Jaarverslag 2014
& outlook 2015

Amsterdam, 7 januari 2015

Ad Reuijl

1. INHOUD

2. HIGHLIGHTS 2014

De meerjarenontwikkeling, die startte in 2012 met het vestigen van de eerste werkverbanden (domeingroepen, conferenties, etc.) en in 2013 werd uitgebreid met de oplevering van concrete producten en handreikingen (zoals voor Secure Software Development (SSD), e-Learning, etc.) heeft in 2014 verdere versterking gekregen met een focus op implementatie. Nadrukkelijk zijn we nu ook bezig geweest met 'de volgende stap': de stap naar meer samen dóen. Voorbeelden hiervan zijn onze betrokkenheid bij Local Box, implementatietrajecten rond SSD en BIR bij meerdere overheidsbedrijven en het mobiliseren van de aanbodkant bij Kennispartners in de markt.

Tegelijkertijd zien we een permanente groei van het netwerk, dat inmiddels ruim 850 mensen telt die bij 200+ organisaties werken en zijn er nieuwe werkvormen ontstaan, die passen bij de 'doefase': de zogenaamde 'Practitioners Communities'.

De domeingroepen voor Ketens, Normatiek, Awareness en Privacy zijn met regelmaat bijeen geweest om te werken aan kennisdeling en –ontwikkeling, een bezigheid die op onderdelen ook geleid heeft tot nieuwe of verbeterde producten. Voor de Domeingroepen Ketens en Privacy zijn nieuwe trekkers aangetreden vanuit resp. SVB (Frank Katsburg) en DUO (Wim Molema). Het voorzitterschap van Domeingroep Awareness was enige tijd vacant. Hierin is inmiddels voorzien door de combinatie van Jan Renshof/Brenno de Winter. Voor het thema Identiteitsfraude is een nieuwe domeingroep ontstaan die getrokken wordt door Wouter Fellendans van het ministerie van BZK.

De benutting van de kennispartners is dit jaar wat sterker vormgegeven. Dit leidt enerzijds tot nieuwe vormen van productcreatie (bijv. materiaal van opleidingsaanbod dat om niet als CIP-product beschikbaar mag worden gesteld) en anderzijds tot een stukje organisatie van de aanbodzijde (bijv. verwerking van SSD in het productaanbod van softwareleveranciers en consultancybedrijven). Het aantal voor het netwerk beschikbare producten is in 2014 flink toegenomen: zie het overzicht in hoofdstuk 3.

Door het jaar heen hebben meerdere kennissessies plaatsgevonden met Kennispartners en enkele kennissessies van het Cyber Security Platform. CIP heeft in 2014 i.s.m. de Rijks-BVA ook het Rijks-ISAC opgezet, dat inmiddels in regulier vaarwater is gekomen en (evenals de reeds bestaande ISAC's) nu wordt gefaciliteerd door het NCSC.

De twee conferenties in 2014 vonden plaats in Kasteel Vanenburg, te Putten. Uitwijk naar deze nieuwe locatie was nodig met het oog op de toenemende belangstelling. De conferenties werden door de resp. 190 en 210 deelnemers weer positief gewaardeerd.

3. BESCHIKBARE PRODUCTEN PU. 31 DECEMBER 2014

Op dit moment zijn de volgende producten uit de CIP-samenwerking vrijgegeven voor algemeen gebruik (onder Creative Commons – Naamsvermelding/Gelijk Delen). De links geven direct toegang tot de producten.

Onderwerp	Product	Doel/omschrijving
Secure Software Development (SSD)	**Grip op SSD: Het proces** http://www.cip-overheid.nl/wp-content/uploads/2014/05/Grip-op-SSD-Het-proces-v1-03.pdf	Proces voor sturing op tot stand brengen en onderhoud van veilige software .
	Grip op SSD: Beveiligingseisen http://www.cip-overheid.nl/wp-content/uploads/2014/10/Grip-op-SSD-Beveiligingseisen-v2_0.pdf	Basisnormenkader als richtsnoer voor veilige software.
	ICT Security Training met SSD-Normen http://www.cip-overheid.nl/wp-content/uploads/2014/05/ICT-Security-Training-met-SSD-normen.pdf	Training voor bouwers en testers voor omgaan met SSD-Normen.
	Receptuur Veilige Software ontwikkeling http://www.cip-overheid.nl/wp-content/uploads/2014/06/ReceptuurVeiligeSoftwareOntwikkeling-lunchsessies-v07_1.pdf	Presentatie met uitleg van de methode Grip op SSD. Te gebruiken voor 'evangelisatie' binnen bijv. de eigen organisatie.
Beveiliging in Inkoopcontracten	Grip op Beveiliging in Inkoopcontracten http://www.cip-overheid.nl/wp-content/uploads/2014/10/Grip-op-Beveiligingsovereenkomsten-v1_0.pdf	Methode en voorbeeld-normenkader voor komen tot beveiligings-afspraken met leveranciers.
Awareness: e-learning-modules	**Bring Your own Device** http://www.cip-overheid.nl/wp-content/uploads/2014/05/20140403_CIP-BYOD.zip	Korte module voor aanleren basisbewustzijn. Over Bring Your Own Device.
	Veilig omgaan met Internet http://www.cip-overheid.nl/wp-content/uploads/2014/05/20140403_CIP-Veilig-omgaan-met-internet.zip	Korte module voor aanleren basisbewustzijn. Over veilig omgaan met internet.
	Social Engineering http://www.cip-overheid.nl/wp-content/uploads/2014/05/20140403_CIP-Social-Engineering.zip	Korte module voor aanleren basisbewustzijn. Over social engineering.
	Fishing http://www.cip-overheid.nl/wp-content/uploads/2014/05/20140403_CIP-Phishing.zip	Korte module voor aanleren basisbewustzijn. Over fishing.

Onderwerp	Product	Doel/omschrijving
	Veilig omgaan met Bezoekers http://www.cip-overheid.nl/wp-content/uploads/2014/05/20140403_CIP-Veilig-omgaan-met-bezoekers.zip	Korte module voor aanleren basisbewustzijn. Over veilige omgang met bezoekers.
	Overheidsnormen http://www.cip-overheid.nl/wp-content/uploads/2014/05/20140403_CIP-Overheidsnormen.zip	Korte module voor aanleren basisbewustzijn. Over normen in de overheid.
Awareness: gebruiks instructies e-learning- modules	**Gebruiken via Pleio:** https://leren.pleio.nl/	Via de link kunnen de modules uitgevoerd worden: Kies cursussen, dan CIP en log in als gast.
	Instructies voor installatie op eigen omgeving http://www.cip-overheid.nl/wp-content/uploads/2014/05/20140515_install-instructies-e_learning_v2.docx	Met deze instructies installeert u de modules op eigen infrastructuur en kunt u ze inbedden in uw eigen leeromgeving.
Awareness: Campagneaanpak	**Borging Awareness Informatieveiligheid** http://www.cip-overheid.nl/wp-content/uploads/2014/05/Borging-awareness-informatiebeveiliging_.pdf	Tips voor organiseren van permanente aandacht voor informatieveiligheid.
	Nadere achtergrondinformatie http://www.cip-overheid.nl/wp-content/uploads/2014/05/Achtergrondinformatie-bij-borging-awareness-informatiebeveiliging.pdf	Nadere uitwerking bij Borging Awareness Informatieveiligheid.
	Publicatie Veranderen is geen kunst http://www.cip-overheid.nl/wp-content/uploads/2014/08/Veranderen-is-geen-kunst-onderzoek.pdf	Enkele waarnemingen m.b.t. de zachte kant in de aanpak van verandering naar informatieveilig gedrag.
	Introductietraining 'Van veilig voelen naar Veilig zijn" http://www.cip-overheid.nl/wp-content/uploads/2014/08/Training-SogetiSecurityAwareness-1_0.pdf	Diapack voor cursusdoeleinden.
Awareness: Overig herbruikbaar materiaal	**Inventarisatie herbruikbaar materiaal** https://cip.pleio.nl/file/group/8737852/all#13324662	Materiaal van een aantal organisaties. Toegang op www.cip.pleio.nl is hiervoor nodig.
	e-Mail Authenticatie http://www.cip-overheid.nl/wp-content/uploads/2014/06/20140528_Emailauthenticatie_def.pdf	Een publicatie over het nut en de wenseljikheid om e-Mailauthenticatie in te zetten.
Keten Governance	**Keten Service Library** http://www.cip-overheid.nl/wp-content/uploads/2014/05/KSL_v201403.pdf	versie 1 van een gesystematiseerde inventarisatie van praktijken rond keten- governance.

Onderwerp	Product	Doel/omschrijving
Responsible Disclosure	**Handreiking voor implmentatie** http://www.cip-overheid.nl/wp-content/uploads/2014/04/Handreiking-implementatie-Responsible-Disclosure-v099-1.pdf	Handreiking die helpt bij de inrichting van dit proces in de organisatie.
Privacy	**Handreiking Meldplicht Datalekken** http://www.cip-overheid.nl/wp-content/uploads/2014/09/201409xx_Meldplicht_v01.pdf	Statusoverzicht en praktische adviezen bij de implementatie in de organisatie.
	Testen met Persoonsgegevens http://www.cip-overheid.nl/wp-content/uploads/2014/04/Testen-met-persoonsgegevens-v1_2-CIP-DEF4.pdf	Testen met 'echte' persoonsgegevens is soms bijna onvermijdelijk. Hoe kan je hiermee omgaan?
	Publicaties over Privacy management http://www.cip-overheid.nl/downloads/privacy-management/	Van kennispartner PMP: over privacy aspecten rond de Decentralisaties.
	Aanpak PIA http://www.cip-overheid.nl/wp-content/uploads/2014/05/Whitepaper-PIA.pdf	Van kennispartner Consideratie: PIA, hoe pak je het aan?
	PIA Norea http://www.cip-overheid.nl/wp-content/uploads/2014/05/Norea-PIA-Introductie-Handreiking-en-Vragenlijst.pdf	NOREA-Uitwerking van de PIA-aanpak.
	PIA Checklist http://www.cip-overheid.nl/wp-content/uploads/2014/05/Checklist-PIA.docx	Tool voor PIA checklist.
Cloud	**Handreiking Beveiligingsbeleid Clouddiensten** http://www.cip-overheid.nl/wp-content/uploads/2014/04/Beveiligingsbeleid-clouddiensten-CIP-DEF-v2_3-excl-ARD.pdf	Praktische richtlijnen voor het gebruik van Clouddiensten.
	De rol van de IT-Auditer http://www.cip-overheid.nl/wp-content/uploads/2014/08/Clouddiensten-van-de-Rijksoverheid-en-de-rol-van-de-IT-auditor-1.0.pdf	Van ADR: Een verkenning van de auditmogelijkheden van clouddiensten bij de rijksoverheid (ingebracht document).
Normatiek	**SIVA, ISBN9789086596706** Auteur Wiekram Tewarie	Methodiek voor de ontwikkeling van auditreferentiekaders.
	NCSC-Webrichtlijnen, versie 2 Overgedragen aan NCSC.	Op SIVA gebaseerde uitwerking van de NCSC-webrichtlijnen

4. ACTIVITEITEN I.K.V. KENNISDELING EN -ONTWIKKELING

Met het doel kennisdeling en interactie over het vakgebied te stimuleren, zijn door het jaar heen tal van bijeenkomsten belegd, soms gericht op de gehele community, soms op doelgroepen daarbinnen. De belangrijkste worden hierna genoemd.

Conferenties

De conferenties, die plaatsvonden op 5 juni en 27 november, trokken resp. 190 en 210 mensen van ca. 110 organisaties. De conferenties hebben een opbouwende werking bij de versterking van de community. Naast de inhoud wordt door de deelnemers veel waarde gehecht aan het onderlinge netwerken. Overall waardering van beide conferenties lag op een 8.

Domeingroepen

De vier domeingroepen hebben door het jaar heen kennis gedeeld over de thema's Privacy, Awareness, Ketenproblematiek en Normatiek. Over de drie laatste thema's is ook uitwisseling geweest met de Taskforce BID.

Een nieuwe domeingroep werd opgericht: Identiteitsfraude. Een tweetal sessies trokken een flink aantal mensen. Deze domeingroep wordt voorgezeten door Wouter Fellendans van het ministerie van BZK.

Kennispartnersessies

In Kennispartnersessies komen een of meerdere CIP-kennispartners aan het woord over specifieke thema's. Vaak ook met inschakeling van sprekers uit de overheid. Opkomst is zeer verschillend. De sessies over privacy trekken i.h.a. veel mensen (ca. 70 per sessie).

Een drietal Privacysessies werd gehouden, in maart, april en oktober, met wisselende inbreng van kennispartners Privacy Management Partners, Considerati en KPN i.s.m. Nationale politie, Eenheid High Tech Crime, UWV en Gemeente Enschede.

In oktober vond een bijeenkomst plaats met Ordina over Meetbaar Veilig Gedrag, iets dat in 2015 een vervolg krijgt naar een concrete aanpak. Daarnaast werd i.s.m. de Taskforce BID een sessie belegd in november over het beschikbare aanbod van iBewustzijn.

Presentaties

CIP maakt enthousiast gebruik van de mogelijkheden om als spreker het belang van informatieveiligheid onder de aandacht te brengen en ook richtingen voor oplossingen aan te reiken. De belangrijkste optredens bij andere organisaties waren:

- 15 jan: presentatie en aanbieding SSD op iBestuur-congres;

- 28 jan: presentatie op iBestuursessie over de bijdrage van IB aan de business;
- 7 febr: presentatie van CIP aan Amsterdamse Young Professionals (YAIC);
- 19 febr: presentatie SSD in ICCIO/Subcommissie IB;
- 21 maart congres Saxion Hogescholen bij de Belastingdienst;
- 7 mei: Presentatie CIP bij BIR-Coordinatorenoverleg van het Rijk;
- 27 mei: presentatie SSD bij het Nederlands Genootschap voor Informatica (NGI);
- 3 juni: presentatie samen met SIG op NCSC-congres over SSD;
- 30 juni: presentatie in sessie RBB, over samenwerking en leeraanbod;
- 6 oktober: (betrokkenheid bij) kennisexpeditie naar Shell;
- 27 oktober (betrokkenheid bij) Bestuurlijk Diner Taskforce BID;
- 9 oktober congres ISACA/PvIB/Norea: presentatie SSD;
- 3 nov. CIO-Café: Goed Opdrachtgeverschap, CIP betrokken vanuit Grip op Beveiliging in Inkoopcontracten.

CIP Cyber Security Platform (CSP)

Het Cyber Security Platform kent een uitdrukkelijk publiekprivate samenstelling. De opkomst bij de sessies varieerde tussen de 30 en 35 mensen van zo'n 20 tot 25 organisaties. De volgende sessies vonden plaats in 2014:

- januari: CSP-sessie over SOC; hierbij werd ook een werkgroep SOC gevormd die mogelijkheden voor verdergaande samenwerking onderzoekt;
- maart: CSP-sessie over Crisismanagement;
- juni: CSP-sessie met 'ISAC-deelnemerssegment' als kick-off van het Rijks-ISAC.

Rijks-ISAC

CIP nam halverwege dit jaar het initiatief tot de vorming van het Rijks-ISAC, i.s.m. de Rijks-BVA. Dit is een overleg dat verder gefaciliteerd wordt door het NCSC en inmiddels in de reguliere overlegstructuur van het NCSC is opgenomen. I.s.m. NCSC werden de volgende vergaderingen belegd in 2014:

- In september: de eerste echte vergadering als ISAC (22 mensen uit 20 organisaties namen deel);
- In december de tweede vergadering van het ISAC. Frank Katsburg van SVB werd daarbij benoemd in de rol van voorzitter voor de duur van 2 jaar.

Nu NCSC de facilitering op zich heeft genomen, is CIP teruggetreden als facilitator.

5. ACTIVITEITEN OP HET GEBIED VAN SAMEN-WERKEN.

Practitioners Communities

In 2014 is een tweetal zg. 'Practioners Communities' (PraCo's) in werking gegaan: een voor Secure Software Development (SSD) en een voor 'Keten Service Library' (KSL). De PraCo's zijn gericht op organisaties die deze producten echt gebruiken of het voornemen hebben dat te doen. Doel is: leren van elkaars ervaringen, stimuleren en inspireren van elkaar tot implementatie, het stimuleren van het opnemen van het gedachtegoed in het aanbod van leveranciers en het evolueren van de producten.

Nadat in januari op het iBestuurcongres de lancering van SSD en de aanbieding daarvan aan de Rijks-CIO plaatsvond, is in de loop van het voorjaar de PraCo opgericht. Aangesloten organisaties zijn:

- Overheid: ADR, AMC, Belastingdienst, Ministerie van BZK, V&J/DJI, VWS/CIBG, Rijkswaterstaat, SSC-ICT Haaglanden, SVB, UWV.
- Markt: Capgemini, CGI, DKTP, IBM, KBBa, Key2Control,Ordina, SIG, SNS Reaal, Sogeti, Valori, Cert2Connect, Open Novations, Owasp/Chapter leader Nederland.

PraCo-bijeenkomsten werden belegd in maart, april, juni, september en november. Verschillende presentaties werden gehouden bij enkele participanten, Noordertest, e.a. Door het ondertekenen van een manifest kunnen partijen zich committeren aan het toepassen en uitdragen van SSD.

De roep om een Engelse versie van SSD wordt steeds sterker. Marktpartijen willen het document ook in hun offshorevestigingen opleggen aan de ontwikkelaars. Daarnaast zou de verbreiding en bredere acceptatie van de methode gediend kunnen zijn met een neutrale ophanging als algemene standaard, die zich zou kunnen ontwikkelen naar een internationale standaard. In 2015 zullen we bezien welke stappen op deze gebieden te maken zijn.

De PraCo KSL is eveneens meerdere keren bijeen geweest. Het accent in de meetings lag vooral op het delen van ervaringen met ketenproblematiek door Kennispartners. Aangezien de inventarisatie van governancepraktijken binnen de Keten Service Library nog niet compleet is, wordt ook bezien of er praktijken zijn die zich lenen voor opname in de library.

Gezamenlijke normatiek

T.b.v. het stimuleren van gezamenlijke normstelling zijn de volgende activiteiten ondernomen.

- Meerdere sessies werden belegd met de Audit Dienst Rijk over SIVA en de NCSC-richtlijnen, ter bevordering van het gebruik van SIVA in normenkaders. Verschillende thema's voor uitwerking met SIVA zijn ter hand genomen maar nog niet afgerond:

- het beheer van de IT-infrastructuur van een gemeentelijk jeugdzorgproject,
- het beheer van medewerkers en toegang: authenticatie van zowel medewerkers als beheerders en
- uitbestede netwerkdiensten en hosting.

- Introductie van ITOMM (IT-Object Maturity model). Dit is een op SIVA gebaseerde toepassing van een organisatievolwassenheidsmodel, m.m.v. DPA/B-Able, die ook een eigen tool (de Securimeter) hierop heeft ingericht.
- Voorbereiding en Kick-off dagen BIR/ZBO, samen met de Taskforce BID.
- Op 19 mei werd een kick-off dag gehouden met SZW, UWV en SZW, waarbij een bestuursverklaring werd getekend.

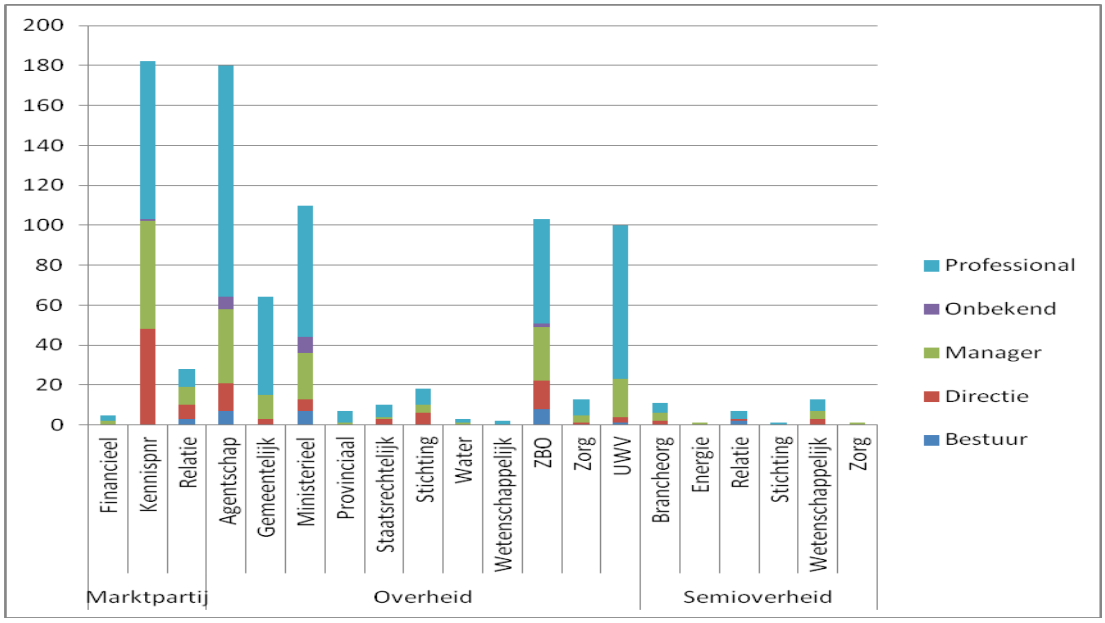
Veilig Delen: Local Box

In juni vond een tweetal sessies plaats (inschrijven was mogelijk tijdens de voorjaarconferentie) om partijen te informeren over de ontwikkeling van local box. In september volgde een sessie 'Seminar Veilig Delen' in sociëteit de Witte in samenwerking met ECP, waarbij veel belangstelling was voor Local Box. Een bruikbare betaversie heeft enige vertraging opgelopen. Deze wordt nu verwacht in januari 2015.

6. ONTWIKKELING VAN HET CIP-NETWERK

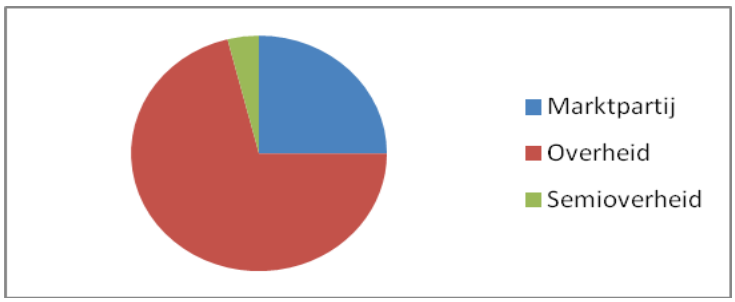
Aantallen personen naar soort organisatie en functie

In onderstaande grafiek is te zien in welke typen organisaties en functies de ruim 850 personen in het CIP-netwerk werken en in welke verdeling.



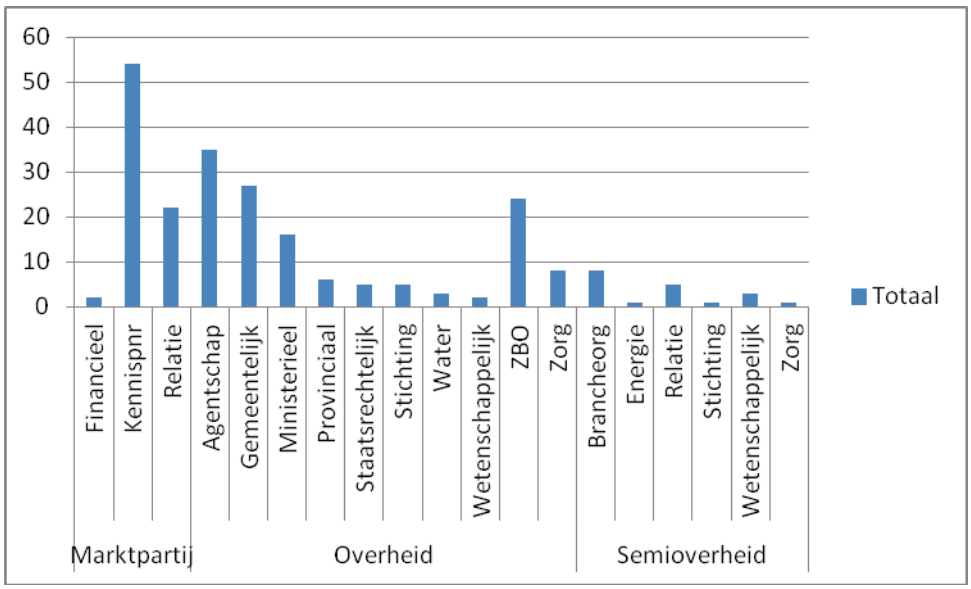
NB. Aangezien vanuit UWV een relatief groot aantal mensen is aangehaakt, en daarmee de cijfers van de categorie ZBO zou vertekenen, is UWV in deze grafiek apart uitgesneden.

Verdeling personen in het netwerk over Overheid, Semioverheid en Markt:



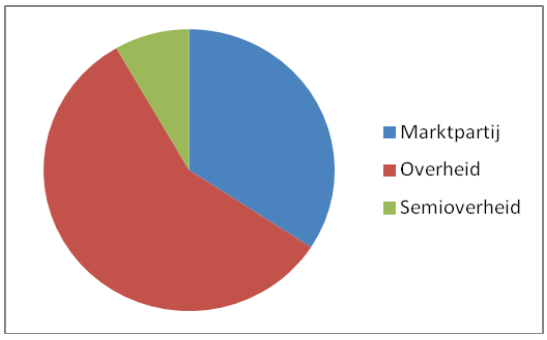
Aantallen organisaties naar sector en soort

Onderstaande grafiek geeft een beeld van de verdeling over sectoren van de ca 220 organisaties die zijn aangehaakt bij CIP.



NB. De kolom kennispartners is relatief hoog. Dit komt omdat binnen deze categorie geen nadere indeling is gemaakt; alle marktpartijen die een convenant met CIP hebben, worden hier samengepakt. Hetzelfde geldt voor de categorie 'Relaties': marktpartijen zonder kennispartnerstatus.

Het volgende schema laat duidelijker zien hoe de organisaties zijn verdeeld over Overheid, Semioverheid en Markt:



Toename kleine ZBO's

In het belang van brede aandacht voor informatieveiligheid binnen de gehele overheid, zijn in 2014 stappen gezet om ook kleinere ZBO's te interesseren voor de CIP-samenwerking. Dit heeft een aantal nieuwe participanten opgeleverd. De kleinere partijen zullen in de eerste plaats nut hebben van hetgeen grotere partijen bijdragen. Van de volgende kleinere ZBO's mochten we mensen verwelkomen in het netwerk:

- Autoriteit Consument en Markt
- Autoriteit Financiële Markten
- Huurcommissie
- Kansspelautoriteit
- Koninklijke Bibliotheek
- Luchtverkeersleiding Nederland
- Participatiefonds
- Raad voor Strafrechttoepassing en Jeugdbescherming
- Staatsbosbeheer
- Stichting Nederlands Fonds voor Podiumkunsten

7. OUTLOOK 2015

Het jaar 2015 zal in het teken staan van het voortzetten van de portfolio van werkverbanden/kennisdelingssessies die zijn opgezet, het voorzetten en actueel houden van het productportfolio en het voorzetten en intensiveren van de in 2014 gestarte, meer op implementatie gerichte activiteiten.

In het eerste kwartaal van 2015 zal de Taskforce BID worden afgebouwd. Een aantal interbestuurlijke verbanden zullen worden voortgezet. In samenwerking met het ministerie van BZK en enkele koepelorganisaties zal CIP hierin een belangrijke rol blijven spelen. We verwachten de komende tijd in overleg met de Taskforce BID meer zicht te ontwikkelen op de consequenties van het beëindigen van de taskforce voor de rol van CIP. Daarbij zal ook bepaald worden welke van de producten van de taskforce door CIP overgenomen worden in het productaanbod.

De grote belangstelling waarin CIP zich mag verheugen en de toename van zowel het aantal producten als het aantal implementatiegerichte werkverbanden, ervaren we als een zeer positief teken van betrokkenheid bij de thematiek van informatieveiligheid bij een groot aantal overheidsorganisaties. CIP zit hiermee in het hart van zijn missie, die als volgt verwoord werd in het inrichtingsplan (2012):

'Het CIP helpt en ondersteunt de Participanten bij het zodanig veilig krijgen en houden van hun informatievoorziening dat

- *Participanten elkaar kunnen vertrouwen op het gebied van de integriteit en beschikbaarheid van de onderlinge gegevensstromen in de ketens die zij vormen en*
- *burgers kunnen vertrouwen op de integriteit, de beschikbaarheid en de vertrouwelijkheid van de gegevens en diensten die zij via de aangeboden kanalen afnemen bij de Participanten.'*

Het managen van enerzijds deze groei en anderzijds het verwezenlijken van de hiervoor genoemde ambities zal in 2015 extra creativiteit vergen. Met de huidige budgetten en inzet zitten we in dit jaar aan de grens van de mogelijkheden. De budgetten van de Founding Fathers blijven in 2015 gelijk aan die van 2014; eventuele groei zal alleen gerealiseerd kunnen worden door inzet van de andere deelnemers (participanten en kennispartners).

De plannen voor 2015 zijn nadere uitgewerkt in het CIP-Jaarplan. Voor het jaarplan, plak deze URL in uw browser: https://cip.pleio.nl/file/view/29267182/cip-jaarplan-2015.