

RISICO ANALYSE SUWINET MAIL

Privacy en Beveiliging van Suwinet Mail

Inhoudsopgave

1. Inleiding.....	3
2. Eisen aan betrouwbaarheid en privacy Suwinet-Mail.....	4
2.1 Het gebruik van e-mail binnen Suwi.....	4
2.2 Eisen aan het gebruik van Suwinet Mail.....	4
2.3 Waardering beveiligingsniveau Suwinet Mail.....	5
3. Risico inschatting op verschillende niveaus.....	7
3.1 Risico's ten aanzien van de inhoud van het e-mailbericht.....	7
3.2 Risico's ten aanzien van het transport van het e-mailbericht.....	8
3.2.1. Infrastructuur.....	8
3.2.2 Authenticiteit.....	8
3.2.3 Routing.....	10
3.2.4. Verantwoordelijkheid.....	11
3.2.5. Regels en afspraken.....	11
3.3 Risico's betreffende het archiveren van e-mailberichten.....	11
4. Conclusie en aanbevelingen.....	19
4.1 Conclusies risico-analyse Suwinet Mail.....	19
4.2 Aanbevelingen.....	20
Bijlage: Geraadpleegde documenten.....	22

1. Inleiding

Bij de uitvoering van taken zijn de organisaties die onderdeel uitmaken van de Structuur Uitvoering Werk en Inkomen (Suwi) keten, te weten de Centra voor Werk en Inkomen (CWI), het Uitvoeringsorgaan Werknemersverzekeringen (UWV) en gemeenten (met name GSD'en) gebonden aan de wettelijke bepalingen op het gebied van privacy en beveiliging met betrekking tot het berichtenverkeer dat tussen deze organisaties plaatsvindt. Naast de bestaande media zoals het al dan niet aangetekende briefverkeer, de telefoon en de fax is, om zo gemakkelijk mogelijk informatie uit te wisselen tussen de ketenpartners, de wens ontstaan om informatie via e-mail uit te wisselen. Deze uitwisseling moet plaats gaan vinden door gebruikmaking van Suwinet, de elektronische infrastructuur die de organisaties binnen Suwi met elkaar verbindt. Het geheel wordt aangeduid als 'Suwinet Mail'.

Dit document bevat een risico-analyse van de aspecten rondom beveiliging en privacy van het gebruik van e-mail binnen het Suwinet en gaat meer in op de aspecten van het voldoen aan de gestelde eisen, dan aan de risico's, welke gelopen worden ten aanzien van mogelijke schade aan vertrouwen, imago of financiële schade. Hierbij moet genoemd worden dat risico's ten aanzien van brief, fax- en telefoonverkeer van dezelfde orde zijn als dezelfde risico's bij Suwinet-Mail en daarvan kan gesteld worden dat deze risico's van een blijkbaar acceptabel niveau zijn en dat maatregelen bij gebrek aan technische mogelijkheden veelal organisatorisch of procedureel van aard zijn.

De risico-analyse is uitgevoerd in opdracht van het Bureau Keteninformatisering Werk en Inkomen (BKWI) en is een analyse op basis van met name door BKWI verstrekte informatie.

Leeswijzer

In het tweede hoofdstuk wordt een beschrijving gegeven van de eisen die gesteld moeten worden aan Suwinet Mail. Vervolgens worden in hoofdstuk drie de risico's rondom Suwinet-Mail in kaart gebracht. In het laatste hoofdstuk worden aanbevelingen gedaan om de risico's te voorkomen. In de bijlage zijn de documenten vermeld waar de voorliggende analyse op is gebaseerd.

2. Eisen aan betrouwbaarheid en privacy Suwinet-Mail

2.1 Het gebruik van e-mail binnen Suwi

De CWI's, het UWV en gemeenten maken bij de uitvoering van de taken binnen de Suwiketenen gebruik van de elektronische infrastructuur Suwinet. Om te komen tot een optimale uitvoering van de Suwi wetgeving, maar zeker ook de Wet Werk en Bijstand (WWB), moeten de partijen in de keten zoveel mogelijk informatie uitwisselen. De wens is ontstaan om e-mail te gebruiken binnen de Suwiketenen om zo te komen tot een meer optimale uitwisseling van informatie. Deze wens is een direct afgeleide van de voordelen van het gebruik van e-mail. E-mail kan leiden tot een efficiëntere, effectievere en flexibelere communicatie tussen gebruikers. Het gebruik van e-mail tussen partners in de Suwiketenen kan dus een positief effect hebben op de communicatie tussen Suwipartners en derhalve een goede samenwerking en uitvoering tussen de partijen bevorderen.

Daar de e-mailberichten tussen de Suwi-partijen cliëntgegevens kunnen (en zullen) bevatten, is het belangrijk dat de uitwisseling van deze ongestructureerde informatie niet onbeveiligd via openbare netwerken zoals Internet wordt verstuurd. Derhalve zal er gebruik worden gemaakt van een e-mail voorziening binnen de grenzen van het Suwi-netwerk voor het versturen van e-mail, genaamd Suwinet Mail.

2.2 Eisen aan het gebruik van Suwinet Mail

Binnen Suwi geldt dat de communicatie tussen de ketenpartners aan formele eisen van betrouwbaarheid en privacy dient te voldoen, voortvloeiend uit de Wet Bescherming Persoonsgegevens (WBP). De eisen die in deze wet gesteld worden aan het uitwisselen van persoonsgegevens gelden onverkort voor het gebruik van e-mail binnen Suwi. In de wettelijke regeling Suwi staat beschreven dat de Suwi-partijen zorgdragen voor de beveiliging van de gegevensuitwisseling tegen inbreuken op de beschikbaarheid, de integriteit en de vertrouwelijkheid overeenkomstig de wettelijk gestelde normen.

Deze beveiliging- en privacyeisen hebben effect op de processen in het kader waarvan de informatie-uitwisseling plaatsvindt. De eisen vanuit de WBP laten zich binnen deze proces-

sen vertalen in organisatorische en technische eisen van betrouwbaarheid die zowel betrekking hebben op de deelnemers aan het communicatieproces als op de inhoud van een e-mailbericht. In het projectplan¹ en het functioneel kader² is beschreven hoe de opzet van Suwinet-Mail eruit komt te zien, waarbij rekening wordt gehouden met de eisen van beveiliging en privacy.

2.3 Waardering beveiligingsniveau Suwinet Mail

In het beveiligingsbeleid rondom Suwinet (Beveiliging Suwinet 1.0) wordt betrouwbaarheid van het versturen van Suwinet-Mail vertaald in termen van beschikbaarheid, integriteit en vertrouwelijkheid:

- *Beschikbaarheid* is de mate waarin Suwinet-Mail in bedrijf is en de informatie beschikbaar is op het moment dat de organisatie deze nodig heeft. Vanuit efficiencyoverwegingen is de beschikbaarheid van Suwinet-Mail *wenselijk*;
- *Integriteit* is de mate waarin Suwinet-Mail zonder fouten is. Binnen het Suwinet domein worden per definitie persoonsgegevens uitgewisseld. De integriteit is derhalve *belangrijk*;
- *Vertrouwelijkheid* is de mate waarin toegang tot Suwinet-Mail en kennisname van informatie is beperkt tot een beperkte groep gerechtigden. De eis van vertrouwelijkheid wordt gesteld vanuit de leverende processen omdat de verzender van persoonsgegevens vanuit de WBP wordt aangemerkt als verantwoordelijke. Deze verantwoordelijkheid houdt in dat de leverende organisatie er zeker van is dat de ontvangende organisatie zorgvuldig omgaat met de verstuurd gegevens. Ook is de ontvangende organisatie vanuit de WBP gehouden aan de verantwoordelijkheid voor de bescherming van de gegevens. De eis van vertrouwelijkheid wordt derhalve als *essentieel* onderkend.

In het kader van het informatiebeveiligingsbeleid voor Suwinet zijn hierover eisen gesteld en afspraken gemaakt.

¹ Projectplan F5 Mail via besloten netwerk binnen de keten Werk en Inkomen, BKWI

² Functioneel Kader F5 Mail via besloten netwerk, BKWI
Risico-analyse Suwinet-Mail

In onderstaande tabel is een vertaling van de waardering gemaakt naar de eisen die aan Suwinet-Mail kunnen worden gesteld in het kader van betrouwbaarheid.

betrouwbaarheidseis	Waardering		
	Wenselijk	Belangrijk	essentieel
	een zekere mate van beveiliging wordt op prijs gesteld	beveiliging is absoluut nodig, gezien de belangen van de organisatie	beveiliging is primair criterium en verplicht voor de organisatie
Beschikbaarheid	<u>Noodzakelijk</u> een enkele keer uitval is aanvaardbaar	<u>Wezenlijk</u> nauwelijks uitval gedurende de openingstijd	<u>onmisbaar</u> slechts in uitzonderlijke gevallen niet operationeel
Integriteit	<u>Actief</u> bedrijfsproces tolereert enkele fouten	<u>Detecteerbaar</u> een zeer beperkt aantal fouten is toegestaan	<u>onontbeerlijk</u> bedrijfsproces eist foutloze informatie
Exclusiviteit	<u>Afgeschermd</u> gegevens alleen ter inzage voor een bepaalde groep	<u>Cruciaal</u> gegevens alleen toegankelijk voor direct betrokkenen	<u>dwingend</u> de gegevens zijn strikt vertrouwelijk; bedrijfsbelangen worden ernstig geschaad als ongeautoriseerden toegang krijgen

3. Risico inschatting op verschillende niveaus

De eisen die aan Suwinet-Mail worden gesteld in het kader van beveiliging en privacy, zijn in het vorige hoofdstuk beschreven. In dit hoofdstuk zullen de risico's op het gebied van de beveiliging en privacy van Suwinet-Mail worden beschreven.

In de huidige opzet van Suwinet-Mail zijn de volgende risiconiveaus te onderkennen, deze zijn gecategoriseerd naar:

- a) Inhoud van het e-mailbericht;
- b) Transport van het e-mailbericht, te weten risico's op het gebied van;
 - infrastructuur;
 - authenticiteit;
 - routing;
 - verantwoordelijkheid;
- c) Archivering van het e-mailbericht.

3.1 Risico's ten aanzien van de inhoud van het e-mailbericht

Inhoudelijk juist gebruik persoonsgegevens niet controleerbaar

E-mail heeft de inherente eigenschap dat het ongestructureerde informatie bevat en het een medium is dat informele communicatie in de hand kan werken. Hierdoor is de inhoud van de berichtenuitwisseling redelijkerwijs niet structureel te controleren op formele eisen in het kader van de WBP (doelbinding, ter zake dienend, toereikend, et cetera). Ook kan er redelijkerwijs geen structurele validatie plaatsvinden op de juistheid en nauwkeurigheid van de verzonden informatie. Een risico dat hier direct mee te maken heeft, is dat de afzender gestructureerde informatie via e-mail kan versturen. Dit is onwenselijk, aangezien de controle op de procesgang bij het gebruik van e-mail niet gegarandeerd is. Het is redelijkerwijs niet mogelijk structureel de inhoud van e-mailberichten te controleren op naleving van de formele regels die aan de inhoud worden gesteld. Er zou wel gebruik kunnen worden gemaakt van het steekproefsgewijs controleren van e-mail op de naleving van de WBP.

Aangezien de afzender op dit moment via andere diverse communicatiemiddelen (telefoon, documenten, etc.) reeds omgaat met persoonsgegevens, waarbij het gebrek aan controle-

mogelijkheden niet als probleem gezien wordt, wordt dit risico voor Suwinet-Mail als beperkt gezien. Een handreiking over het gebruik van e-mail binnen Suwi is opgesteld ten behoeve van de gebruikers en hierin wordt duidelijk gewezen op de verantwoordelijkheden van de afzender en geadresseerden.

3.2 Risico's ten aanzien van het transport van het e-mailbericht

3.2.1. Infrastructuur

Er bestaat een afbreukrisico voor beveiliging Suwinet

In de Rapportage Beveiliging Suwinet³ wordt door de Security Officer van het BKWI de conclusie getrokken omtrent de beveiliging van Suwinet dat het geheel aan procedures en maatregelen van de beveiliging van Suwinet bij elk van de afzonderlijke Suwi-organisaties nog niet voldoet aan de wettelijke eis en dat de rapportages niet op elkaar aansluiten. Dientengevolge kunnen we stellen dat er een afbreukrisico bestaat voor de beveiliging van Suwinet en dat we bij het geheel aan procedures en maatregelen ten behoeve van de beveiliging van Suwinet niet alle risico's kunnen overzien en dat er een risico bestaat dat misbruik wordt gemaakt van de beschikbaar gestelde gegevens waarbij de privacy van cliënten geschonden kan worden. Dit afbreukrisico blijft bestaan zolang iedere partij die zelf verantwoordelijk is voor de eigen invulling van het beveiligingsbeleid voor Suwinet, dit volgens eigen interpretatie kan doen. Hierbij vormt de zwakste schakel een risico voor het totaal. Dit risico wordt middels een Gemeenschappelijke Verantwoordingsrichtlijn en bijbehorend Normenkader inzichtelijk gemaakt en door het structureel zoeken en vinden van oplossingen beheersbaar gemaakt.

In deze rapportage wordt derhalve de conclusie getrokken dat ten aanzien van de beveiliging van Suwinet een risico bestaat dat misbruik wordt gemaakt van de beschikbaar gestelde gegevens waardoor privacy van cliënten geschonden kan worden, maar dat dit een geaccepteerd risico is. Vanzelfsprekend geldt bovenstaande ook ten aanzien van Suwinet Mail.

3.2.2 Authenticiteit

Er is geen controle op ongeschonden berichtgeving en juistheid afzender

³ Rapportage beveiliging Suwinet, BKWI, 2 juli 2003
Risico-analyse Suwinet-Mail

Er is binnen de huidige opzet van Suwinet-Mail geen garantie voor de afzender en de ontvanger van de e-mail dat een bericht in ongeschonden staat arriveert (integriteit). Ook kan de geadresseerde niet met zekerheid weten of het bericht afkomstig is van degene die beweert de afzender te zijn (vertrouwelijkheid). Deze aspecten gelden echter ook voor telefoon en briefverkeer.

De kans dat dit zich voordoet is klein, omdat dit technische kennis vereist.

De afzender ontvangt geen ontvangstbericht

In de huidige opzet is er geen mogelijkheid dat de afzender zeker weet dat de ontvanger in staat is het bericht te lezen, of dat de ontvanger ook daadwerkelijk de beoogde ontvanger is. De afzender ontvangt van de geadresseerde in de huidige opzet geen ontvangstbericht. Dit houdt een risico in voor de afzender, daar deze volgens de WBP verantwoordelijk is voor de inhoud en de juiste overdracht van het bericht.

Adresseren juiste personen niet ondersteund

Er geldt verder dat *alleen* de juiste ontvanger van het bericht in staat mag zijn het bericht te lezen. De verdeling van taken, verantwoordelijkheden en bevoegdheden van de diverse organisaties leggen formele eisen op ten aanzien van de juiste adressering van personen in de Suwi keten. Ook bij Suwinet-Mail bestaat een risico dat een afzender die via Suwinet-Mail een bericht stuurt niet op de hoogte is van de bevoegdheden van de geadresseerde. Het kan dus gebeuren dat privacy gevoelige cliëntinformatie wordt gelezen door een niet bevoegde functionaris. Een adressenboek of directory waarin inzicht is in de functiegegevens van de medewerkers binnen de Suwiketen ontbreekt. Ook bestaat de kans op het foutief invoeren van een e-mailadres. Met behulp van een adressenboek kunnen typefouten voorkomen worden, echter het verkeerd adresseren is ook eenvoudiger.

Systeembeheerders kunnen inzage hebben in privacy gevoelige berichten

Voor de mailservers van de organisaties die gebruik gaan maken van Suwinet-Mail geldt dat de mogelijkheid bestaat dat systeembeheerders inzage kunnen hebben in privacy gevoelige berichten. Een dergelijk risico dient afgedekt te zijn door het afsluiten van de inhoud van e-mailberichten voor systeembeheerders en door het opnemen van een geheimhoudingsverklaring in het arbeidscontract van een systeembeheerder. Voor mailservers die niet bij organisaties binnen de Suwiketen staan, maar waar bij en juist gebruik van Suwinet-Mail wel

Suwi mail terecht kan komen, is het vanzelfsprekend onmogelijk om maatregelen te nemen. Doordat mail echter wel het Internet op kan (zie boven) is dit een groot risico. Dit risico beperkt zich niet tot Suwinet-Mail, maar heeft betrekking tot de gehele ICT-infrastructuur.

3.2.3 Routing

Routing e-mail buiten besloten domein Suwinet mogelijk

Buiten het feit dat de afzender niet zeker kan weten of de geadresseerde het bericht ontvangen heeft, is een garantie vanuit Suwinet-Mail dat de e-mail veilig is aangekomen in de huidige opzet niet te geven. Dit heeft meerdere oorzaken:

- om een gebruiker in staat te stellen e-mail naar een andere gebruiker te sturen over het Suwinet is besloten dat de gebruiker bij een GSD een toevoeging moet plaatsen achter het reguliere adres van de gebruiker naar wie hij of zij wenst te mailen. Deze toevoeging is '.suwi'. CWI en het UWV hebben echter aangegeven deze toevoeging niet in het e-mailadres op te nemen. Dit heeft tot gevolg dat de herkenbaarheid van een e-mail aan geadresseerden binnen UWV en CWI afneemt. Door het weglaten van de toevoeging '.suwi' is in de huidige opzet het verschil tussen interne (via Suwinet) en externe mail (via Internet) niet zichtbaar.
- Door middel van het gebruik van mailservertabellen binnen het CWI en het UWV hebben e-mailberichten die gericht zijn aan Suwipartners niet de toevoeging '.suwi' maar deze berichten worden op basis van de mailservertabellen over Suwinet gerouteerd. e-Mail domeinnamen die niet in deze tabellen zijn opgenomen, worden via het Internet gerouteerd. Daar UWV en CWI geen gebruik maken van de toevoeging '.suwi' zal de afzender binnen het UWV en CWI een mogelijkheid moeten hebben om te controleren of de domeinnaam in de mailservertabel is opgenomen, anders bestaat de mogelijkheid dat e-mail alsnog via het Internet gerouteerd wordt.
- niet alle gemeenten zullen worden aangesloten op Suwinet-Mail. Deze gemeenten zullen de e-mail die zij ontvangen via het openbare internet toegezonden krijgen. Voor een afzender van e-mail, die vanuit de WBP verantwoordelijk is voor het bericht, is door het vervallen van de toevoeging '.suwi' niet zichtbaar of een gemeente wel of niet is aangesloten op Suwinet-Mail. De centrale organisaties van CWI en UWV zullen heldere richtlijnen moeten opstellen en moeten communiceren over welke gemeenten het hier betreft.

Suwinet-Mail berichten niet herkenbaar binnen CWI en UWV

De toevoeging ‘.suwi’ voegt maar heel weinig toe aan de herkenbaarheid van de ontvanger, daarnaast is ieder verplicht netjes om te gaan met persoonsgegevens.

Een geautomatiseerde oplossing is echter nog niet mogelijk. Dit risico is kleiner naar mate er meer gemeentes deelnemen aan Suwinet-Mail. Wanneer maar een klein aantal gemeenten deelneemt aan Suwinet-Mail, zal de beslissing omtrent de toevoeging ‘.suwi’ moeten worden herzien.

3.2.4. Verantwoordelijkheid

Er is geen duidelijke verantwoordelijkheidsstructuur voor Suwinet Mail

Er is binnen de huidige opzet van Suwinet-Mail geen duidelijkheid over de grenzen aan de verantwoordelijkheid van de afzender. Deze verantwoordelijkheid houdt in dat de leverende organisatie er zeker van is dat de ontvangende organisatie zorgvuldig omgaat met de verstuurd gegevens. Ook is de ontvangende organisatie vanuit de WBP gehouden aan de verantwoordelijkheid voor de bescherming van de gegevens. Deze verantwoordelijkheden moeten vertaald worden naar de logistieke grenzen van deze verantwoordelijkheid. Er moet worden vastgesteld tot welk moment in de elektronische overdracht de afzender verantwoordelijk is en vanaf welk moment in de elektronische overdracht de geadresseerde verantwoordelijk is.

De verantwoordingsstructuur is een geaccepteerd risico, omdat dit ook geldt voor andere communicatiemediën, zoals briefwisseling en telefoonverkeer.

3.2.5. Regels en afspraken

Een apart risico bestaat uit het feit dat mensen zich niet altijd aan regels en gemaakte afspraken houden

Dit aspect vormt een groot risico, maar is niet specifiek voorbehouden aan Suwinet-Mail.

3.3 Risico's betreffende het archiveren van e-mailberichten

Beveiliging van opslag van e-mail voor dossiervorming niet vormgegeven

Vanuit de WBP wordt gesteld dat een cliënt recht heeft op inzage, verbetering, aanvulling, verwijdering en verzet van zijn of haar persoonsgegevens. Dit stelt eisen aan de opslagmogelijkheid en de bewaartermijn van elektronische informatieverwerking, zo ook e-mail, die medewerkers binnen de Suwi-organisaties ontvangen. In het projectplan Suwinet-Mail wordt geen rekening gehouden met deze eis. Eisen die gesteld worden (ook vanuit de WWB) aan dossiervorming van het e-mailverkeer, zijn vertaald in het informatiebeveiligingsbeleid van de

Suwi-organisaties en gelden onverminderd voor Suwinet-Mail. Daarbij moet medewerkers de mogelijkheid geboden worden om berichten gedurende een bepaalde termijn te kunnen archiveren.

De mogelijkheid tot elektronische of fysieke dossiervorming van privacygevoelige informatie dient bij de participerende organisaties te worden gewaarborgd. In het geval dat e-mail in een fysiek dossier moeten worden opgeslagen zullen printers aanwezig moeten zijn die niet in publieke ruimten mogen staan. Bij het archiveren van elektronische berichten dienen de toegangswegen tot de elektronische opslagplaats (PC's, netwerken) afdoende beveiligd te zijn tegen inbraak van binnen en buiten de organisatie, door afscherming middels, firewalls, passwords, en dergelijke.

	Aspect	Situatie	Maatregelen
3.1 Risico's ten aanzien van de inhoud van het e-mailbericht	<i>Inhoudelijk juist gebruik persoonsgegevens niet controleerbaar</i>	<p>E-mail heeft de inherente eigenschap dat het ongestructureerde informatie bevat en het een medium is dat informele communicatie in de hand kan werken. Hierdoor is de inhoud van de berichtenuitwisseling nauwelijks structureel te controleren op formele eisen in het kader van de WBP (doelbinding, ter zake dienend, toereikend, et cetera).</p> <p>Ook kan er geen structurele validatie plaatsvinden op de juistheid en nauwkeurigheid van de verzonden informatie.</p> <p>Een risico dat hier direct mee te maken heeft, is dat een afzender gestructureerde informatie via e-mail kan versturen. Dit is onwenselijk, aangezien de controle op de procesgang bij het gebruik van e-mail niet gegarandeerd is. Het is redelijkerwijs niet mogelijk de inhoud van alle e-mail te controleren op naleving van de formele regels die aan de inhoud worden gesteld.</p>	<p>Binnen de Suwi-organisaties zullen ten aanzien van de informatievoorziening (in het kader van de WBP) gedragsregels opgesteld moeten zijn hoe om te gaan met privacygevoelige informatie. Dit is niet alleen gericht op het e-mail gebruik, maar geldt ook voor brieven, telefoon- en faxverkeer. Wanneer de Suwinet-Mail gebruikers zich houden aan de instructies in de handreiking, zal de inhoud van de e-mail berichten dit risico terugbrengen tot acceptabele proporties.</p> <p>Net als bij briefwisseling en telefoonverkeer is het redelijkerwijs niet mogelijk de inhoud van alle e-mail te controleren op naleving van de formele regels die aan de inhoud worden gesteld. Het steekproefsgewijs controleren van e-mail op de naleving van de WBP is theoretisch haalbaar, maar in de praktijk is het algemeen gebruikelijk dit te beperken tot die situaties waarbij een reële verdenking op misbruik bestaat.</p> <p>Voor dit aspect liggen de risico's dus binnen acceptabele grenzen. In de Handreiking is aangegeven dat Suwinet-Mail hier niet voor is bedoeld.</p>
3.2.1. Infrastructuur	<i>Er bestaat een afbreukrisico voor beveiliging Suwinet</i>	In de Rapportage Beveiliging Suwinet wordt door de Security Officer van het BKWI gemeld dat het geheel aan procedures en maatregelen van de beveiliging van Suwinet bij elk van de afzonderlijke Suwi-organisaties nog niet voldoet aan de wettelijke eis en dat de rapportages hierover niet op elkaar aansluiten.	Dit risico geldt niet specifiek voor Suwinet-Mail en middels de jaarlijkse edp-audit bij de Suwi-organisaties en het jaarlijkse bijsturen via het Jaarplan spannen de Suwi-partijen zich in de informatiebeveiliging op een hoger niveau te brengen

		Dientengevolge kunnen we niet alle risico's overzien en bestaat het risico dat misbruik wordt gemaakt van de beschikbaar gestelde gegevens waarbij de privacy van cliënten geschonden kan worden.	Dit risico ligt voor Suwinet-Inkijk binnen acceptabele grenzen. Door de Handreiking, waarin vermeld staat wat wel en wat niet via Suwinet-Mail verstuurd mag worden, geldt dit ook voor Suwinet-Mail.
3.2.2 Authenticiteit	<i>Er is geen controle op ongeschonden berichtgeving en juistheid afzender</i>	Er is binnen de huidige opzet van Suwinet-Mail geen garantie voor de afzender en de ontvanger van de e-mail dat een bericht in ongeschonden staat arriveert. De geadresseerde kan niet met zekerheid weten of het bericht afkomstig is van degene die beweert de afzender te zijn.	Het is lastiger de inhoud van e-mailberichten te wijzigen, dan inhoud van brieven. Voor het wijzigen e-mailberichten is specialistische kennis nodig. Gebruikers krijgen via de Handreiking te weten welke verantwoordelijkheid zij hebben t.a.v. controle op inkomende en uitgaande e-mailberichten. Hierdoor is dit een beperkt en acceptabel risico. Het is lastiger de route van e-mailberichten te wijzigen, dan het onderscheppen van brieven. Hiervoor is niet alleen specialistische kennis, maar ook nog een organisatorische positie nodig. Bij gebruik van Suwinet-Mail binnen de grenzen zoals beschreven in de Handreiking voor Suwinet-Mail is de kans dat dit zich voordoet is echter zeer klein. Hierdoor is het risico teruggebracht tot een acceptabel niveau.
	<i>De afzender ontvangt geen ontvangstbericht</i>	In de huidige opzet is er geen mogelijkheid dat de afzender zeker weet dat de ontvanger in staat is het bericht te lezen, of dat de ontvanger ook daadwerkelijk de beoogde ontvanger is. De afzender ontvangt van de geadresseerde in de huidige opzet geen ontvangstbericht. Dit houdt een risico in voor de afzender, daar deze volgens de WBP verantwoordelijk is voor de inhoud en de juiste overdracht van het bericht.	Dit risico is vergelijkbaar aan de risico's welke verbonden zijn aan het gebruik van brief- en faxverkeer en wordt derhalve als acceptabel beschouwd.
	<i>Adresseren juiste personen niet ondersteund</i>	Er geldt verder dat <i>alleen</i> de juiste ontvanger van het bericht in staat mag zijn het bericht te lezen. De verdeling van taken, verantwoordelijkheden en bevoegdheden van de diverse organisaties leggen formele eisen op ten aanzien van de juiste adressering van personen in de Suwiketen.	Hiervoor zijn geen technische voorzieningen.

		<p>Ook binnen Suwinet-Mail bestaat een risico dat een afzender die via Suwinet-Mail een bericht stuurt niet op de hoogte is van de bevoegdheden van de geadresseerde. Het kan dus gebeuren dat privacy gevoelige cliëntinformatie wordt gelezen door een niet bevoegde functionaris. Een adressenboek of directory waarin inzicht is in de functiegegevens van de medewerkers binnen de Suwiketen ontbreekt. Ook bestaat de kans op het foutief invoeren van een e-mailadres. Met behulp van een adressenboek kunnen typfouten voorkomen kunnen worden, echter het verkeerd adresseren is ook eenvoudiger.</p>	<p>In de Handreiking Suwinet-Mail wordt op de verantwoordelijkheid van de gebruikers gewezen t.a.v. het controleren van de juiste adressen, waardoor dit risico beperkt blijft.</p>
	<p><i>Systeembeheerders kunnen inzage hebben in privacy gevoelige berichten</i></p>	<p>Voor de mailservers van de organisaties die gebruik gaan maken van Suwinet-Mail geldt dat de mogelijkheid bestaat dat systeembeheerders inzage kunnen hebben in privacy gevoelige berichten. Een dergelijk risico dient afgedekt te zijn door het afsluiten van de inhoud van e-mailberichten voor systeembeheerders en door het opnemen van een geheimhoudingsverklaring in het arbeidscontract van een systeembeheerder.</p> <p>Voor mailservers die niet bij organisaties binnen de Suwiketen staan, maar waar bij onjuist gebruik van Suwinet-Mail wel e-mailberichten vanuit Suwinet-Mail terecht kunnen komen, is het vanzelfsprekend onmogelijk om maatregelen te nemen. Doordat mail echter wel het Internet op kan (zie boven) is dit een groot risico.</p>	<p>Dit risico beperkt zich niet tot Suwinet-Mail, maar heeft betrekking tot de gehele ICT-infrastructuur en binnen de informatiebeveiligingsplannen van de verschillende Suwi-organisaties dient het aspect van autorisaties van beheerders n maatregelen genomen te zijn.</p> <p>Ten aanzien van het risico aangaande systeembeheerders, kan door de inhoud van e-mailberichten af te sluiten voor systeembeheerders en door het opnemen van een geheimhoudingsverklaring in het arbeidscontract het risico beperkt worden.</p> <p>Voor mailservers die niet bij organisaties binnen de Suwiketen staan, maar waar wel e-mailberichten vanuit Suwinet-Mail terecht kunnen komen, is het vanzelfsprekend onmogelijk om maatregelen te nemen, maar wanneer de gebruikers van Suwinet-Mail zich houden aan de maatregelen beschreven in de Handreiking en 'netjes' omgaan met de mailvoorziening, is ook dit risico binnen acceptabele grenzen teruggebracht.</p>

<p>3.2.3 Routing</p>	<p><i>Routing e-mail buiten besloten domein Suwinet mogelijk</i></p>	<p>Buiten het feit dat de afzender niet zeker kan weten of de geadresseerde het bericht ontvangen heeft, is een garantie vanuit Suwinet-Mail dat de e-mail veilig is aangekomen in de huidige opzet niet te geven. Dit heeft meerdere oorzaken:</p> <ul style="list-style-type: none"> · om een gebruiker in staat te stellen e-mail naar een andere gebruiker te sturen over het Suwinet is besloten dat de gebruiker bij een GSD een toevoeging moet plaatsen achter het reguliere adres van de gebruiker naar wie hij of zij wenst te mailen. Deze toevoeging is '.suwi'. · Door middel van het gebruik van mailservertabellen binnen het CWI en het UWV zullen e-mailberichten die gericht zijn aan Suwipartners niet de toevoeging '.suwi' krijgen, maar op basis van de tabellen over Suwinet worden gerouteerd. e-Mail domeinnamen die niet in deze tabellen zijn opgenomen, worden via het Internet gerouteerd. Daar UWV en CWI geen gebruik maken van de toevoeging '.suwi' zal de afzender binnen het UWV en CWI een mogelijkheid moeten hebben om te controleren of de domeinnaam in de mailservertabel is opgenomen, anders bestaat de mogelijkheid dat e-mail alsnog via het Internet gerouteerd wordt. 	<p>Dit risico bestaat bij het briefverkeer ook, waarvoor aangetekend briefverkeer is ontstaan. Naast het feit dat in e-mailberichten binnen Suwinet-Mail, zoals in de Handreiking vermeld, niet zomaar alle informatie verstuurd mag worden, bestaat ook hier de mogelijkheid dat de afzender zich overtuigt van de aankomst van het bericht, door een telefoontje te plegen. De gebruikers binnen de GSD-organisaties krijgen via de Handreiking duidelijke instructies aangaande het adresseren van Suwinet-Mail.</p> <p>Als gevolg van de afwezigheid van de toevoeging '.suwi', bij de CWI- en UWV-organisaties, zullen de diverse mailservertabellen up-to-date moeten worden gehouden.</p> <p>De Suwinet-Mail gebruikers moeten duidelijke instructies krijgen omtrent het zorgvuldig omgaan met het adresseren van Suwinet-Mail berichten.</p>
-----------------------------	--	--	---

		<p>niet alle gemeenten zijn aangesloten op Gemnet (het interne netwerk van de gemeenten). Deze gemeenten zullen de e-mail die zij ontvangen via Internet toegezonden krijgen. Voor een afzender van e-mail, die vanuit de WBP verantwoordelijk is voor het bericht, is door het vervallen van de toevoeging '.suwi' niet zichtbaar of een gemeente wel of niet is aangesloten op Gemnet. De centrale organisaties van CWI en UWV zullen heldere richtlijnen moeten opstellen en moeten communiceren over welke gemeenten het hier betreft.</p>	<p>Een geautomatiseerde oplossing is echter nog niet mogelijk. Dit risico is kleiner naar mate er meer gemeentes deelnemen aan Suwinet-Mail. Wanneer maar een klein aantal gemeenten deelneemt aan Suwinet-Mail, zal de beslissing omtrent de toevoeging '.suwi' moeten worden herzien. Naar mate het aantal Gemeenten beperkt blijft vormt dit een groter risico. Bij een te beperkt aantal deelnemende gemeenten zal de beslissing omtrent de toevoeging '.suwi' heroverwogen moeten worden.</p>
	<i>e-Mail vanuit Suwinet-mail niet herkenbaar binnen CWI en UWV</i>	<p>Het afzien van de toevoeging '.suwi' heeft tot gevolg dat de herkenbaarheid van e-mail aan geadresseerden binnen UWV en CWI afneemt en is in de huidige opzet het verschil tussen interne (via Suwinet) en externe mail (via Internet) niet zichtbaar.</p>	<p>De toevoeging '.suwi' voegt maar weinig toe aan de herkenbaarheid van de ontvanger. De Handreiking stelt heldere regels ten aanzien van het gebruik van persoonsgegevens, waardoor sprake is van een beperkt risico.</p>
3.2.4. Verantwoordelijkheid	<i>Er is geen duidelijke verantwoordelijkheidsstructuur voor Suwinet Mail</i>	<p>Er is binnen de huidige opzet van Suwinet-Mail geen duidelijkheid over de grenzen aan de verantwoordelijkheid van de afzender. Deze verantwoordelijkheid houdt in dat de leverende organisatie er zeker van is dat de ontvangende organisatie zorgvuldig omgaat met de verstuurd gegevens. Ook is de ontvangende organisatie vanuit de WBP gehouden aan de verantwoordelijkheid voor de bescherming van de gegevens. Deze verantwoordelijkheden moeten vertaald worden naar de logistieke grenzen van deze verantwoordelijkheid.</p>	<p>Er moet worden vastgesteld tot welk moment in de elektronische overdracht de afzender verantwoordelijk is en vanaf welk moment in de elektronische overdracht de geadresseerde verantwoordelijk is.</p> <p>Omdat dit aspect ook geldt voor andere communicatiemedi, zoals briefwisseling en telefoonverkeer mag gesteld worden dat de verantwoordingsstructuur een geaccepteerd risico is.</p>

3.3 Risico's ten aanzien van archivering van het e-mailbericht	<i>Beveiliging van opslag van e-mail voor dossiervorming niet vormgegeven</i>	Vanuit de WBP wordt gesteld dat een cliënt recht heeft op inzage, verbetering, aanvulling, verwijdering en verzet van zijn of haar persoonsgegevens. Dit stelt eisen aan de opslagmogelijkheid en de bewaartermijn van elektronische informatieverwerking, zo ook e-mail, die medewerkers binnen de Suwi-organisaties ontvangen. In het projectplan Suwinet-Mail wordt geen rekening gehouden met deze eis. Eisen die gesteld worden (ook vanuit de WWB) aan dossiervorming van het e-mailverkeer, zijn vertaald in het informatiebeveiligingsbeleid van de Suwi-organisaties en gelden onverminderd voor Suwinet-Mail. Daarbij moet medewerkers de mogelijkheid geboden worden om berichten gedurende een bepaalde termijn te kunnen archiveren. De mogelijkheid tot elektronische of fysieke dossiervorming van privacygevoelige informatie dient bij de participerende organisaties te worden gewaarborgd. In het geval dat e-mail in een fysiek dossier moeten worden opgeslagen zullen printers aanwezig moeten zijn die niet in publieke ruimten mogen staan. Bij het archiveren van elektronische berichten dienen de toegangswegen tot de elektronische opslagplaats (PC's, netwerken) afdoende beveiligd te zijn tegen inbraak van binnen en buiten de organisatie, door afscherming middels passwords, firewalls, en dergelijke.	Dit aspect moet in het informatiebeveiligingsplannen van de Suwi-organisaties opgenomen zijn. Voor Suwinet-Mail wordt dit dan ook als een laag risico gezien.
3.4 Human aspect	<i>Een apart risico bestaat uit het feit dat mensen zich niet altijd aan regels en gemaakte afspraken houden</i>	Het menselijk handelen vormt in vele opzichten een groot veiligheidsrisico, zo ook binnen de informatievoorziening. Dit aspect is niet specifiek voorbehouden aan Suwinet-Mail.	Om dit risico te beperken moeten de gebruikers van Suwinet-Mail enerzijds duidelijke instructies krijgen hoe Suwinet-Mail te gebruiken, met daarbij belicht wat wel en wat niet via Suwinet-Mail verstuurd mag worden; en anderzijds zal binnen de verschillende Suwi-organisaties, onder andere middels de edp-audit, controle uitgeoefend worden op de naleving.

4. Conclusie en aanbevelingen

In dit hoofdstuk worden de belangrijkste conclusies uit het vorige hoofdstuk kort herhaald en worden aanbevelingen gegeven voor het beperken van de risico's van Suwinet Mail.

4.1 Conclusies risico-analyse Suwinet Mail

In de huidige opzet van Suwinet-Mail is er geen garantie dat:

- de afzender van een bericht aantoonbaar zeker kan weten dat alleen de juiste ontvanger van het bericht in staat is het bericht te lezen (vertrouwelijkheid) en wel in ongeschonden staat (integriteit) en dat de inhoud van het bericht niet in strijd is met de WBP (privacy) en
- de ontvanger van een bericht aantoonbaar zeker kan weten dat het bericht dat hij of zij leest afkomstig is van degene die beweert het gestuurd te hebben (vertrouwelijkheid) en in ongeschonden staat is aangekomen (integriteit).

Ook is de kans op inbraak van buiten het besloten netwerk, bij onjuist gebruik van Suwinet-Mail is het routeren van e-mail via het Internet mogelijk, niet gegarandeerd.

Bovenstaande conclusie wordt getrokken op basis van de volgende bevindingen:

- het inhoudelijk controleren op een juist gebruik van persoonsgegevens is niet mogelijk;
- over de beveiliging van Suwinet is in een recente rapportage geconcludeerd dat er een afbreukrisico bestaat voor de beveiliging van Suwinet;
- er is geen enkele controle naar het ongeschonden arriveren van een e-mailbericht;
- er is geen enkele controle naar de juistheid van een afzender;
- de afzender ontvangt geen ontvangstbericht waardoor niet te controleren is of een bericht bij de juiste persoon is aangekomen;
- het adresseren van de juiste personen (zowel wat betreft adres als functie) wordt niet ondersteund met bijvoorbeeld een adresboek;
- systeembeheerders kunnen inzage hebben in privacy gevoelige berichten;
- routing van e-mail buiten het besloten domein van Suwinet is in de huidige opzet mogelijk. In de volgende drie gevallen kan hier sprake van zijn:
 1. Een gebruiker maakt een typefout in het adres
 2. De domeinnaam van de ontvanger staat niet in de mailservertabel bij UWV of CWI

3. Een e-mail wordt vanuit een gemeente zonder toevoeging `.suwi`` verstuurd.
- Suwimail is niet herkenbaar binnen het UWV en CWI domein;
 - er is geen duidelijke verantwoordelijkheidsstructuur voor Suwinet Mail;
 - beveiliging van opslag van e-mail voor dossiervorming niet vormgegeven.

De algemene conclusie van deze risicoanalyse luidt dan ook dat Suwinet-Mail in zijn huidige opzet niet voldoet aan de wettelijke eisen van betrouwbaarheid, in termen van integriteit en vertrouwelijkheid. Daarentegen moet geconstateerd worden dat dit ook gesteld kan worden van telefoon-, fax- en en briefverkeer, waarbij de risico's als op een acceptabel niveau gezien worden.

4.2 Aanbevelingen

Het uitwisselen van berichten met privacygevoelige informatie stelt hoge eisen aan de beschikbaarheid, integriteit en vertrouwelijkheid van Suwinet Mail. In zijn huidige opzet voldoet Suwinet-Mail niet aan deze eisen.

In zijn huidige opzet voldoet Suwinet-Mail niet aan de eisen van beschikbaarheid, integriteit en vertrouwelijkheid. Op dit moment is het voor medewerkers van de partijen binnen het Suwi-domein eenvoudig en mogelijk om cliëntgevoelige informatie via e-mail over het openbare internet te verspreiden, derhalve is het gebruik van Suwinet-Mail een duidelijke verbetering ten opzichte van de huidige situatie.

Om bij de routing van e-mail binnen Suwinet-Mail zo veel mogelijk fouten te voorkomen, kunnen een aantal maatregelen worden genomen op korte termijn, die ervoor zorgen dat Suwinet-Mail in het gebruik beter voldoet aan de eis van vertrouwelijkheid. De volgende maatregelen zijn van belang:

- het strekt tot de aanbeveling de gebruikers bewust te laten worden van de gevolgen die onjuist versturen van privacygevoelige e-mail kan hebben. In dit bewustwordingsprogramma dient te worden aangegeven welke maatregelen gebruikers zelf kunnen nemen om op een juiste manier met het versturen van deze e-mail om te gaan.
- het CWI en het UWV dienen zich bewust te zijn van het belang van het *up to date* houden van de mailservertabellen die zorgen voor een juiste routing van e-mail binnen het Suwidomein. Daarnaast dienen het UWV en het CWI toepassingen beschikbaar te hebben waarmee gebruikers in de organisatie kunnen controleren of de geadresseerde van e-mail binnen het Suwidomein valt.

- Nadrukkelijk moeten de gebruikers gewezen worden op de Handleiding en op de noodzaak van het naleven van de richtlijnen uit de handreiking.

Deze beide maatregelen die de verantwoordelijkheid van de gebruiker moeten vergroten, zullen een positieve werking hebben op het op correcte wijze versturen van privacygevoelige e-mail en is zeker een verbetering ten opzichte van de huidige situatie.

Het verdient daarnaast de aanbeveling om de architectuur van Suwinet Mail⁴ zodra hiervoor draagvlak is gecreëerd te herzien. In deze herziene architectuur van Suwinet-Mail dienen ten aanzien van beveiliging en privacy de volgende inrichtingskeuzes te worden geadresseerd:

- de vertaling van de organisatorische bevoegdhedenstructuur naar een elektronische omgeving.
- de afdoende *end to end* beveiliging die plaats moet vinden bij de e-mail uitwisseling van geadresseerde naar afzender (dit heeft mede betrekking op het routeringsvraagstuk en de beveiliging van Suwinet).
- de garantie van de betrouwbaarheid van berichtenuitwisseling (bijvoorbeeld door gebruikmaking van encryptie, het Inlichtingen Bureau als uitgever van sleutels, etc.) en de operationalisering van de verantwoordelijkheid van afzender en geadresseerde.
- de eisen die worden gesteld aan de inhoud van het berichtverkeer en de wijze waarop gebruikers en systeembeheerders kunnen worden geïnstrueerd.

Deze inrichtingskeuzes staan niet op zich, maar vormen mede de totale architectuur van Suwinet Mail. Het is van belang dat er de komende tijd gewerkt wordt aan het creëren van draagvlak bij de Suwipartners zodat zij gezamenlijk inzien dat er beleids- en technische keuzes dienen te worden gemaakt om van Suwinet-Mail een veilige e-mailomgeving te maken voor de Suwipartners.

⁴ Met de architectuur van Suwinet-Mail wordt hier bedoeld de logica achter het organiseren van applicaties, data en technische infrastructuur die wordt beschreven in een verzameling beleids- en technische keuzes welke de doelstellingen van Suwinet-Mail moeten realiseren.

Bijlage: Geraadpleegde documenten

Voor de uitvoering van de voorliggende risicoanalyse is gebruik gemaakt van de volgende documenten:

- Beveiliging Suwinet 1.0, Bijlage XIV;
- Rapportage Beveiliging Suwinet, BKWI, 2 juli 2003;
- Functioneel Kader, Mail via besloten netwerk, BKWI, 11 april 2003;
- Handreiking Suwinet – Mail in de praktijk, BKWI, 3 september 2003;
- Projectplan Mail via besloten netwerk binnen de keten Werk en Inkomen, BKWI, 18 september 2003;
- Circulaire Privacykader uitvoering Algemene Bijstandswet, Ministerie van Sociale Zaken en Werkgelegenheid.