder meer, de betrokken instantie zelf, het CBP en bij de Nationale Ombudsman.
De inspectie heeft onderzocht in hoeverre burgers klagen over misbruik of oneigenlijk gebruik van persoonsgegevens die afkomstig zijn uit de keten van werk en inkomen. Zij heeft voor dit doel de relevante klachten geïnventariseerd die zijn binnengekomen bij het CBP, bij de Nationale Ombudsman, bij de afdeling Publieksinformatie van het Ministerie van SZW, bij de uitvoeringsorganisaties en bij de inspectie zelf.
Uit deze inventarisatie blijkt dat klachten over misbruik of oneigenlijk gebruik van gegevens uit de keten van werk en inkomen zelden voorkomen. Uit 2004 of 2005 heeft de inspectie geen relevante klachten aangetroffen. Klachten over het gebruik van persoonsgegevens binnen de keten van werk en inkomen hebben veelal betrekking op zaken, zoals huisbezoeken door sociaal rechercheurs, die burgers ervaren als inbreuken op hun persoonlijke levenssfeer maar die wettelijk zijn toegestaan.

In 2002 bracht een klacht van een burger een geval aan het licht van grootschalig misbruik van persoonsgegevens die afkomstig waren uit, onder meer, de sociale zekerheid. De betrokken uitvoeringsorganisaties hebben naar aanleiding van dit incident maatregelen genomen.[2]

2
'In goed vertrouwen, onrechtmatige gegevensverstrekking aan een handelsinformatiebureau', IWI, oktober 2004.

2.4 Conclusie

Klachten over misbruik of oneigenlijk gebruik van gegevens uit de keten van werk en inkomen komen zelden voor. Uit het uitblijven van relevante klachten mag niet zonder meer worden geconcludeerd dat misbruik of oneigenlijk gebruik niet voorkomt. Achter één klacht van een burger kan grootschalig misbruik van persoonsgegevens schuil gaan.

3 Waarborgen voor doelbinding en beveiliging

3.1 Eisen aan de beveiliging van Suwinet

Uitvoeringsorganisaties en gemeenten die gebruik maken van Suwinet zijn verantwoordelijk voor de beveiliging van (hun deel van) Suwinet. De eisen waaraan ze zich moeten houden zijn vastgelegd in bijlage XIV bij de Regeling SUWI. Deze eisen vormen de uitwerking van de eisen uit de Wet bescherming persoonsgegevens (Wbp) en de Wet SUWI. De eisen houden, onder meer, in dat uitvoeringsorganisaties en gemeenten voldoende maatregelen moeten treffen om doelbinding en beveiliging te waarborgen.

Het is aan de uitvoeringsorganisaties en gemeenten zelf om invulling aan deze eisen te geven. Ze worden daarbij ondersteund door het Bureau Keteninformatisering Werk en Inkomen (BKWI), dat onder meer verantwoordelijk is voor de inrichting van Suwinet. BKWI biedt, onder meer, technische mogelijkheden die de ketenpartners in staat stellen om hun medewerkers alleen toegang te geven tot die informatie in Suwinet-Inkijk die ze voor hun werkzaamheden nodig hebben, en controleoverzichten die het mogelijk maken om het gebruik van Suwinet-Inkijk achteraf te controleren. De ketenpartijen zelf hebben de verantwoordelijkheid om deze technische middelen op zo'n manier te gebruiken dat doelbinding en beveiliging gewaarborgd zijn.
Gemeenten worden bij het verwerven, gebruiken en beheren van ICT ondersteund door het Coördinatiepunt ICT Gemeenten (CP-ICT). CP-ICT is een initiatief van de Vereniging Nederlandse Gemeenten (VNG) en Divosa, de landelijke vereniging van leidinggevenden bij Nederlandse overheidsorganisaties op het terrein van werk, inkomen en zorg.

3.2 De verantwoording over de beveiliging van Suwinet

De uitvoeringsorganisaties die gebruik maken van Suwinet verantwoorden zich jaarlijks over de maatregelen die ze hebben genomen om aan de eisen uit Bijlage XIV te voldoen. De verantwoording gaat vergezeld van een oordeel en een rapport van bevindingen van een register EDP-auditor. De ketenpartijen hebben een verantwoordingsrichtlijn opgesteld, met daarbij een normenkader dat de EDP-auditor bij het onderzoek moet gebruiken. Het normenkader vormt de 'vertaling' van Bijlage XIV naar een eenduidig toetsingskader. Met het gebruik van de verantwoordingsrichtlijn en het normenkader willen de ketenpartners bereiken dat de beveiliging van Suwinet bij alle uitvoeringsorganisaties op dezelfde manier wordt beoordeeld, waardoor er uit onderzoek en verantwoording een eenduidig beeld ontstaat.
Sinds de invoering van de Wet werk en bijstand op 1 januari 2004 verantwoorden ook gemeenten zich over de beveiliging van Suwinet, zij het veel beknopter dan de uitvoeringsorganisaties dit doen. Het verslag over de uitvoering WWB gaat vergezeld van een accountantsverklaring. De inspectie beoordeelt de verantwoordingen van de uitvoeringsorganisaties en gemeenten ieder jaar in haar verantwoordingsgericht onderzoek.

3.3 Verantwoordingen van uitvoeringsorganisaties

Sinds de invoering van het SUWI-stelsel in 2002 hebben de uitvoeringsorganisaties veel moeite gedaan om aan de eisen uit Bijlage XIV te voldoen. In het verantwoordingsgericht onderzoek over 2004 stelde de inspectie vast dat de beveiliging bij de uitvoeringsorganisaties ten opzichte van 2003 sterk was verbeterd, maar dat de beveiliging van Suwinet als geheel nog niet op het vereiste niveau was. Verder constateerde de inspectie dat het hanteren van de verantwoordingsrichtlijn de inzichtelijkheid van de getroffen beveiligingsmaatregelen heeft verbeterd, al waren door verschillen in toepassing van de verantwoordingsrichtlijn de oordelen van de EDP-

auditors nog onvoldoende onderling vergelijkbaar.
Tot nu toe hebben de uitvoeringsorganisaties zich alleen nog verantwoord over opzet en bestaan van hun maatregelen. Dit betekent dat de verantwoordingen vooral inzicht bieden in de planvorming en de formele inrichting van de maatregelen, en in de concrete afspraken over de uitvoering. In de verantwoording over 2005 zullen de uitvoeringsorganisaties zich, naar verwachting ook gaan verantwoorden over de werking. Dit houdt in dat de verantwoording duidelijkheid moet bieden over de mate waarin de gemaakte afspraken gedurende het jaar daadwerkelijk zijn nageleefd. Er vindt momenteel overleg plaats tussen de uitvoeringsorganisaties over de vraag hoe de werking over 2005 op een eenduidige manier bij alle ketenpartners kan worden vastgesteld. Bij dit overleg wordt ook de Nederlandse Orde van Register EDP-auditors (NOREA) betrokken. Een aantal uitvoeringsorganisaties is nog bezig om de beveiliging van Suwinet op zo'n manier in te richten dat de EDP-auditor de werking van de getroffen maatregelen vast kan stellen, onder meer door uitgevoerde activiteiten voldoende te documenteren.

3.4 Verantwoordingen van gemeenten

Uit een inventariserend onderzoek in 2004 bleek dat veel gemeenten nog niet wisten hoe ze zich over de beveiliging van Suwinet zouden verantwoorden, en wat de rol van de accountant daarbij zou zijn. Medewerkers bij gemeenten realiseerden zich goed dat ze werken met privacygevoelige gegevens van ketenpartners, en dat daarbij zorgvuldigheid is vereist. Veel gemeenten bleken behoefte te hebben aan toelichting op de wettelijke voorschriften en aan praktische hulpmiddelen.[3]

3
'Beveiliging Suwinet bij gemeenten', IWI, februari 2005.

In hun verslag over de uitvoering WWB over 2004 moesten gemeenten zich voor het eerst verantwoorden over de beveiliging van Suwinet. Ten tijde van het uitvoeren van dit onderzoek had het Ministerie van SZW nog niet alle verslagen over 2004 ontvangen. Een eerste inventarisatie van de beschikbare verslagen wijst erop dat ongeveer de helft van de gemeenten niet beschikt over een beveiligingsplan voor Suwinet, of over een algemeen beveiligingsplan met daarin specifieke elementen voor het gebruik van Suwinet.
De verslagen over de uitvoering WWB gaan vergezeld van een accountantsverklaring. De controle op de verslagen over de uitvoering WWB wordt, voor een groot aantal gemeenten, uitgevoerd door een beperkt aantal grote accountantskantoren. De controle door deze accountantskantoren blijkt met name gericht te zijn op de formele aspecten: de aanwezigheid van een beveiligingsplan en de goedkeuring door burgemeester en wethouders. Dit is in overeenstemming met het verantwoordings- en controleprotocol dat op deze controle van toepassing is. De accountants beoordelen niet of het beveiligingsplan, bijvoorbeeld, aansluit bij organisatie en werkwijze van de betreffende gemeente. Ook stelt de accountant niet vast of de medewerkers van de gemeente op de hoogte zijn van wat er in het beveiligingsplan staat, en of ze dit in de praktijk daadwerkelijk naleven. Wel geven de accountantskantoren aan dat ze dit soort aspecten in voorkomende gevallen onder de aandacht van de gemeenten brengen.
Het toezicht op de uitvoering door gemeenten berust primair bij de gemeenteraad. Het is mogelijk dat burgemeesters en wethouders, om zich tegenover de gemeenteraad te kunnen verantwoorden, hun beveiligingsplannen door externe deskundigen hebben laten toetsen. Dit komt echter niet in de verantwoording tot uiting.

De aandacht voor de beveiliging van Suwinet in het gemeentelijk domein neemt toe. In 2004 heeft BKWI, samen met het CP-ICT, een informatiemap samengesteld die gemeenten moet ondersteunen bij het opstellen van een informatiebeveiligingsplan (de zogenaamde 'sprekende kluis'). In 2005 hebben BKWI en CP-ICT een website gepubliceerd, met aanvullende informatie en voorbeelden van beveiligingsplannen.
In de praktijk blijken met name de kleinere gemeenten grote moeite te hebben met het opstellen van een beveiligingsplan en met het nemen van de vereiste maatregelen. Ze zijn van mening dat de aangeboden richtlijnen en voorbeelden zijn toegesneden op grote gemeenten, en hebben moeite deze toe te passen. BKWI en CP-ICT hebben toegezegd ondersteunend materiaal aan te zullen reiken dat is toegespitst op middelgrote en kleine gemeenten.

3.5 Waarborgen voor doelbinding en beveiliging

Uitvoeringsorganisaties en gemeenten zijn verplicht om maatregelen te nemen om doelbinding en beveiliging te waarborgen. De belangrijkste maatregelen zijn:

- Logische toegangsbeveiliging.
  Door middel van logische toegangsbeveiliging zorgen uitvoeringsorganisaties en gemeenten dat alleen die medewerkers die dat voor hun werk nodig hebben toegang krijgen tot Suwinet-Inkijk, en dat deze medewerkers daarbij alleen toegang krijgen tot die gegevens die ze daadwerkelijk nodig hebben. Logische toegangsbeveiliging is van groot belang voor het waarborgen van doelbinding.
- Beveiliging bij ICT-dienstverleners.
  Het technisch beheer van Suwinet is voor een groot deel uitbesteed aan ICT-dienstverleners. Om de beveiliging van de gegevens te waarborgen moeten deze dienstverleners voldoende maatregelen nemen om, bijvoorbeeld, inbraken door hackers te voorkomen.
- Controle op het gebruik van Suwinet-Inkijk.
  BKWI maakt overzichten van het gebruik van Suwinet-Inkijk door medewerkers van uitvoeringsorganisaties en gemeenten. Controle van deze overzichten helpt de ketenpartners bij het opsporen van misbruik of oneigenlijk gebruik van gegevens uit Suwinet. Dit is van belang voor zowel doelbinding als beveiliging.
- Beveiligingstests.
  In een beveiligingstest of penetratietest proberen gespecialiseerde testers toegang te krijgen tot gegevens in Suwinet. Ze kunnen daarbij technische inbraakpogingen doen ('hacking') of proberen om van medewerkers informatie los te krijgen ('social engineering'). Uitvoeringsorganisaties en gemeenten zijn niet verplicht om beveiligingstests uit te laten voeren. Wel kunnen dergelijke tests inzicht geven in de zwakke plekken in de beveiliging van Suwinet, en kunnen ze een indicatie geven van de mate waarin doelbinding en beveiliging daadwerkelijk gewaarborgd zijn.

Het vervolg van deze paragraaf gaat in op de manier waarop uitvoeringsorganisaties en gemeenten invulling geven aan deze maatregelen.

Logische toegangsbeveiliging

Bij de ingebruikname van Suwinet-Inkijk was het voor alle aangesloten gebruikers mogelijk om alle beschikbare gegevens van burgers in te zien. De ketenpartners vonden dit ongewenst, en besloten in 2003 om maatregelen te treffen om te zorgen dat medewerkers in Suwinet-Inkijk alleen toegang krijgen tot die informatie die ze nodig hebben om hun taken uit te kunnen voeren.

Bij het nemen van deze maatregelen werken de ketenpartners samen met BKWI. De ketenpartners inventariseren welke rollen er binnen hun organisatie zijn, zoals baliemedewerker of claimbehandelaar, en welke informatie medewerkers uit Suwinet-Inkijk nodig hebben om hun rol naar behoren te kunnen vervullen. BKWI implementeert deze rollen vervolgens in Suwinet-Inkijk, zodat medewerkers die Suwinet-Inkijk raadplegen alleen maar die gegevens kunnen zien die bij hun rol horen.
Uitvoeringsorganisaties en gemeenten zijn zelf verantwoordelijk voor het toekennen van de juiste rol aan de juiste medewerker. Ze moeten ook zorgen dat de koppeling van rollen aan medewerkers actueel blijft, door periodiek te controleren of de betreffende medewerkers nog steeds in dienst zijn en nog steeds dezelfde informatie nodig hebben om hun taken uit te kunnen voeren.

De manier waarop uitvoeringsorganisaties en gemeenten invulling geven aan deze verantwoordelijkheid verschilt. Er zijn verschillen in het aantal rollen dat binnen organisaties worden gehanteerd: het Uitvoeringsinstituut Werknemersverzekeringen (UWV) onderscheidt er 28 en CWI 17, waarvan er in de praktijk maar één daadwerkelijk wordt gebruikt. Voor het gemeentelijk domein zijn vier rollen gedefinieerd. In de manier waarop gemeenten deze rollen aan medewerkers toekennen bestaan grote verschillen. Ook zijn er, bij ongeveer even grote gemeenten, grote verschillen in de aantallen medewerkers die toegang hebben tot Suwinet-Inkijk. De verschillen kunnen maar voor een deel worden verklaard uit, bijvoorbeeld, organisatieomvang en inrichting van de werkprocessen.

Bij de ingebruikname van Suwinet-Inkijk hadden de uitvoeringsorganisaties nog geen sluitende procedures voor het aan- en afmelden van gebruikers. Dit leidde ertoe dat er in Suwinet-Inkijk gebruikers in een bepaalde rol bekend waren, die in werkelijkheid van functie waren veranderd of niet meer in dienst waren bij de betreffende uitvoeringsorganisatie. In de loop van 2004 hebben de uitvoeringsorganisaties een schoning uitgevoerd. UWV heeft inmiddels een procedure ontwikkeld om periodiek een dergelijke schoning uit te voeren. De inspectie heeft geen informatie over soortgelijke acties in het gemeentelijk domein.

Beveiliging bij ICT-dienstverleners

Het technisch beheer van het Suwinet is door de Suwi-organisaties uitbesteed aan ICT-dienstverleners. Deze dienstverleners voeren dagelijkse handelingen uit als het instellen en onderhouden van systeemcomponenten en het maken van backups. Een deel van de werkzaamheden die ze uitvoeren, bijvoorbeeld het instellen van firewalls en het implementeren van beveiligd berichtenverkeer, is ook specifiek van belang voor de beveiliging van de gegevens in Suwinet-Inkijk tegen inbraken van buitenaf.

De Wbp verplicht uitvoeringsorganisaties en gemeenten om ervoor te zorgen dat ICT-dienstverleners, die in opdracht van hen persoonsgegevens verwerken, zich aan dezelfde wettelijke voorschriften houden die ook voor henzelf gelden. Dit betekent dat de normen uit bijlage XIV bij de Regeling SUWI, en het normenkader waarin deze zijn vertaald, onverkort gelden voor ICT-dienstverleners.

Uitvoeringsorganisaties en gemeenten zijn ook verplicht erop toe te zien dat de ICT-dienstverleners deze voorschriften naleven. Ze kunnen de naleving van deze voorschriften vooraf borgen door hierover afspraken te maken in de contracten, serviceniveauovereenkomsten (SNO's) of service level agreements (SLA's) die ze met de dienstverleners afsluiten. Verder is het gebruikelijk dat dienstverleners door een onafhankelijke EDP-auditor laten toetsen of ze zich aan de gemaakte afspraken houden. Het resultaat van deze toetsing, de 'third party mededeling' (TPM) wordt beschikbaar gesteld aan de opdrachtgevers van de ICT-dienstverlener.

UWV heeft dit enige jaren geleden in de contracten met ICT-dienstverleners geïmplementeerd, onder meer door met de dienstverleners afspraken te maken over het afgeven van TPM's. UWV heeft een uitgebreid normenkader opgesteld dat de EDP-auditors, bij het afgeven van TPM's, toe moeten passen. Inmiddels heeft UWV met de dienstverleners afgesproken dat die, over 2005, ook de specifieke normen die gelden voor Suwinet zullen laten onderzoeken. CWI vraagt hun ICT-dienstverleners niet om een specifieke TPM volgens het SUWI-normenkader, maar hanteert hiervoor een algemeen normenkader. Het normenkader van CWI is, onder meer, gebaseerd, op het SUWI-normenkader. BKWI heeft met zijn ICT-dienstverlener afgesproken dat deze met ingang van 2005 een TPM volgens het SUWI-normenkader afgeeft.

De uitvoeringsorganisaties zullen de TPM's betrekken in het onderzoek dat ze jaarlijks uitvoeren, of laten uitvoeren, ten behoeve van de verantwoording over de beveiliging van Suwinet.

Controle op het gebruik van Suwinet-Inkijk

Het is van belang om vast te stellen dat medewerkers, die voor hun werk toegang hebben tot Suwinet-Inkijk, de gegevens uitsluitend gebruiken voor de doeleinden waarvoor ze bestemd zijn. Behalve maatregelen zoals voorlichting van medewerkers, en het laten ondertekenen van een geheimhoudingsverklaring, hebben uitvoeringsorganisaties en gemeenten weinig mogelijkheden om misbruik van Suwinet-Inkijk te voorkomen.

De ketenpartners hebben daarom gekozen voor controle achteraf. BKWI registreert alle raadplegingen van Suwinet-Inkijk, en maakt daar periodiek rapportages van. Deze rapportages informeren de ketenpartners, op totaalniveau, over de raadplegingen van hun eigen medewerkers. De rapportages zijn zo ingericht dat afwijkend gebruik van Suwinet-Inkijk binnen de eigen uitvoeringsorganisatie of gemeente, zoals raadplegingen buiten werktijd en grote aantallen raadplegingen door specifieke (groepen) medewerkers, zichtbaar worden. BKWI verstrekt de rapportage periodiek aan de security officers (functionarissen die belast zijn met de informatiebeveiliging) van uitvoeringsorganisaties en gemeenten.

Bij vermoeden van misbruik kan de security officer van de uitvoeringsorganisatie aanvullende overzichten opvragen bij de security officer van BKWI. Security officers van gemeenten kunnen deze overzichten opvragen via de Suwinet Servicedesk. In deze overzichten kan informatie zijn opgenomen over het gebruik van Suwinet-Inkijk door individuele medewerkers.

Een eerste inventarisatie van het gebruik van deze overzicht laat zien dat er, wat dit betreft, tussen de ketenpartners verschillen in benadering bestaan.
CWI geeft aan de overzichten te gebruiken, en alleen aanvullende overzichten op te vragen bij een duidelijk vermoeden van misbruik. De security officer van UWV geeft aan dat hij de periodieke overzichten van BKWI bij zijn controles gebruikt, en dat hij jaarlijks een steekproef uitvoert waarbij hij bij BKWI detailrapportages opvraagt en analyseert.
Veel gemeenten hebben (nog) geen security officer benoemd. Aangezien BKWI de rapportages over het gebruik van Suwinet-Inkijk uitsluitend naar security officers stuurt, krijgen gemeenten zonder security officer deze rapportages niet. In het najaar van 2004 kregen tien gemeenten periodiek een rapportage toegestuurd. In september 2005 is dit aantal toegenomen tot 86. Sinds 2004 hebben gemeenten een kleine dertig aanvullende rapportages opgevraagd.

Beveiligingstests
Een aantal uitvoeringsorganisaties heeft in de afgelopen jaren tests uit laten voeren op de beveiliging van Suwinet, zogenoemde penetratietests. In dergelijke tests proberen gespecialiseerde testers om met ongeoorloofde middelen toegang te krijgen tot Suwinet-Inkijk.

In november 2004 heeft een penetratietest plaatsgevonden bij UWV. De uitkomst was dat het voor ongeautoriseerde gebruikers van buiten het netwerk van UWV niet mogelijk was om toegang te krijgen tot Suwinet-Inkijk.
Ook BKWI heeft, in juli 2004, een penetratietest laten uitvoeren. Hier kwam uit dat Suwinet uitsluitend vanuit het SUWI-domein, dus vanuit uitvoeringsorganisaties en gemeenten, benaderbaar was. De beveiligingsinspanningen zullen zich dan ook met name richten op het verminderen van de kwetsbaarheid voor 'aanvallen' van binnenuit.

Deze tests zijn uitgevoerd bij één uitvoeringsorganisatie, en geven geen beeld voor de keten als geheel. Er is tot nu toe nog geen test uitgevoerd met een opdracht als 'probeer, op welke manier dan ook en via welke ketenpartij dan ook, toegang te krijgen tot gegevens in Suwinet'. Een dergelijke test zou belangrijke inzichten op kunnen leveren over de zwakke plekken in de keten.
Ook hebben de ketenpartijen nooit een ketenbrede risicoanalyse voor Suwinet gemaakt. Dit betekent dat er op dit moment geen goed onderbouwd beeld is van de risicogebieden waar mogelijk extra maatregelen noodzakelijk zijn.

3.6 Conclusie

De inspectie heeft geen zicht op de waarborgen voor doelbinding en beveiliging in het gemeentelijk domein. Wel bieden de verslagen over de uitvoering WWB, hoe summier ook, enig zicht op de stand van zaken rond de beveiliging van Suwinet in het algemeen. Het wordt steeds duidelijker dat veel gemeenten, met name de kleinere gemeenten, moeite hebben om de beveiliging van Suwinet aantoonbaar in overeenstemming met de wettelijke voorschriften in te richten. De aandacht voor de beveiliging van Suwinet in het gemeentelijk domein neemt toe, en BKWI en CP-ICT bieden gemeenten ondersteuning.
De uitvoeringsorganisaties hebben in de afgelopen jaren waarneembare vorderingen gemaakt bij het nemen van de maatregelen die noodzakelijk zijn voor doelbinding en beveiliging. Ze zijn nog bezig om de werking van hun maatregelen aantoonbaar te maken.
Verschillen in de manier waarop de verschillende ketenpartijen hun maatregelen hebben geïmplementeerd zijn niet altijd verklaarbaar. Verder ontbreekt een ketenbrede risicoanalyse, en geven de beveiligingstests die de ketenpartners hebben uitgevoerd geen beeld van de zwakke plekken van de beveiliging van Suwinet binnen de keten als geheel.

4 Oordeel

Uitvoeringsorganisaties en gemeenten die gebruik maken van Suwinet zijn verantwoordelijk voor de beveiliging van (hun deel van) Suwinet. Ze moeten zich daarbij houden aan de eisen die zijn vastgelegd in bijlage XIV bij de Regeling SUWI. Naleving van deze eisen is een belangrijke randvoorwaarde voor het waarborgen van doelbinding en beveiliging bij het gebruik van Suwinet.

Een eerste inventarisatie van de verslagen over de uitvoering WWB over het jaar 2004 wijst uit dat veel gemeenten de beveiliging van Suwinet niet aantoonbaar in overeenstemming met de wettelijke eisen hebben ingericht. Gemeenten hoeven zich in het verslag over de uitvoering WWB uitsluitend te verantwoorden over de aanwezigheid van een beveiligingsplan voor Suwinet, of een algemeen beveiligingsplan met daarin specifieke elementen voor het gebruik van Suwinet. De verslagen over de uitvoering WWB bieden dientengevolge geen inzicht in de mate waarin beveiligingsmaatregelen in de praktijk daadwerkelijk worden nageleefd. Binnen het gemeentelijk domein heeft de beveiliging van Suwinet in toenemende mate de aandacht, en BKWI en CP-ICT ondersteunen de gemeenten bij de inrichting.

De uitvoeringsorganisaties hebben in de afgelopen jaren waarneembare vorderingen gemaakt bij de beveiliging van Suwinet in het algemeen, en het waarborgen van de privacyaspecten doelbinding en beveiliging in het bijzonder. Gedurende de looptijd van het onderzoek waren de uitvoeringsorganisaties nog bezig om de werking van hun beveiligingsmaatregelen, de mate waarin de maatregelen in de praktijk worden nageleefd, aantoonbaar te maken. Uit de verantwoordingen van de uitvoeringsorganisaties over 2005 zal blijken in hoeverre ze daarin geslaagd zijn. Zolang de werking van de maatregelen niet aantoonbaar op orde is, blijft er onzekerheid bestaan over de mate waarin de beveiliging van Suwinet daadwerkelijk is gewaarborgd.

Uit het al dan niet voorkomen van klachten van burgers over misbruik of oneigenlijk gebruik van hun persoonsgegevens kunnen geen conclusies worden getrokken over de mate waarin doelbinding en beveiliging gewaarborgd zijn. Het is daarom van groot belang dat de Suwinetpartijen voldoende maatregelen nemen om doelbinding en beveiliging te waarborgen, en dat deze maatregelen over de gehele keten heen van voldoende niveau zijn. Een ketenbrede risicoanalyse, en ketenbrede beveiligingstests, kunnen een indicatie geven van de mate waarin doelbinding en beveiliging binnen de keten als geheel daadwerkelijk gewaarborgd zijn.

5 Reacties betrokken uitvoerings-organisaties

De inspectie heeft de conceptrapportage voor een bestuurlijke reactie voorgelegd aan BKWI, CWI, IB, SVB en UWV. Als het onderzoek over gemeenten gaat, vraagt de inspectie een bestuurlijke reactie van de VNG. Dat is ook gebeurd bij dit rapport. De VNG heeft afgezien van het geven van een bestuurlijke reactie. Hieronder volgt per ketenpartner een samenvatting van de reacties met commentaar daarop van de inspectie. Aan het einde van dit hoofdstuk geeft de inspectie een overall reactie. De schriftelijke reacties van de ketenpartners zijn integraal opgenomen in de bijlagen bij dit rapport.

5.1 Bureau Keteninformatisering Werk en Inkomen

Het BKWI spreekt waardering uit voor het rapport.

5.2 Centrale organisatie werk en inkomen

CWI licht de genomen maatregelen toe op het gebied van logische toegangsbeveiliging. CWI geeft aan meerdere varianten op één basisrol te onderscheiden en toe te passen, en het bestand van gebruikers regelmatig te schonen.
Uit het uitblijven van klachten over misbruik of oneigenlijk gebruik van gegevens uit de keten van werk en inkomen in 2004 en 2005 mag naar mening van CWI de voorzichtige conclusie worden getrokken dat de maatregelen, die de uitvoeringsorganisaties hebben genomen om misbruik en oneigenlijk gebruik te voorkomen, effectief zijn gebleken. Verder is CWI van mening dat uit verschillen in de manier waarop uitvoeringsorganisaties en gemeenten hun beveiligingsmaatregelen hebben geïmplementeerd, niet zonder meer conclusies kunnen worden getrokken voor het beveiligingsniveau van de keten als geheel.
CWI ziet het rapport als een stimulans om, bij het waarborgen van doelbinding en beveiliging, op de ingeslagen weg voort te gaan. CWI geeft daarbij aan dat het eerste aandachtspunt, het aantonen van de werking van de beveiligingsmaatregelen, in het kader van de jaarverantwoording over 2005 zijn beslag zal krijgen.

5.3 Stichting Inlichtingenbureau Gemeenten

Het bestuur van de Stichting Inlichtingenbureau onderschrijft het belang van beveiliging en doelbinding en kan zich ook overigens geheel vinden in de inhoud en strekking van het rapport.

5.4 Sociale Verzekeringsbank

De SVB vindt Suwinet-Inkijk een positieve ontwikkeling, en heeft een proef met het gebruik van Suwinet-Inkijk gestart. Wel geeft de SVB bij het uitwisselen van gegevens de voorkeur aan massale, batchgewijze geautomatiseerde gegevensuitwisseling. Aangezien Suwinet-Inkijk gericht is op individuele gegevens zal de SVB hier naar verwachting minder gebruik van maken.
De SVB geeft aan alleen volledig in Suwinet-Inkijk te kunnen participeren als de beveiliging voldoende is gewaarborgd. De SVB vindt het dan ook een grote stap voorwaarts dat de uitvoeringsorganisaties ten aanzien van de verplichtingen aangaande beveiliging grote vooruitgang hebben geboekt. Wel constateert de SVB dat er ten aanzien van de beveiliging bij gemeenten grote vraagtekens blijven bestaan, die ook hun weerslag hebben op de manier waarop de SVB op dit moment aankijkt tegen participatie in Suwinet-Inkijk.

5.5 Uitvoeringsinstituut Werknemersverzekeringen

UWV kan zich vinden in het door IWI geschetste beeld en het oordeel met betrekking tot doelbinding en beveiliging van de keten van werk en inkomen als geheel. UWV geeft aan de beveiliging van Suwinet zeer belangrijk te vinden, en illustreert dit met een aantal maatregelen die de organisatie op dit gebied heeft genomen. UWV onderschrijft het nut van een ketenbrede risicoanalyse en beveiligingstest voor het vaststellen van de waarborgen voor doelbinding en beveiliging binnen de keten als geheel.

5.6 Nawoord IWI

IWI neemt met waardering kennis van de lopende en geplande activiteiten waaraan in de bestuurlijke reacties gerefereerd wordt. De inspectie ziet in de ontvangen reacties geen aanleiding om haar oordeel te wijzigen. Wel hebben de reacties geleid tot enige tekstuele wijzigingen in het rapport.

Lijst van afkortingen

BKWI	Bureau Keteninformatisering Werk en Inkomen
CBP	College bescherming persoonsgegevens
CP-ICT	Coördinatiepunt ICT gemeenten
CWI	Centrale organisatie werk en inkomen
CWI	Centrum voor Werk en Inkomen
Divosa	Vereniging van directeuren van overheidsorganen voor sociale arbeid
EDP	electronic dataprocessing, elektronische gegevensverwerking
ICT	Informatie- en communicatietechnologie
IWI	Inspectie Werk en Inkomen
NOREA	Nederlandse Orde van Register EDP-auditors
SIOD	Sociale Inlichtingen en Opsporingsdienst
SLA	service level agreement, serviceniveauovereenkomst
SNO	Serviceniveauovereenkomst
SUWI	Structuur uitvoering werk en inkomen
SVB	Sociale Verzekeringsbank
SZW	Sociale Zaken en Werkgelegenheid
TPM	third party mededeling
UWV	Uitvoeringsinstituut Werknemersverzekeringen
VNG	Vereniging van Nederlandse Gemeenten
Wbp	Wet bescherming persoonsgegevens
WWB	Wet werk en bijstand

Bijlagen

Reactie Bureau Keteninformatisering Werk en Inkomen
Reactie Centrale organisatie werk en inkomen
Reactie Stichting Inlichtingenbureau Gemeenten
Reactie Sociale Verzekeringsbank
Reactie Uitvoeringsinstituut Werknemersverzekeringen

BUREAU KETENINFORMATISERING
WERK & INKOMEN

IWI
De heer mr. L.H.J. Kokhuis
Postbus 11562
2502 AN DEN HAAG

Datum:	Ons Kenmerk:	Contactpersoon:
19 januari 2006	2006/014	E.J.Rietbergen
Onderwerp:	Uw brief:	Doorkiesnummer:
Rapport "Doelbinding en beveiliging in de keten van Werk en Inkomen"	2005/7126	(020) 8513 730

Geachte heer Kokhuis,

Gaarne voldoe ik aan uw verzoek van 7 december jl om een bestuurlijke reactie te geven op bovengenoemd rapport. Hieronder is deze reactie opgenomen:

Wij vinden dit een uitstekend rapport.

Hoogachtend,

Drs. O.M. Kinkhorst
directeur

BKWI Bureau Keteninformatisering Werk en Inkomen
Naritaweg 37 1043 BP Amsterdam
Postbus 20581 1001 NN Amsterdam
Telefoon 020 - 851 37 00
Fax 020 - 851 37 01
info@bkwi.nl / www.bkwi.nl

CENTRUM VOOR WERK EN INKOMEN

Centrale organisatie Werk en Inkomen

Naritaweg 1
Postbus 58191
1040 HD Amsterdam
Tel 020-7515000
Fax 020-7515099
www.cwinet.nl

Aan de Inspecteur-generaal voor werk en inkomen
De heer mr. L.H.J. Kokhuis
Postbus 11563
2502 AN Den Haag

Kenmerk:	Contactpersoon:	Datum:
CWI/2005/6662	drs J.P.M. van Straaten	16 december 2005
Uw kenmerk:	**Doorkiesnummer:**	**Direct faxnummer:**
2005/7127	020 - 7515225	020 – 7515212

Betreft:
Bestuurlijke reactie op rapport "Doelbinding en beveiliging in de keten van werk en inkomen"

Geachte heer Kokhuis,

Hierbij doe ik u de reactie toekomen van de Raad van Bestuur op het rapport "Doelbinding en beveiliging in de keten van werk en inkomen".

In de conclusie van de Inspectie voor wat betreft doelbevinding en beveiliging vanuit de burger bezien (paragraaf 2.4) komt naar voren dat is gebleken dat in 2004 en 2005 geen gevallen van misbruik of oneigenlijk gebruik zijn geconstateerd. Om gevallen van misbruik of oneigenlijk gebruik te constateren moet de inspectie teruggaan naar een klacht uit het jaar 2002 ("handelsinformatiebureau X"). Een voorzichtige conclusie kan derhalve zijn dat de naar aanleiding van die klacht door de betrokken uitvoeringsorganisaties (CWI was overigens niet één van de betrokken partijen maar heeft wel maatregelen getroffen) genomen maatregelen effectief zijn gebleken.

Wat betreft de waarborgen voor doelbinding en beveiliging wordt in het rapport ten onrechte geschetst dat CWI bij de logische toegangsbeveiliging in de praktijk slechts één gebruikersrol hanteert. Er worden door CWI echter meerdere varianten op één basisrol onderscheiden en toegepast. CWI schoont het bestand van gebruikers bovendien regelmatig. In de tekst (blz. 14) wordt nu ten onrechte gesuggereerd dat dat eenmalig in 2004 heeft plaatsgevonden. CWI zal de uitvoering van opschoningacties binnenkort bovendien in een procedure vastleggen om te garanderen dat "niet-langer-bevoegden" geen toegang meer hebben tot Suwinet.

De conclusies met betrekking tot de waarborgen voor doelbinding en beveiliging (blz. 17 van het rapport) geven voor wat betreft de uitvoeringsorganisaties mogelijk

een te negatief beeld van de situatie. Zo wordt geconstateerd dat verschillen in de manier waarop de verschillende ketenpartijen hun maatregelen hebben geïmplementeerd niet altijd verklaarbaar zijn. Daaraan ligt de kennelijke veronderstelling ten grondslag dat door alle ketenpartijen de implementatie op eenzelfde wijze zou moeten plaatsvinden, hetgeen naar onze mening niet nodig is.

In het oordeel (blz. 19 van het rapport) spreekt de Inspectie uit dat uit het al dan niet voorkomen van klachten van burgers over misbruik of oneigenlijk gebruik van hun persoonsgegevens geen conclusies kunnen worden getrokken over de mate waarin doelbinding en beveiliging gewaarborgd zijn. Wel kan echter worden geconstateerd dat in de afgelopen jaren (na 2002) geen klachten van burgers meer naar voren zijn gekomen. Het rapport geeft bovendien aan dat bij de uitvoeringsorganisaties waarneembare vorderingen zijn gemaakt bij de beveiliging van Suwinet in het algemeen en het waarborgen van privacyaspecten doelbinding en beveiliging in het bijzonder.
Het rapport vormt daarmee een stimulans om op de ingeslagen weg voort te gaan. Eerste aandachtspunt in dit verband is het aantonen van de werking van de beveiligingsmaatregelen. Dit zal in het kader van jaarverantwoording over 2005 zijn beslag gaan krijgen.

Ik vertrouw erop u hiermee voldoende te hebben geïnformeerd.

Hoogachtend,

drs. R. de Groot
Voorzitter Raad van Bestuur

Inlichtingenbureau

Bordewijklaan 18 Postbus 19125 2500 CC Den Haag T (0800) 023 37 86 F (0800) 023 13 21 WWW inlichtingenbureau.nl

Inspectie Werk en Inkomen
t.a.v. de heer mr. L.H.J. Kokhuis
Postbus 11563
2502 AN DEN HAAG

Onderwerp	Datum	Uw kenmerk	Ons kenmerk
Reactie op conceptrapport Doelbinding en beveiliging in de keten van werk en inkomen	22 december 2005	2005/7128	IB05-1075

Geachte heer Kokhuis,

Op 12 december ontving ik uw verzoek om binnen twee weken te reageren op het oordeel zoals geformuleerd door de inspectie in het conceptrapport *Doelbinding en beveiliging in de keten van werk en inkomen.*

Hieronder is de reactie van het bestuur van de Stichting Inlichtingenbureau opgenomen:

Het bestuur van de Stichting Inlichtingenbureau onderschrijft het belang van beveiliging en doelbinding en kan zich ook overigens geheel vinden in de inhoud en strekking van het onderhavige rapport.

Hoogachtend,
Voorzitter Bestuur Inlichtingenbureau

U. Groen

Sociale Verzekeringsbank **Voorzitter Raad van Bestuur**
Van Heuven Goedhartlaan 1
Postbus 1100
1180 BH Amstelveen

Inspectie Werk en Inkomen
T.a.v. de heer mr. L.H.J. Kokhuis, Inspecteur Generaal
Postbus 11563
2502 AN DEN HAAG

datum	ons kenmerk	contactpersoon	telefoonnummer
1 december 2005	RvB.252/05/ES/ptb		020 656 4809

Betreft: IWI-rapport "De beveiliging van Suwinet en de privacy van de burger

Geachte heer Kokhuis,

Op 17 november 2005 verzocht u ons schriftelijk om een bestuurlijke reactie op het bovengenoemde concept-rapport (uw kenmerk: 2005/6690). Deze reactie doe ik u hierbij toekomen.

U geeft aan ons dit concept-rapport aan te bieden ter verificatie van bevindingen.
Aangezien er geen bevindingen aangaande de SVB worden geuit zullen wij in meer algemene zin ingaan op de voor ons relevante punten.

Ten eerste willen wij aangeven dat wij positief staan tegenover de ontwikkelingen ten aanzien van Suwinet-Inkijk. De SVB heeft de gegevensuitwisseling rond bijvoorbeeld basisregistraties vergaand geautomatiseerd, vandaar dat de SVB zich op het standpunt stelt dat slechts in beperkte gevallen het gebruik maken van Suwinet-Inkijk aan de orde is. Daar waar het uitwisselen van informatie geautomatiseerd kan plaatsvinden, zullen wij die weg bewandelen in verband met de arbeidsintensiviteit van Suwinet-Inkijk.

De bevindingen uit het rapport, zoals verwoord in de conclusie, onderschrijven wij. Wij willen daarbij benadrukken dat een goede beveiliging bij alle betrokkenen voor de SVB een randvoorwaarde is om aan te sluiten.
Daarbij willen wij er op wijzen dat, door bepalingen in de wet Suwi, wij gehouden zijn aan strikte verplichtingen aangaande beveiliging. Wij pleiten er voor dat vergelijkbare verplichtingen ook voor andere partijen van toepassing worden opdat herhaling van de casus 'het handelsinformatiebureau' voorkomen wordt.

Ik vertrouw u hiermee voldoende te hebben geïnformeerd.

Hoogachtend,
Sociale Verzekeringsbank

drs. E.F. Stoové
voorzitter Raad van Bestuur

Postbus 58285, 1040 HG AMSTERDAM

Inspectie Werk en Inkomen,
De heer mr. L.H.J. Kokhuis
Postbus 11563
2502 AN DEN HAAG

Datum

02 JAN 2006

Van
Drs. E.C.P. Lyre
T 020 - 687 53 74
F 020 - 687 54 95
Milly.Lyre@uwv.nl

Ons kenmerk
SB/68547
Uw kenmerk
2005/6675

Onderwerp
Doelbinding en beveiliging in de keten van werk en inkomen

Geachte heer Kokhuis,

Hiermee geef ik de UWV reactie op het concept rapport "Doelbinding en beveiliging in de keten van werk en inkomen".

UWV kan zich vinden in het door IWI geschetste beeld en het oordeel met betrekking tot doelbinding en beveiliging van de keten van werk en inkomen als geheel.

UWV vindt de beveiliging van Suwinet zeer belangrijk. Zo hebben wij in de afgelopen periode op eigen initiatief netwerkbeveiligingstesten laten uitvoeren. Met het hanteren van de TPM-systematiek, waarbij getoetst wordt dat ICT-leveranciers zich aan de gemaakte afspraken houden ten aanzien van o.a. technische beheer en beveiliging, laat UWV zien ver met dit proces te zijn in de keten. Tevens kan aangegeven worden dat UWV belangrijke resultaten heeft geboekt in de logische toegangsbeveiliging van Suwinet door roldifferentiatie met 28 rollen te implementeren en Suwinet useraccounts periodiek te controleren en te schonen.

Wij ondersteunen de aanbeveling van IWI om een ketenbrede risicoanalyse en beveiligingstest uit te voeren, waarmee een indicatie verkregen kan worden over het waarborgen van doelbinding en beveiliging in de keten van werk en inkomen.

Ik vertrouw u hiermee van dienst te zijn.

Hoogachtend,

Dr. J.M. Linthorst
Voorzitter Raad van Bestuur

Publicaties van de Inspectie Werk en Inkomen

2006

R06/01 Doelbinding en beveiliging in de keten van werk en inkomen
De beveiliging van Suwinet en de privacy van de burger

2005

R05/24 UWV en Walvis
Vierde rapportage
R05/23 Tussen oordeel en advies
Uitvoering van het deskundigenoordeel 'geschiktheid tot werken' door UWV
R05/22 De korste weg naar werk
Een onderzoek naar reïntegratiecoaching WW bij UWV
R05/21 Gezocht: werklozen
Activiteiten van CWI, UWV en gemeenten om werklozen aan het werk te krijgen in moeilijk vervulbare vacatures voor laag- en ongeschoolde arbeid
R05/20 Vangnet of springplank?
De reïntegratie van zieke werknemers zonder dienstverband door UWV
R05/19 Informatie: aantoonbaar betrouwbaar?
Een onderzoek naar de kwaliteit van de niet-financiële informatievoorziening in het SUWI-domein
R05/18 Opnieuw beoordeeld
R05/17 Zicht op kansen?
Onderzoek naar systematische kennisopbouw over bijstandsgerechtigden door gemeenten
R05/16 Werken aan samenwerking
Een onderzoek naar de invulling van de overlegverplichting van certificatie- en keuringsinstellingen
R05/15 De gevolgen van selectie bij reïntegratietrajecten voor WW-gerechtigden
R05/14 Invloed van WW-gerechtigden op hun reïntegratietraject
R05/13 Beëindiging van dienstbetrekkingen Wsw bij arbeidsongeschiktheid
R05/12 Handhaving door de Sociale Verzekeringsbank in 2004
Toezicht op de Wet kinderopvang
R05/11 Kiezen en delen
De selectie door gemeenten voor reïntegratietrajecten/Casestudies bij acht gemeenten
R05/10 Vuurwerk meester
Een onderzoek naar de certificering van vakbekwaamheid vuurwerk
Jaarplan 2006
Meerjarenplan 2006-2009
R05/09 Pensioen bewaakt
Een onderzoek naar het risicogericht toezicht van De Nederlandsche Bank op pensioenfondsen
R05/08 Ontwikkeling van het handhavingsbeleid binnen UWV
R05/07 UWV en Walvis
Derde rapportage
R05/06 Intake en beoordeling bij de bijstand
R05/05 ICT als verbindende schakel
Keteninformatisering in het stelsel van werk en inkomen
R05/04 Afgesproken?
Gemeenten en CWI-vestigingen over onderlinge afspraken in het kader van de uitkeringsintake voor de WWB
Jaarverslag 2004

R05/03 Kwaliteit van arbeid: een kwestie van zorg
Een onderzoek naar gemeentelijk beleid en sturing op zorg voor kwaliteit van arbeid in de sociale werkvoorziening
R05/02 Gebruikswaarde Suwinet-Inkijk
R05/01 De certificatie van deskundig toezichthouders verwijdering asbest en crocidoliet

U kunt deze publicaties opvragen bij:

Inspectie Werk en Inkomen
Afdeling Communicatie

communicatie@iwiweb.nl
www.iwiweb.nl
Telefoon (070) 304 44 44
Fax (070) 304 44 45

Prinses Beatrixlaan 82
2595 AL Den Haag

Postbus 11563
2502 AN Den Haag