

# 4-kwartaals terugblik CIP. Datum 1-12-2016.

Verslagperiode: 1-1-2016 - 31-12-2016

## Inhoud

1.	Over CIP .....	2
1.1	CIP-diensten zijn te positioneren op 3 niveaus .....	2
1.2	Kernpunten in de opzet, de werkwijze en de cultuur van CIP .....	2
1.3	Tevreden als.....	2
2.	CIP-Netwerk in cijfers .....	3
2.1	Aantal en verdeling van personen in het CIP-Netwerk .....	3
2.2	Aantal en verdeling van organisaties in het CIP-Netwerk.....	3
3	De subcommunities.....	4
3.1	Domeingroepen.....	4
3.2	Practitioners Communities .....	5
4	De sites .....	6
4.1	Cip-overheid.nl: .....	6
4.2	Cip.pleio:.....	6
5	CIP-Conferenties.....	6
6	Diensten.....	6
6.1	Privacy vraagbaak:.....	6
6.2	Privacy Workshop:.....	7
6.3	Uitvoering Serious Game Crisis: .....	7
6.4	Collegiale Toetsing.....	7
7	Externe betrekkingen en belangstelling.....	7

## 1. Over CIP

CIP is een publiek-private netwerkorganisatie voor zowel kennisdelen en- ontwikkelen als krachtenbundeling op het terrein van Informatieveiligheid en Privacybescherming.

Trekker is UWV; de overige 'founding fathers' zijn Belastingdienst, DUO en SVB.

Bestuurders van deze organisaties vormen (samen met die van CIZ en CAK) het Bestuurlijk Overleg Compacte Uitvoering (BOCU), dat het CIP faciliteert en een RvT-achtige functie invult t.o.v. CIP. CIP heeft daarmee de signatuur van de uitvoerende overheid.

Vele organisaties - uit alle overheidslagen - hebben zich aangesloten bij het CIP, met mensen die meedoen of meeliften in verschillende werkverbanden en subcommunities.

### 1.1 CIP-diensten zijn te positioneren op 3 niveaus

- 1 Activiteiten voor kennisdeling: domeingroepen, themasessies en conferenties.
- 2 Kennisproducten: handreikingen, normenkaders, e-learning, filmmateriaal, etc.
- 3 Implementatie en samenwerking: practitioners communities en netwerkdiensten.

### 1.2 Kernpunten in de opzet, de werkwijze en de cultuur van CIP

- Klein kernteam - groot netwerk;
- Open voor alle overheidsorganisaties;
- Open voor marktpartijen die bij convenant uren toezeggen voor kennisdeling op relevante kennisgebieden;
- Gerichtheid: dienstbaarheid, niet voorschrijvend;
- Geen hiërarchie in het netwerk; iedere organisatie is operationeel verantwoordelijk voor de eigen informatieveiligheid;
- Dingen alleen doen in zoverre er energie voor is vrij te maken in het netwerk, én die dan ook te bemannen zijn met uren van participanten en kennispartners uit het netwerk;
- Maximale waardering van diversiteit en het aanboren daarvan bij de kennisontwikkeling;
- Als er geen energie (meer) is voor een activiteit: stoppen;
- Ongeacht de omvang van het netwerk: waar mogelijk persoonlijke communicatie. Dus: mailmerge en op voornaam (één stijl);
- Zorgvuldig communiceren, hetgeen (ook bij massa-mailings) betekent: denken in termen van de context van de ontvanger. Dit leidt vaak tot mailings in meerdere tekstvarianten;
- Sluitende netwerkregistratie om voorgaande mogelijk te maken.

### 1.3 Tevreden als...

CIP is succesvol als overheidsorganisaties en hun medewerkers de producten, diensten en bijeenkomsten van het CIP ervaren als een relevante bijdrage bij hun inspanningen de informatieveiligheid en het privacy-bewust handelen te vergroten.

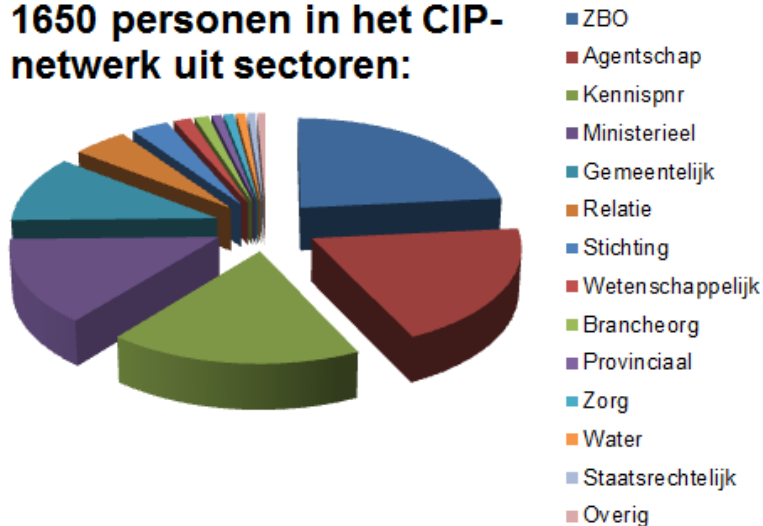
In november is een enquête naar productgebruik uitgezet onder 900 mensen in het netwerk. De response was 40%. De cijfers geven het beeld van een flink verspreid gebruik van de producten en van de sites. Dit schraagt de hoop die we hierover al hadden op grond van de vele positieve reacties in de praktijk. Uitzondering: de CIP-casts waarvoor extra – en meer toegespitste communicatie nodig is.

## 2. CIP-Netwerk in cijfers

### 2.1 Aantal en verdeling van personen in het CIP-Netwerk

Op 1-12-2016 bestaat CIP-netwerk uit 1650 personen. Onderstaand schema geeft aan bij welke typen organisaties zij werken.

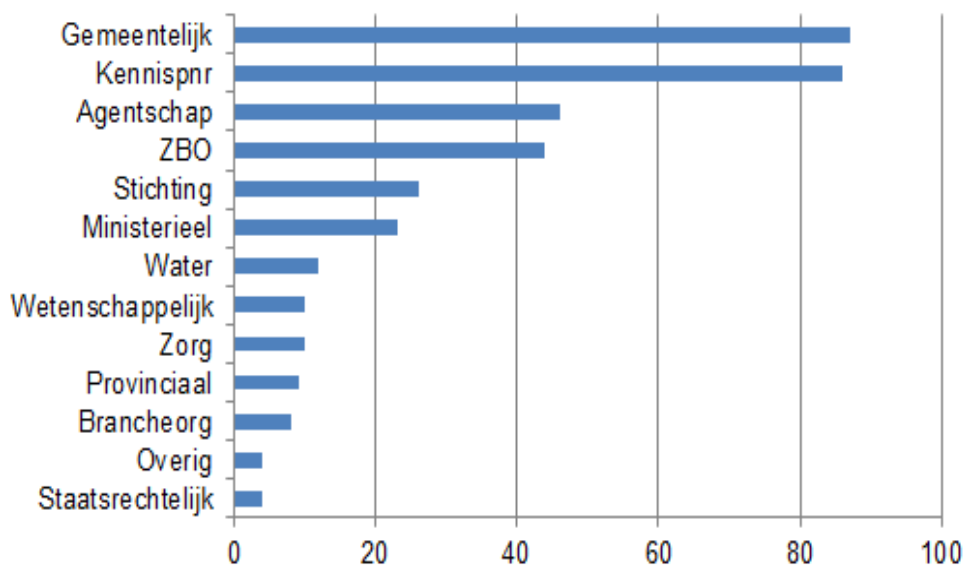
#### 1650 personen in het CIP-netwerk uit sectoren:



### 2.2 Aantal en verdeling van organisaties in het CIP-Netwerk

Onderstaande grafiek geeft aan hoeveel organisaties er zijn vertegenwoordigd in het CIP-netwerk, per 1-12-2016. In de balk 'Kennispartners' zijn alle met convenant aangesloten marktpartijen bijeen geteld. Overige balken betreffen de organisaties in de verschillende overheidslagen. Doordat de site iBewustzijn (voortzetting van de taskforce) opgeheven wordt per 1-12-17 en de mensen naar CIP verwezen zijn, is het aandeel gemeenten flink toegenomen. Vaak overigens met maar 1 of 2 mensen per gemeente.

#### Aantallen organisaties naar soort



## 3 De subcommunities

### 3.1 Domeingroepen

#### DG Awareness

Brengt 2-wekelijks CIP-casts uit. Dit zijn filmpjes die in enkele minuten een IB&P-vraagstuk belichten. De voorraad groeit. We werken met een systeem van sponsors die voorzien in de kosten van een draaidag. Een draaidag levert 4 filmpjes op.

Draaidagsponsors in de verslagperiode waren: OM, SVB, DUO, LBVD en Fox-IT.

Serious Game 'Crisis' is ontwikkeld en geniet grote belangstelling. D.m.v. een slim verspreidingsmodel hebben we in korte tijd een kring van 25 moderators kunnen samenstellen uit het netwerk. VNG/IBD biedt het aan, aan gemeenten en hanteert een vergelijkbaar verspreidingsmodel. Ook is een gemeentevariant opgeleverd door VNG. Deze is ook in uitvoering genomen in het CIP-netwerk.

#### DG Governance & Normatiek

Ontwikkelt gestaag aan thema-uitwerkingen o.b.v. SIVA. Als handvatten voor implementatie BIR. Dit leidt op termijn tot een 'Objectgebaseerde Normen Bibliotheek' die de complete scope van de BIR invult: de 'Information Security Object Repository' (ISOR). Daarbij wordt samengewerkt met BZK, VNG/IBD, Waterschappen en Provincies in de 'Werkgroep Normen'.

Voor de vastlegging en ontsluiting van ISOR maken we inmiddels gebruik van de WIKI-oplossing van NORA. In NORA worden daarmee alle Normen op het terrein van Informatieveiligheid opgenomen en beschikbaar gesteld.

#### DG Privacy

De afgelopen anderhalf jaar is een rijke productontwikkeling tot stand gebracht gericht op concrete handvatten voor verantwoord, privacy-bewust handelen in organisaties: Grip-op-Privacy. Dit omvat een 'Baseline Privacy', een handreiking voor Privacy by Design en een volwassenheids-groeimodel.

Uit de door CIP in november 2015 gehouden enquête over privacy governance (79 respondenten) En uit de recente enquête over productgebruik (november 2016) blijkt een forse belangstelling voor het gebruik van de privacy-producten.

In het voorjaar werd een themasessie belegd. De opkomst lag in de orde van 70 mensen van 50 organisaties.

#### DG Ketens

Om verschillende redenen liep deze domeingroep niet goed meer. Energie in het netwerk ontbrak. Deze domeingroep is daarom omgebouwd naar een werkgroep die één product oplevert, tw: een Serious Game Informatieveiligheid in Ketens. Deze ontwikkeling loopt door tot medio 2017.

Het game-instrument heeft een groot leereffect en de belangstelling om het in te zetten is groot. Voor de ontwikkeling bleek veel energie vrij te maken, getuige een aantal nieuwe mensen dat eraan wil bijdragen.

Het product Keten Service Library is geactualiseerd naar een 2016-versie.

#### DG ID-Fraude

Dit is een samenwerking met BZK. Herbezinning volgt in de loop van de komende maanden, nu de voorzitter in de reorganisatie van BZK een andere functie heeft betrokken.

## 3.2 Practitioners Communities

De PraCo is een vorm van uitwisseling die specifiek is bedoeld om van elkaars praktijkvragen en -problemen te leren en de producten en practices die het CIP aanbiedt, te helpen implementeren en verbeteren met leereffecten vanuit de praktijk. In 2016 is één PraCo beëindigd (de PraCo KSL), waarvoor niet langer voldoende energie was vrij te maken in het netwerk. Ketenthematiek wordt vanaf het najaar 2016 uitdrukkelijk meegenomen/verweven in de andere PraCo's.

De volgende PraCo's zijn actief, dan wel gestart in 2016.

### **PraCo SSD: (publiek-privaat)**

Blijvend veel belangstelling. Ook in landelijke pers. Implementatie verspreidt zich: Overheid: UWV, DUO, SVB, CAK, ICTU, DICTU, ACM, CIBG, VWS en Logius zijn de belangrijkste. SSCI/DJI wil de SSD-mobile gebruiken als toets in de teststraat die in opzet is.

Grote en kleine ICT-leveranciers en een groep overheidsorganisaties hebben het 'SSD-Manifest' ondertekend.

Een aantal marktpartijen kunnen SSD-conform leveren en voeren het in (IBM, Capgemini, Sogeti, Centric en een aantal kleinere partijen). Ordina en CGI overwegen manifestpartij te worden.

In 2016 vonden 3 meetings plaats van de PraCo. Opkomst was doorgaans: ca. 40 aanwezigen van ca. 25 organisaties.

Enkele werkgroepen werken aan nuttige toevoegingen. SSD – testen werd opgeleverd.

Verschillende masterclasses en trainingen met gebruikmaking van kennispartners (Valori, Securify) op dit gebied in 2016.

Medio 2016 is ook de Engelse vertaling van het volledige Grip-op-SSD compleet geworden. Deze is ook toegelicht door kennispartner SIG op de OWASP-conferentie in Rome.

### **PraCo BIR: (publiek)**

Een levendige groep, met verschillende werkgroepjes die uitwerkingen doen. Deze PraCo is een samenwerking met de implementatiecoördinator bij het rijk (BZK).

### **PraCo Awareness: (publiek-privaat)**

Gestart 7 april 2016. Deze community omvat ca.60 mensen.

I.s.m. iBewustzijn Rijk. Belangstelling is groot om ervaringen te delen uit awareness-campagnes en materiaal te delen. CIP-awareness materiaal komt ook ruim aan de orde.

In 2016 hebben drie bijeenkomsten plaatsgevonden.

### **PraCo Veilig Inkopen (publiek)**

Gestart 16 maart 2016. 137 mensen zijn aangesloten op deze subcommunity.

Dit is bedoeld als een community voor de geleding inkopers en contractmanagers binnen het CIP-netwerk. Doel is versterking en ook in deze geleding enthousiasmeren tot ingebruikname van nuttig CIP-materiaal.

Twee bijeenkomsten vonden plaats.

## PraCo Privacybescherming.

Op 14 september is gestart met de 'Practitioners Community' (PraCo) voor het thema Privacybescherming. De PraCo Privacybescherming is daarnaast ook bedoeld om de documenten Grip-op-Privacy uit te leggen en toe te passen. Met de feedback van PraCo-leden worden deze stukken ook verder verrijkt en aan de praktijkervaringen aangepast, als daartoe behoefte is.

Bij de belangstellingsuitvraag, die in juni plaatsvond, blijkt zeer veel animo voor deze PraCo. De eerste bijeenkomst werd bezocht door 75 mensen.

## 4 De sites

### 4.1 Cip-overheid.nl:

Gebruik voor distributie van deelbaar materiaal. Alles op deze site wordt gedeeld onder Creative Commons/Naamsvermelding-Gelijk delen. Zie productenlijst.

Hoeveelheid updates neemt aanzienlijk toe. Logischer ontsluiting van de producten op de site is nodig en wordt bereikt in juni.

Met het oog op de beveiliging van site zijn we medio 2016 overgegaan naar een andere hostingpartij.

### 4.2 Cip.pleio:

Besloten samenwerkingsomgeving voor het CIP-netwerk. Hier staan ook halffabricaten van komende producten, discussies, laatste IB&P-nieuws, etc. Cip.pleio wordt ook gebruikt om allerlei stukken en practices te delen die (nog) niet als afgerond CIP-product op de externe site worden geplaatst.

Het aantal leden is de laatste tijd fors gegroeid: 725 mensen zijn lid.

## 5 CIP-Conferenties

In 2016 op 26 mei en 24 november.

Beide conferenties trokken een volle zaal. Met het oog op de capaciteit van de locatie is het aantal aanwezigen gemaximeerd op ca. 250 personen. De belangstelling is inmiddels groter, maar met het oog op zowel kosten als sfeer leggen we hier vooralsnog de grens. De conferenties werden ook hoog gewaardeerd (voorjaar: 8.3). Aanwezigen kwamen uit meer dan 150 verschillende organisaties. Een kleine helft van de deelnemers was er voor het eerst.

## 6 Diensten

In het jaarplan 2016 is een start gemaakt met zg. netwerk-gebaseerde dienstverlening. Dit zijn diensten door en voor leden van het CIP-netwerk. De stand van zaken is als volgt:

### 6.1 Privacy vraagbaak:

Iedereen met een vraag over Privacy kan die stellen in een aparte groep op cip.pleio. Het kernteam ziet toe op beantwoording. Deze dienst is gestart in febr 2016 en komt na een aarzelende start goed op gang. Deze dienst is in de nieuwe PraCo Privacybescherming voor het voetlicht gebracht en regelmatig gecommuniceerd. Daarna is het gebruik toegenomen. Beantwoording van de vragen behoeft vrijwel geen moderatie vanuit CIP-Sloterdijk.

## 6.2 Privacy Workshop:

Rond de CIP-producten 'Grip-op Privacy' zijn inmiddels meerdere workshops georganiseerd die goed gewaardeerd werden. Verbeterpunten werden geïnventariseerd en zijn verwerkt in de opzet van de workshop. De workshop wordt ook in het netwerk aangeboden als dienst en kan ook worden afgenomen bij kennispartner PBLQ.

## 6.3 Uitvoering Serious Game Crisis:

In 2015 is product tot stand gebracht en uitgevoerd op de najaarsconferentie. We hebben dit product aangeboden om uit te voeren bij organisaties in het netwerk.

Om een olievlekwerking te bereiken, hanteren we een verbreidingsstrategie, waarbij organisaties die het willen uitvoeren twee moderators door ons laten instrueren. Tijdens de eerste uitvoering door deze moderators loopt nog een ervaren moderator mee; bij volgende groepen doet men het zelf, waarbij we de bereidheid vragen het ook eens te willen doen bij een collega-organisatie. Zo ontstaat een groeiende groep moderators (nu ca. 25) die de dienst kunnen leveren. Ook dit gebeurt met gesloten beurs.

De animo om de game in te zetten is zeer groot in het netwerk. In 2016 is de game ca. 25 maal uitgevoerd bij/door tal van organisatie, waarvan ca. 12 maal in de AlertOnline weken. Ook op de heidag van departementale CIO's (7 december) wordt de game uitgevoerd.

Veel deelnemers aan deze sessies gaven aan de game in hun eigen organisatie te gaan uitvoeren. CIP verzorgt de instructie van de moderators in deze organisaties.

## 6.4 Collegiale Toetsing

Binnen het CIP-netwerk wordt kennis uitgewisseld inzake allerlei onderwerpen op het gebied van de Informatieveiligheid. Zowel in bijeenkomsten van verschillende aard en verschillende bloedgroepen waarin praktijkkennis wordt uitgewisseld, als door middel van diverse downloadbare kennisproducten en practices. Dit laat onverlet dat soms behoefte kan bestaan meer de diepte in te gaan op specifieke thema's en heel gericht te spiegelen met collega's in het netwerk over specifieke probleemstellingen, plannen, etc binnen de eigen organisatie.

Met het ook hierop ontwikkelt CIP een Collegiale Toets met als doel het verkrijgen van inzichten en tips van collega's, die zich vanuit een niet directe betrokkenheid met het onderwerp (maar wel met de benodigde kennis) als neutrale gesprekspartner kunnen opstellen.

Een eerste pilot-uitvoering vond plaats op 19 mei binnen de PraCo BIR in laboratoriumopstelling, uitgevoerd in de vorm van een 'vissenkomsessie'. Bij de observerende groep aanwezige Praco-leden is interesse gewekt en werd feedback geogst, die is meegenomen in het protocol/format van deze dienst.

Een groep van 9 reviewers is gemotiveerd om af en toe een Peer Review uit te voeren. In het najaar wordt deze dienst aangeboden in het netwerk. Provincie Noord-Holland is de eerste die meedoet. Een team van 3 mensen (van Rijkswaterstaat, Belastingdienst en Gemeente Amsterdam) verzorgen de review onder de CIP-vlag.

## 7 Externe betrekkingen en belangstelling

CIP is veelvuldig in de vakpers. Zowel in Computable, Automatiseringsgids, Computer Weekly, en andere ICT-organen, als op digitale overheid, nieuwsbrieven van ministeries, privacy-nieuwsbrieven, ed. zijn we met regelmaat te vinden. Meestal gaat het dan over Secure Software Development of Grip op Privacy. Ook de BIT-bijlage van het FD is bereikt met een artikel over SSD-mobiel.

CIP neemt deel in het SIB van het CIO-Beraad, zit in de adviesraad van VNG-Informatiebeveiligings-dienst, is lid van de Redactieraad iBewustzijn Overheid en het NCSC-Nationaal Expertisenetwerk en is jaarlijks partner van Alert-Online.

CIP neemt deel in het overleg over de implementatie van de AVG in de Nederlandse wetgeving. (Trekker SZW).

Op de site iOverheid heeft CIP een partnerpagina waarop o.a. nieuwe releases van CIP-producten worden geannonceerd.

Na de zomer zal CIP ook het onderdeel Informatieveiligheid binnen NORA gaan behartigen. Daartoe wordt een partnership met NORA ondertekend.

Met iBewustzijn Overheid worden de mogelijkheden verkend om nog een aantal awareness-producten over te nemen op de CIP-site. Dit hangt samen met het al of niet doorgaan van het programma iBewustzijn Overheid. (Op het moment van schrijven is dit nog niet duidelijk).

Daarnaast spreken we ook dit jaar weer op meerdere congressen (Software Industry Congress, Norea/ISACA-congres, Platform voor Informatiebeveiliging, Congres Privacy V&J, Landelijk Architectuurcongres en KleinLef), Ketenoverleg Zorginstituut Nederland, iBestuur).